



COPYRIGHT

This manual is proprietary to SAMSUNG Electronics Co., Ltd. and is protected by copyright. No information contained herein may be copied, translated, transcribed or duplicated for any commercial purposes or disclosed to the third party in any form without the prior written consent of SAMSUNG Electronics Co., Ltd.

TRADEMARKS

Ubigate iBG is a registered trademark of SAMSUNG Electronics.
All other company and product names may be trademarks of the respective companies with which they are associated.

This manual should be read before the installation and operation, and the operator should correctly install and operate the product by using this manual.

This manual may be changed for the system improvement, standardization and other technical reasons without prior notice.

If you have a question for the content of manual or want to obtain further information on the updated manual, please contact the homepage below.

Homepage: <http://www.samsungdocs.com>



GENERAL USER INFORMATION

Radio Frequency Interference

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

FCC Requirements

This equipment complies with Part 68 of the FCC rules and the requirements adopted by the ATCA. On the side or bottom of the equipment is a label that contains, among other information, a product identifier in the format **US: A3LIS00BiBGxxxx**. If requested, this number must be provided to the telephone company.

Unauthorized Modifications

Any changes or modifications performed on this equipment that are not expressly approved in writing by SAMSUNG ELECTRONICS, CO., LTD. could cause non-compliance with the FCC rules and void the user's authority to operate the equipment.



Allowing this equipment to be operated in such a manner as to not provide for proper answer supervision is a violation of Part 68 of the FCC's rules.

Telephone Connection Requirement

A plug and jack used to connect this equipment to the premises wiring and telephone network must comply with the applicable FCC Part 68 rules and requirements adopted by the ATCA. A compliant telephone cord and modular plug is provided with this product. It is designed to be connected to a compatible modular jack that is also compliant. See installation instructions for details.

FCC Part 68

This equipment complies with Part 68 of the FCC rules. The FCC Part 68 label is located on the bottom chassis panel. This label contains the FCC Registration Number and Ringer Equivalence Number (REN) for this equipment.

If requested, this information must be provided to your telephone company. Connection to the telephone network should be made by using standard modular telephone jacks, type RJ-11C. The RJ-11C plug and/or jacks used must comply with the FCC Part 68 rules.

CIRCUIT TYPE	MODULE TYPE	FACILITY INTERFACE CODE	NETWORK JACK
LOOP START LINE	FXO-4M, FXO-2M T1E1-2M, T1E1-1M	02LS2 04DU9.DN 04DU9.1KN 04DU9.1SN 04DU9.1SN (PRI)	RJ11C RJ48C
	T1E1-4	04DU9.DN 04DU9.1KN 04DU9.1SN 04DU9.1SN (PRI)	RJ48C
DID LINE	FXS-4M, FXS-2M, FXS-24	02RV2.T	RJ11C
	T1E1-2M, T1E1-1M T1E1-4	04DU9.BN 04DU9.BN	RJ48C RJ48C
E & M TIE LINE	E & M-2M, E & M-1M	TL11M	RJ45S
	T1E1-2M, T1E1-1M T1E1-4	04DU9.BN 04DU9.BN	RJ48C RJ48C

Ringer Equivalence Number

The REN is used to determine the number of devices that may be connected to a telephone line. Excessive RENs on a telephone line may result in the devices not ringing in response to an incoming call. In most but not all areas, the sum of RENs should not exceed five (5.0). To be certain of the number of devices that may be connected to a line, as determined by the total RENs, contact the local telephone company. For earlier products, the REN is separately shown on the label.

Incidence of Harm

If this equipment causes harm to the telephone network, the telephone company will notify you in advance that temporary discontinuance of service may be required. But if advance notice isn't practical, the telephone company will notify the customer as soon as possible. Also, you will be advised of your right to file a complaint with the FCC if you believe it is necessary.

Changes to Telephone Company Equipment or Facilities

The telephone company may make changes in its facilities, equipment, operations or procedures that could affect the operation of the equipment. If this happens, the telephone company will provide advance notice in order for you to make necessary modifications to maintain uninterrupted service.

Service Center

If trouble is experienced with this equipment, contact your local office of SAMSUNG ELECTRONICS, CO., LTD. for repair or warranty information. If the trouble is causing harm to the telephone network, the telephone company may request that you remove the equipment from the network until the problem is resolved.

Field Repairs

Only technicians certified on the Ubigate iBG2006/2016/3026 are authorized by SAMSUNG ELECTRONICS, CO., LTD. to perform system repairs. Certified technicians may replace modular parts of a system to repair or diagnose trouble. Defective modular parts can be returned to SAMSUNG ELECTRONICS, CO., LTD. for repair.

General

Connection to party line service is subject to state tariffs. Contact the state public utility commission, public service commission or corporation commission for information.

Equipment with Direct Inward Dialing ('DID')

ALLOWING THIS EQUIPMENT TO BE OPERATED IN SUCH A MANNER AS TO NOT PROVIDE FOR PROPER ANSWER SUPERVISION IS A VIOLATION OF PART 68 OF THE FCC'S RULES

PROPER ANSWER SUPERVISION IS WHEN:

- A) This equipment returns answer supervision to the Public Switched Telephone Network (PSTN) when DID calls are:
- Answered by the called station
 - Answered by the attendant
 - Routed to a recorded announcement that can be administered by the Customer Premises Equipment (CPE) user.
 - Routed to a dial prompt
- B) This equipment returns answer supervision on all DID calls forwarded to the PSTN.
- Permissible exceptions are:
- A call is unanswered
 - A busy tone is received
 - A reorder tone is received

Equal Access Requirements

This equipment is capable of providing users access to interstate providers of operator services through the use of access codes. Modification of this equipment by call aggregators to block access dialing codes is a violation of the Telephone Operator consumers Act of 1990.

Electrical Safety Advisory

Parties responsible for equipment requiring AC power should consider including an advisory notice in their customer information suggesting the customer use a surge arrestor. Telephone companies report that electrical surges, typically lightning transients, are very destructive to customer terminal equipment connected to AC power sources. This has been identified as a major nationwide problem.

Music on Hold Warning



In accordance with US copyright laws, a license may be required from the American Society of Composers, Authors and Publishers (ASCAP) or other similar organizations if copyright music is transmitted through the Music on Hold feature.

SAMSUNG ELECTRONICS, CO., LTD. hereby disclaims any liability arising out of failure to obtain such a license.

DISA Warning

Lines that are used for the Direct Inward System Access feature must have the disconnect supervision options provided by the telephone company.



As it is impossible to control who may access your DISA line it is suggested that you do not turn this feature on unless you intend to use it. If you do use this feature, it is good practice to frequently change pass codes and periodically review your telephone records for unauthorized use.

Safety Warning



High touch current earth connection essential before making telecommunication network connection.



Energy Hazard-careful treatment is needed.



Every wire for communication should be larger than 26 AWG.



Double pole/neutral fusing.

Underwriters Laboratories

This system has been tested to comply with safety standards in the United States and Canada. This system is listed with Underwriters Laboratories.

The cUL Mark is separately shown on the label.

The following statement from Underwriters Labs applies to the Ubigate iBG2006/2016/3026 System:

- 1.** Separation of TNV and SELV - Pluggable A:
INSTRUCTION: The separate protective earthing terminal provided on this product shall be permanently connected to earth.
- 2.** Separation of TNV and SELV - Pluggable B:
INSTRUCTION; Disconnect TNV circuit connector(s) before disconnecting power.

3. Warning to service personnel:
CAUTION: Double pole/neutral fusing
4. Telephone line cord:
CAUTION: To reduce the risk of fire, use only No. 26 AWG or larger (e.g., 24 AWG) UL Listed or CSA Certified Telecommunication Line Cord
5. Leakage currents due to ringing voltage - Earthing installation instructions: '1. A supplementary equipment earthing conductor is to be installed between the product or system and earth, that is, in addition to the equipment earthing conductor in the power supply cord. 2. The supplementary equipment earthing conductor may not be smaller in size than the unearthed branch-circuit supply conductors. The equipment earthing conductor is to be connected to the product at the terminal provided, and connected to earth in a manner that will retain the earth connection when the power supply cord is unplugged. The connection to earth of the supplementary earthing conductor shall be in compliance with the appropriate rules for terminating bonding jumpers in Part K of Article 250 of the National Electrical Code, ANSI/NFPA 70 and Article 10 of Part 1 of the Canadian Electrical Code, Part 1, C22.1. Termination of the supplementary earthing conductor is permitted to be made to building steel, to a metal electrical raceway system, or to any earthed item that is permanently and reliably connected to the electrical service equipment earthed. 3. Bare, covered, or insulated earthing conductors are acceptable.
A covered or insulated conductor must have a continuous outer finish that is either green, or green with one or more yellow stripes.'
6. Safety Instructions - Rack Mount 'Rack Mount Instructions -
The following or similar rack-mount instructions are included with the installation instructions:
 - A) Elevated Operating Ambient - If installed in a closed or multi-unitrack assembly, the operating ambient temperature of the rack environment may be greater than room ambient. Therefore, consideration should be given to installing the equipment in an environment compatible with the maximum ambient temperature (T_{ma}) specified by the manufacturer.

- B) Reduced Air Flow - Installation of the equipment in a rack should be such that the amount of air flow required for safe operation of the equipment is not compromised.
- C) Mechanical Loading - Mounting of the equipment in the rack should be such that a hazardous condition is not achieved due to uneven mechanical loading.
- D) Circuit Overloading - Consideration should be given to the connection of the equipment to the supply circuit and the effect that overloading of the circuits might have on overcurrent protection and supply wiring. Appropriate consideration of equipment nameplate ratings should be used when addressing this concern.
- E) Reliable Earthing - Reliable earthing of rack-mounted equipment should be maintained. Particular attention should be given to supply connections other than direct connections to the branch circuit (e.g., use of power strips).'



INTRODUCTION

Purpose

This document provides the command usage of routing applications supported by the Ubigate iBG2006/2016/3026.

This manual is for engineers, technicians, and others involved with the planning and operation of the Ubigate iBG2006/2016/3026.

Document Content and Organization

This manual contains the following chapters:

PART I. System Configuration

CHAPTER 1. Basic Configuration

CHAPTER 2. Port Numbering

CHAPTER 3. Management Configuration

CHAPTER 4. System Logging

CHAPTER 5. RMON Configuration

CHAPTER 6. Image Update

CHAPTER 7. Hot Swap

PART II. WAN Interface and Protocols

CHAPTER 1. Serial Interfaces

CHAPTER 2. WAN Interfaces

CHAPTER 3. PPP, MLPPP, and HDLC

CHAPTER 4. FR and MFR

CHAPTER 5. PPPoFR and MLPPPoFR

PART III. Switching and Routing Protocols

CHAPTER 1. Layer-2 Switching

CHAPTER 2. DHCP Relay

CHAPTER 3. Static Routing

CHAPTER 4. RIP

CHAPTER 5. RIPng

CHAPTER 6. OSPF

CHAPTER 7. OSPFv3

CHAPTER 8. BGP

CHAPTER 9. BGP4+

CHAPTER 10. Multicast Protocols

CHAPTER 11. VRRP

CHAPTER 12. QoS

PART IV. Security

CHAPTER 1. Authentication Authorization Accounting

CHAPTER 2. Packet Filtering

CHAPTER 3. Firewall NAT

CHAPTER 4. GRE

CHAPTER 5. IPSEC

CHAPTER 6. SSL VPN Configuration

CHAPTER 7. Management

PART V. Voice

CHAPTER 1. Voice Feature

CHAPTER 2. VoIP Gateway Management

CHAPTER 3. SIP Gateway Management

CHAPTER 4. H.323 Gateway Management

CHAPTER 5. Analog Voice Port

CHAPTER 6. Digital Voice Port

CHAPTER 7. ISDN

CHAPTER 8. Routing and Digit Manipulation

CHAPTER 9. Extended VoIP Services

CHAPTER 10. Call Admission Control

CHAPTER 11. Management

CHAPTER 12. Survivable Telephony

CHAPTER 13. Integrated Communication Manager

CHAPTER 14. Case Study

Conventions

The following types of paragraphs contain special information that must be carefully read and thoroughly understood. Such information may or may not be enclosed in a rectangular box, separating it from the main text, but is always preceded by an icon and/or a bold title.



NOTE

Indicates additional information as a reference.

Console Screen Output

- The lined box with ‘**Courier New**’ font will be used to distinguish between the main content and console output screen text.
- ‘**Bold Courier New**’ font will indicate the value entered by the operator on the console screen.

Information for Product and Technical Support

For questions regarding the product and technical supports:

<http://www.samsungnetwork.com>

Revision History

EDITION	DATE OF ISSUE	REMARKS
00	09. 2007.	First edition
01	05. 2008.	Add ADSL configuration guide (Part II. Chapter 2 WAN Interfaces)
02	09. 2008.	Add VPN-SSL module configuration guide (Part IV. Chapter 6 SSL VPN Configuration)
03	02. 2010.	Add ICM configuration guide (Part V Chapter 13 Integrated Communication Manager)



This page is intentionally left blank.



TABLE OF CONTENTS

GENERAL USER INFORMATION

I

Radio Frequency Interference	I
FCC Requirements	I
Music on Hold Warning	V
DISA Warning	V
Safety Warning	VI
Underwriters Laboratories	VI

INTRODUCTION

IX

Purpose	IX
Document Content and Organization	IX
Conventions	XII
Console Screen Output	XII
Information for Product and Technical Support	XII
Revision History	XIII

PART I. System Configuration

1

CHAPTER 1. Basic Configuration

1

Logging in	1
Command-Line Interface Basics	4

CHAPTER 2. Port Numbering

9

Main Board Port Numbering	10
Network Modules Ports Numbering	11
Mini Modules Ports Numbering	12
Port Numbering Examples	13

CHAPTER 3. Management Configuration	15
Configuring Simple Network Management Protocol.....	15
SNMP Applications Supported.....	25
Configuring SNMP	25
Verifying SNMP configuration	29
CHAPTER 4. System Logging	33
Logging Commands.....	33
Syslog messages' severity.....	35
Syslog Configuration.....	36
Verifying Syslog Configuration	37
CHAPTER 5. RMON Configuration	39
Configuring Remote Monitoring	39
Configuring RMON.....	40
Verifying RMON Configuration.....	41
CHAPTER 6. Image Update	45
SNOS Update Procedure.....	45
Verify the Amount of Free Space.....	46
Verify that the FTP/TFTP Server Connectivity	48
Copy the New Image into the Compact Flash.....	49
Verify SNOS image's validation	50
Setting Boot Parameter for the New Image	52
Verify the Upgraded Image Version	54
CHAPTER 7. Hot Swap	55
Hot-Removal of a Module Procedure.....	55
Hot-Insertion of a Module Procedure	58

PART II. WAN Interface and Protocols 1

CHAPTER 1. Serial Interfaces 1

Serial Interfaces Overview.....	1
Multi-Protocol Serial Interface.....	1
HSSI Interface	3
Module Configuration.....	5
Configuring V.35	5
Bundle Configuration	7
Configuring HSSI	11

CHAPTER 2. WAN Interfaces 15

Module Configuration.....	15
Configuring T1 and E1.....	15
Configuring CT3	18
Configuring CT3 bundle.....	22
Configuring ADSL	23

CHAPTER 3. PPP, MLPPP, and HDLC 31

Protocol Configuration.....	33
PPP Configuration	34
MLPPP Configuration	35
HDLC Configuration.....	36
ISDN	46

CHAPTER 4. FR and MFR 57

Layer Two Configurations	57

CHAPTER 5. PPPoFR and MLPPPoFR 73

Protocol Configuration	75
PPPoFR Configuration	75
MLPPPoFR Configuration	77

PART III. Switching and Routing Protocols 1**CHAPTER 1. Layer-2 Switching 1**

Layer 2 LAN Switching and Bridging.....	1
VLAN (Virtual LAN)	3
IGMP Snooping.....	3
Layer2 Features Configuration.....	4
MSTP and VLAN Configurations.....	4
Configuring 802.1x.....	16
LACP Configuration	20
Configuring IGMP Snooping	24

CHAPTER 2. DHCP Relay 29**CHAPTER 3. Static Routing 33**

Configuring Static Routes	33

CHAPTER 4. RIP 35

RIP Protocol Features.....	35
Configuring RIP.....	38
Specifying the RIP version	40
Configuring RIPv2 authentication.....	42
Configuring RIP Split Horizon.....	45
Configuring RIP on a bundle interface	47
Verifying and Troubleshooting Commands	48

CHAPTER 5. RIPng 51

RIPng Protocol Features.....	52
Configuring RIPng.....	52
Configuring RIPng Split Horizon.....	54
Verifying and Troubleshooting Commands	56

CHAPTER 6. OSPF	59
OSPF Protocol Features.....	60
System Basic Configuration.....	61
Configuring OSPF Router.....	65
Configuring OSPF Interface.....	69
Verifying and Troubleshooting Commands	74
CHAPTER 7. OSPFv3	79
OSPFv3 Protocol Features.....	79
System Basic Configuration.....	80
Configuring OSPFv3 Area	83
Configuring OSPFv3 Interface.....	86
Verifying and Troubleshooting Commands	88
CHAPTER 8. BGP	93
Protocol Features	95
Minimum BGP Configuration	97
BGP Application using Route-Map.....	100
CHAPTER 9. BGP4+	105
Minimum BGP Configuration	106
BGP Application using Route-Map.....	109
CHAPTER 10. Multicast Protocols	113
Protocol Independent Multicast (PIM).....	113
Distance Vector Multicast Routing Protocol (DVMRP).....	125
Internet Group Management Protocol (IGMP)	130
Verifying and Troubleshooting Commands	134
CHAPTER 11. VRRP	137
Configuring VRRP	138

CHAPTER 12. QoS	141
Quality of Service	141
Features.....	142
Definitions.....	144
Classification Types	145
Configuration.....	146
Create Bundle AppTest	146
Create Traffic Classes.....	146
VLAN Identifiers.....	148
Configuration.....	149
Create bundle VLANtest	149
Create Traffic Classes and Assign Classifications	149
Historical Statistics	150
Configuring Historical Statistics.....	150
Traffic Policing versus Traffic Shaping	151
Need for Traffic Policing.....	151
Traffic Policing Functionality	152
Configuring Traffic Policing	152
Verifying Policing Status and Configuration	153
Limitations.....	154
Multi-Field Classification	155
Packet Marking	156
Configuring MF Classification	156
Traffic Policing.....	160
Policing Using Single Rate Three Color Marking (srTCM)	161
Configuring srTCM.....	163
The trTCM (Two Rate Three Color Marker).....	164
Configuring trTCM.....	166
Statistics.....	166
Egress Queuing, Shaping and Scheduling	167
CBQ Scheduler Operation	167
Buffer Management for Class Queues.....	170
Output Queue Congestion Management.....	171
Buffer Reservation for Interfaces	172

Buffer Management for Class Queues.....	173
Congestion Management on Output Queues	177
Drop Probability Calculation	179
Configuring RED parameters.....	180
Differentiated Services	183
Assured Forwarding (AF), Expedited Forwarding (EF), and Class Selector Code Points (CSCP).....	183
QoS Statistics	184
Ingress and egress FR-QoS on FR PVCs.....	184
Ingress and egress QoS for IP tunnels	185
Hardware QoS	185
CoS Attributes Marking	185
L2 Bridge Based CoS Marking.....	186
Configuration Example	187
Verifying the Configuration.....	187
InLIF Based CoS Marking	188
Configuration Example	188
Verifying the Configuration.....	188
Policy Based CoS Marking	189
Configuration Example	190
Verifying the Configuration.....	190
Policing-based CoS Marking, CoS Re-marking, and L2-based CoS Re-marking	191
Configuration Example	192
Verifying the Configuration.....	192
Multi-Field Classification using PCLs	193
Configuration Example	194
Verifying the Configuration.....	194
Traffic Policing	195
Configuration Example	196
Verifying the Configuration.....	196
Billing & Conformance Counters	197
Configuration Example	197
Verifying the Configuration.....	198
Egress Queuing, Scheduling and Shaping	199
Verifying the Configuration.....	199

TABLE OF CONTENTS

Congestion Management on Egress Queues.....	200
Verifying the Configuration	200
Buffer Management	201
Verifying the Configuration	201

PART IV. Security	1

CHAPTER 1. Authentication Authorization Accounting	1

Configuration Examples	2

CHAPTER 2. Packet Filtering	7

Example: Blocking Telnet Access.....	8
Step-by-Step Configuration	8

CHAPTER 3. Firewall NAT	9

Overview	9
Virtual Firewall	10
Access Policy Database.....	12
Application Level Gateways	14
Network Address Translation	14
Application Content Filtering	15
Configuring Firewalls.....	17
NAT configuration Examples	19
Dynamic NAT (many to many)	19
Port Address Translation (Many to one).....	20
Static NAT (one to one)	22
Reverse NAT	25
NAT-Failover for Firewalls	26

CHAPTER 4. GRE	27

GRE Configuration Examples	28
Configuring Site to Site Tunnel.....	28
Configuring GRE Site to Site with IPSec.....	30
Configuring GRE Site to Site with IPSec and OSPF.....	32

CHAPTER 5. IPSEC

33

Introduction to Security	33
Securing Remote Access Using IPsec VPN	33
Access Methods	34
Securely Managing the Ubigate iBG Router Example	36
Joining Two Private Networks Example	52
Joining Two Networks using Multiple IPsec Proposals Example	70
Supporting Remote User Access Example	83
Configuring IPsec Remote Access Example	92

CHAPTER 6. SSL VPN Configuration

103

Overview	103
Deployment	103
SSL VPN Modes	104
Clientless mode	104
Port Forwarding mode	104
Tunnel Mode	105
Configuring SSL VPN Gateway	106
Configuring Trustpoint	109
Configuring SSL VPN EPS policy	114
Configuring SSL VPN Portal	117
Configuring SSL VPN Resource	124
Configuring SSL VPN Domain	126
Configuring Groups within SSL VPN Domain	129
Configuring Group Policies	131
Configuring SSL VPN Users within a Group	133
Configuring SSL VPN Group Bookmark	135
Configuring User Policies	137
Configuring User Login Policies	140
Configuring SSL VPN User Bookmark	142
Configuring SSL VPN Clientless mode	144
Configuring SSL VPN Tunnel mode	149
Configuring SSL VPN Port Forwarding mode	151
Configuring SSL VPN Global Bookmark	153

CHAPTER 7. Management 155

Statistics	155
Debug Management	161

PART V. Voice 1

CHAPTER 1. Voice Feature 1

Introduction of Voice Feature	1
Network Architecture	1
Interface Between Network Entities	4
Operation Mode	5
Key Functions	8
Voice Deployment Scenario	23

CHAPTER 2. VoIP Gateway Management 26

Introduction to VoIP Gateway Features	26
Configuring VoIP Gateway	27

CHAPTER 3. SIP Gateway Management 35

Introduction to SIP Gateway Features	35
Configuring Basic SIP Gateway	54
Configuring Enhanced SIP Gateway Features	65
Configuring SIP Security Features	88
Verifying and Troubleshooting SIP Features	95

CHAPTER 4. H.323 Gateway Management 101

Introduction to H.323 Gateway Features	101
Configuring a H.323 Gateway	114
Verifying and Troubleshooting H.323 Features	143

CHAPTER 5. Analog Voice Port 147

Introduction to Analog Voice Port Features	147

Analog Voice Port Monitoring	155
Configuring Analog FXS Voice Port	158
Configuring Analog FXO Voice Port.....	164
Configuring Analog E & M Voice Port	169
Configuring Analog DID	176
Configuring E911 CAMA.....	179

CHAPTER 6. Digital Voice Port 187

Digital Trunk E1-R2 Features	187
Digital Trunk T1-CAS Features.....	209

CHAPTER 7. ISDN 235

Overview.....	235
Configuring ISDN BRI.....	238
Configuring ISDN PRI.....	257

CHAPTER 8. Routing and Digit Manipulation 273

Dial Peer Management.....	273
Dial Plan Mode	299
Dialed Number Analysis.....	300
Digit Manipulation	301
Access Group Management	311
Trunk Group Management.....	314
PLAR	317
COR.....	321

CHAPTER 9. Extended VoIP Services 325

Fax Relay with VoIP.....	325
Supplementary Services for Call Manager Interworking Mode	330
Supplementary services for Survivable Telephony Mode	342
Supplementary Services for Stand Alone Mode.....	344

CHAPTER 10. Call Admission Control 351

Local CAC	351
Resource-based CAC.....	362

TABLE OF CONTENTS

Call-admission Spike.....	365
Call admission Treatment	366

CHAPTER 11. Management	367

Alarm	367
Statistics.....	370
Debug Management	381
CDR Management	384

CHAPTER 12. Survivable Telephony	389

Configuring Call Forward for Survivable Telephony	389
Configuring System Message for Survivable Telephony	392
Configuring COR List for Survivable Telephony	394
Configuring Translation for Survivable Telephony	396

CHAPTER 13. Integrated Communication Manager	401

Introduction to Integrated Communication Manager Features	401
Configuring Integrated Communication Manager	406
Enable Integrated Communication Manager Features.....	406
Configuring Voice Stations	406
Configure Automatic Callback service	414
Enable automatic callback Features	415
configure Idle guard timer	415
configure maximum originator session number.....	416
configure maximum terminator session number	416
configure maximum ringing time	417
configure monitor minutes.....	417
Show Automatic Callback session information.....	418
Configuring Number-Plan	418
Hunt Group service	420
Station Group service.....	426
Configuring Time-based Service.....	431
Configuring Time and Holiday schedules.....	431
Configuring Time-based service.....	433
Configuring Phone Provisioning Service.....	435

Prerequisites.....	435
Configuring Server (TFTP, DHCP).....	435
Generation of global provisioning file.....	436
Generation of specific provisioning files.....	436
Connect or reboot the phone.....	438
Configure Shared-Group Services	439
Prerequisites.....	439
Service Scenarios.....	439
Shared-group configuration	441
Service Assignments	442
Shared-service configuration.....	443
Phone-profile configuration.....	443
Verification of configuration.....	444
Configure Intercom Services	447
Enable Intercom Features	447
Verification of configuration.....	449
Configure Hold call pickup Services	450
Enable Hold call pickup Features	450
Verification of configuration.....	451
Configure Multi-ring Services	452
Enable Multi-ring Features.....	452
Verification of configuration.....	453
Configure Transfer Recall Services.....	454
Enable Transfer Recall Features	454
Configure Call Override Services	455
Enable Call Override Features	455
Configure Group Call (Dispatch, Paging) Services	456
group-call group configuration	456
Verification of configuration.....	457
Configure Barge-In Services	458
Enable Barge-In Features.....	458
Enable Barge-in warning tone Features	459
Configure Ring-Group Services.....	460
Ring-group configuration	460
Verification of configuration.....	460
Configure Convert COR Services	461
Enable Convert COR Features.....	461

Configure Mixer Warning Tone Services	462
Enable Mixer Warning Tone Features	462
Verification of configuration	462
Configure Call Forwarding Unreachable Services	463
Enable Call Forwarding Unreachable Features	463
Configure Call Forwarding DND Services	464
Enable Call Forwarding DND Features	464
Configure Call Forwarding VMS Services	465
Enable Call Forwarding VMS Features	465
Configure Huntgroup logout Services.....	466
Enable Huntgroup logout Features	466
Configuring Media Connection Point (MCP)	468
Prerequisites	468
How to enable Allow-interfaces on VoIP Gateway	469
How to configure MCP	470
Verification of configuration	472
Configuring Basic Automatic Call Distributor (B-ACD).....	474
Overview	474
How to Configure B-ACD	475
Configure Call Queue	478
Verification of configuration	479
Audio Prompts Files	479
Configuring Personal Web Pages Service	483
Prerequisites	483
Configuring Server(HTTP, HTTPS).....	483
Confirm whether relevant files exist for pwp service	483
Connect to personal web page	484
Configure personal phone book	485
Exit from Personal web page	486
Configuring Voice Mail (Internal Voice Mail)	487
Prerequisites	487
How to update IVM packages	487
How to reset IVM	488
How to configure voice-mail entity	488
How to configure voice station to use voice-mail	489
Verification of configuration	490
Auto Configuration	490

Quick Setup	491
System Administration	491
Configuration Tools	492
Web Management	492
DTMF System Administration	494
Voice Mail CLI.....	496
Configuration Categories	499
Ubigate IVM Directory Structure	499
The TABLE Files (*.TBL).....	499
PMT Directories (Prompts)	500
MSG Directory (Messages)	500
MBX Directory (Mailboxes)	500
TEMP Directory	500
Defaulting the Configuration	501
Select Package Update	501
Select the file to update	502
Upload the package.....	502
Configurable Feature Codes	503
Changed default value of Feature codes	503
Toggled feature code Example	505

CHAPTER 14. Case Study	507

Toll-by-pass Configuration Examples.....	507
iPX Interworking Configuration Examples.....	514
SIP Server Interworking Configuration Examples.....	520
SIPconnect Interworking Configuration Examples.....	524
Gatekeeper Interworking Configuration Examples	530
ICM Configuration Example.....	533

LIST OF FIGURES

PART I

Figure 2.1	LAN Port Numbering	10
Figure 2.2	20-port Network Module Port Numbering	11
Figure 2.3	1-Port WAN Network Module Port Numbering	11
Figure 2.4	4-Port WAN Network Module Port Numbering	11
Figure 2.5	Voice Carrier and Mini Module Ports Numbering.....	12
Figure 2.6	1-Port Mini Module Port Numbering	12
Figure 2.7	2-Port Mini Module Port Numbering	12
Figure 2.8	4-Port Mini Module Port Numbering	12

PART II

Figure 2.1	ADSL interface card configuration example	24
Figure 2.2	ADSL deployment scenario	25
Figure 2.3	ADSL deployment scenario	27
Figure 3.1	Overview of PPP	31
Figure 3.2	ISDN BRI connection with ISDN switches.....	46
Figure 3.3	ISDN PRI connection with ISDN switches.....	47
Figure 3.4	Common ISDN message Flow	52
Figure 4.1	Multilink Frame Relay with Three Sites	57
Figure 4.2	Multilink Frame Relay with Three Site Details	58
Figure 5.1	Overview of PPPoFR	74
Figure 5.2	MLPPPoFR deployment scenario	75

PART III

Figure 1.1	VLANs Example	5
Figure 1.2	VLANs Example with multiple instances of MSTP.....	9
Figure 1.3	Configuring 802.1x Security	16
Figure 1.4	Link Aggregation Example.....	20
Figure 1.5	IGMP Snooping Example	24
Figure 2.1	DHCP relay overview	29
Figure 2.2	BOOTP Requests.....	30
Figure 2.3	BOOTP Replies.....	30

Figure 2.4	Typical Scenario for DHCP Relay with NAT	31
Figure 7.1	DVMRP Network.....	127
Figure 11.1	Configuring a VRRP Network.....	138
Figure 12.1	Assigning Classification Types.....	145
Figure 12.2	Assigning VLAN Identifiers.....	148
Figure 12.3	Screen Display for show QoS bulkstats_config Command	150
Figure 12.4	MF Classification.....	156
Figure 12.5	Single Rate Three Color Marking	162
Figure 12.6	Two Rate Three Color Marking	165

PART IV

Figure 3.1	Virtual Firewall	11
Figure 3.2	Three Legged Firewall Network	12
Figure 3.3	Access policy database lookup	13
Figure 3.4	Dynamic NAT	19
Figure 3.5	Mapping Multiple NAT Addresses to One Public IP Address.....	20
Figure 3.6	Static NAT	22
Figure 3.7	Dynamic and Static NAT	23
Figure 3.8	Mapping Ports.....	24
Figure 3.9	Reverse NAT.....	25
Figure 3.10	NAT-Failover for Firewalls.....	26
Figure 4.1	Simple GRE configuration.....	28
Figure 5.1	Tunnel Mode Between Two Security Gateways-Single Proposal	36
Figure 5.2	Tunnel Mode Between Two Security Gateways-Single Proposals	52
Figure 5.3	Tunnel Mode Between Two Security Gateways-Multiple Proposals.....	70

PART V

Figure 1.1	Ubigate iBG Network Diagram.....	2
Figure 1.2	Example of Call Manager Interworking Mode Network Configuration	6
Figure 1.3	Example of Stand-alone mode network configuration	7
Figure 1.4	Toll Bypass for Voice and Fax services.....	23
Figure 1.5	Connection to IP Phone, Analog Phone and FAX	24
Figure 1.6	Management using CLI/GUI/NMS.....	25

TABLE OF CONTENTS

Figure 2.1	Architecture of VoIP Network.....	26
Figure 3.1	Architecture of SIP Network	36
Figure 3.2	SIP Request Through a Proxy Server	39
Figure 3.3	SIP Response Through a Proxy server	40
Figure 3.4	SIP Session Through a Proxy Server	40
Figure 3.5	SIP Session Through a Redirect Server.....	41
Figure 3.6	SIP Request Through a Redirect Server	42
Figure 3.7	SIP Gateway-to-SIP Gateway-Call Setup and Disconnect.....	43
Figure 3.8	SIP Gateway-to-SIP Gateway-Call Via SIP Redirect Server	46
Figure 3.9	SIP Gateway-to-SIP Gateway-Call via SIP Proxy Server with Record Route Enabled	49
Figure 4.1	Call Setup from a known H.323 Endpoint.....	102
Figure 4.2	Call Setup from a unknown H.323 Endpoint, no Gatekeepers	103
Figure 4.3	Call Setup from a unknown H.323 Endpoint, with Gatekeeper.....	103
Figure 4.4	Call Setup from Gatekeeper	104
Figure 4.5	Call Setup to a known H.323 Endpoint.....	105
Figure 4.6	Call Setup to a Gatekeeper	106
Figure 4.7	RAS Registration Procedure	108
Figure 5.1	Loop Start Signaling	148
Figure 5.2	Ground-start signaling for Analog FXS (Idle-state)	149
Figure 5.3	Ground-start signaling for Analog FXS (seizure-state)	150
Figure 5.4	Immediate method signaling sequence	151
Figure 5.5	wink method signaling sequence.....	152
Figure 5.6	delay method signaling sequence	153
Figure 5.7	E & M 2-Wire, 4-Wire loop Cable Pin Map	170
Figure 5.8	E & M Jumper Information.....	171
Figure 5.9	E911 Network Diagram	180
Figure 6.1	an E1 frame.....	187
Figure 6.2	E1 timeslots for R2 signaling.....	188
Figure 6.3	E1-R2 Network Diagram	189
Figure 6.4	Conceptual view of voice port	193
Figure 6.5	DS0 groups on a digital voice port.....	193
Figure 6.6	Echo problem	203
Figure 6.7	T1 frame and T1 timeslots for CAS signaling	209
Figure 6.8	T1 CAS signaling network.....	210

Figure 6.9	T1 CAS FXS/FXO signaling operation	224
Figure 6.10	Wink-start method signaling sequence	230
Figure 6.11	Immediate-start method signaling sequence.....	230
Figure 6.12	Delay-dial method signaling sequence	231
Figure 7.1	ISDN Call Flow.....	237
Figure 8.1	Dial Peer Call Legs	273
Figure 8.2	Call Legs from the Perspective of the Originating Router	274
Figure 8.3	Call Legs from the Perspective of the Terminating Router	275
Figure 8.4	Matching Call Legs to Dial Peers	278
Figure 8.5	Dial Peers from the Perspective of the Originating Ubigate iBG router..	279
Figure 8.6	Dial Peers from the Perspective of the Terminating Ubigate iBG router.	279
Figure 8.7	Communication Between Dial Peers Sharing the Same Ubigate iBG router	280
Figure 8.8	Relationship Between Destination Pattern and Session Target	294
Figure 8.9	VoIP Example for Number Expansion	303
Figure 8.10	Example of PLAR configuration	317
Figure 8.11	Example of PLAR-OPX configuration.....	319
Figure 10.1	DS0 Limitation.....	353
Figure 10.2	max call per dialpeer	354
Figure 10.3	Call-admission spike window size	365
Figure 13.1	Relation of voice station 1000 and pots dial-peer	407
Figure 13.2	Relation of voice station 2000 and voip dial-peer.....	407
Figure 13.3	Device configuration example for shared-service	439
Figure 13.4	MCP Network Diagrams.....	468
Figure 13.5	General architecture of IVM	487

LIST OF TABLES**PART IV**

Table 6.1	Firewall Statistics command.....	155
Table 6.2	IPSec Statistics command	159
Table 6.3	IPSec Statistics Item - Inbound IPSec Packet Errors	159
Table 6.4	IPSec Statistics Item - Outbound IPSec Packet Errors	160
Table 6.5	Firewall Debug	161
Table 6.6	IPSec Debug.....	163

PART V

Table 1.1	High Availability Cases.....	20
Table 3.1	Call Setup and Disconnect.....	44
Table 3.2	Call via Redirect Server	47
Table 3.3	Call via Proxy Server	50
Table 3.4	Table Default PSTN cause code to SIP status code mapping.....	65
Table 3.5	Default SIP Event to PSTN cause code mapping	67
Table 4.1	Standards.....	101
Table 4.2	RAS Registration Trial.....	107
Table 4.3	RAS UnRegistration Trial.....	107
Table 4.4	Supported Supplementary Services in H.323 Gateway	111
Table 4.5	H.323 Call Statistics Command.....	112
Table 4.6	H.323 Call Tracing & Debug Command	113
Table 4.7	combination to enable or shutdown H.323 Service.....	120
Table 4.8	commands of 'voice service h323' configuration and 'voice class h323' configuration.....	138
Table 5.1	E & M Wiring and Signaling Methods.....	154
Table 7.1	switch-type parameter description (BRI).....	239
Table 7.2	switch-type parameter description (PRI).....	258
Table 8.1	Wild card Symbol.....	293
Table 8.2	Number Expansion Commands	304
Table 8.3	Characters of Translation Rule	307

Table 9.1	Supplementary services for Call Manager Interworking mode.....	330
Table 9.2	Supplementary services for Survivable telephony mode	342
Table 9.3	Supplementary services for Stand Alone mode	344
Table 10.1	Bandwidth per Codec	355
Table 11.1	Alarm List.....	367
Table 11.2	Fault List	369
Table 11.3	Call Statistics command.....	370
Table 11.4	Call Statistics Item.....	370
Table 11.5	SIP protocol Statistics command.....	372
Table 11.6	SIP protocol Statistics command.....	372
Table 11.7	Call Statistics command.....	376
Table 11.8	H.225.0 CS Statistics command	376
Table 11.9	H.225.0 RAS Statistics command	377
Table 11.10	H.245Statistics command	379
Table 11.11	Voice Call Control Debug	381
Table 11.12	Voice Protocol Module Debug.....	382
Table 11.13	H323 Debug.....	382
Table 11.14	SIP Debug	383
Table 11.15	Voice Debug	383
Table 11.16	Voice Call log Debug.....	383
Table 11.17	Attribute List.....	385
Table 11.18	Vendor Specific Attribute List	387



This page is intentionally left blank.

PART I. System Configuration



- CHAPTER 1. Basic Configuration**
- CHAPTER 2. Port Numbering**
- CHAPTER 3. Management Configuration**
- CHAPTER 4. System Logging**
- CHAPTER 5. RMON Configuration**
- CHAPTER 6. Image Update**
- CHAPTER 7. Hot Swap**



CHAPTER 1. Basic Configuration

This chapter describes the initial configuration steps and command-line interface (CLI) basics.

Logging in

After the Ubigate iBG router being powered-on, the login sequence should be executed as follows:

```
login: samsung
password: samsung

samsung logged in on Fri May 7 05:28:01 2004 from console

Router#
```

Changing Login Parameters

The System Administrator login consists of two components: the account name and the password. The initial login name is always **samsung**, but you can change this to suit the needs of your facility after logging in. The default administrative password, **samsung**, should be changed as soon as possible to ensure only authorized access to the system. For more information about the command usage, see the iBG Router Command Reference Guide. This guide is available on the Samsung website: <http://www.samsungnetwork.com/>

Changing Password

This procedure enables the system administrator or any user to change their password on an iBG router.

Step	Command	Description
1	Router# password	The command for changing password
2	Type the current user name, and then press Return	The system prompts for the current username to authenticate.
3	Type the current password, and then press Return	The system prompts for the current password.
4	Type your new password, and then press Return	The system prompts for the new password.
5	Type the new password again, and then press Return	The system prompts you to verify the new password.

Changing Administrator Account

This procedure changes the system administrator login name to a user-specific name. Note that the default is **samsung**.

Step	Command	Description
1	Router# configure terminal	Accesses the configure mode
2	Router/configure# admin_name [new_account]	Changes the account name

After the change, the system displays a confirmation message.

Administrator account name changed to [new_account]

Setting Date and Time

There are three commands in 'configure' mode to support date and time setting. To set the current time for the router in Universal Time Coordinated time, specify the time zone offset ahead (+) or behind (-) the time in Greenwich (England), the number of hours ahead or behind Greenwich time, and the number of minutes ahead or behind the time in Greenwich.

Step	Command	Description
1	Router/configure# utc+/-utc hour min	Sets UTC time for current region
2	Router/configure# date month day year	sets the current date
3	Router/configure# time hour min second	sets the current time

User Account

The system administrator can add up to 15 users and assign privileges from level 2 to level 4. The system administrator has the privilege level 1 and only can add, modify, remove the user information.

- Adding a new user

Step	Command	Description
1	Router# configure terminal	Enters the terminal configuration mode
2	Router/configure# user [name] level [number]	Name: 3 to 39 characters Number: 2 to 4
3	Enter Password twice	-

- Removing a user

Step	Command	Description
1	Router# configure terminal	Enters the terminal configuration mode
2	Router/configure# no user [name]	Deletes a user of '[name]'

To view the user information, enter the 'show user_accounts' command.

Command-Line Interface Basics

The Command Line Interface (CLI) is a text-based facility similar to industry standards. Many of the commands may be used in scripts to automate many configuration tasks. Each command CLI is usually associated with a specific function or a common function performing a specific task. Not only a single user issue commands through console interface but also multiple users can telnet and issue commands. However, only one user is allowed to use the Configure mode at a time, to avoid multiple users from issuing configuration commands simultaneously.

The CLI gives users and administrators the ability to issue commands to several daemons from a single telnet session.

Command Line Help

The CLI contains a text-based help facility. Access this help by typing in the full or partial command string then typing '?'. The CLI displays the command keywords or parameters plus a short description. For example, at the CLI command prompt, type show ? (the CLI does not display the question mark). The CLI displays this keyword list with short descriptions for each keyword:

```
Router# show ?

aaa                To access AAA display commands
access-list        List IP access lists
access-lists       display packet filter rule lists
                   for interfaces
access-lists-rules display packet filter rule lists
                   for layer2 interface
arp                display current arp information
arp_timeout        show arp timeout in seconds
aux                Display Aux port status
boot_params        Display boot parameters
bridge             Display forwarding information

...

user_accounts      display all users
users              display only active users
version            Display system versions
virtual-access     access virtual access display
                   commands
vlan               Display VLAN information
vrrp               display vrrp related information
whoami             current user
```

Syntax Help

The CLI can complete the spelling of command or parameter keywords. Begin typing the command or parameter then press TAB. At the CLI command prompt type sh:

```
Router# sh
```

Press TAB. The CLI shows:

```
Router# show
```

If the command or parameter partial spelling is ambiguous, the CLI displays the choices that match the abbreviation. Type 'show i'. Press TAB. The CLI shows:

```
Router# show interface
```

The interface displays 'show interface' and Type TAB once again then it displays another parameter 'show ip'. Any available parameters can be fetched by typing TAB.

Type and the CLI shows the list of parameters for the show interface command.

```
Router# show interface ?

    avc          display information about an
                  DTE-to-DTE MFR avc
    Bundle       display information about a bundle
    Bundles      display all the names of bundles
                  Configured in the system
    Ethernet     display an ethernet interface
    Ethernets    display all ethernet interfaces
    l2tp-server  display l2tp-server interface(s)
    loopback     display loopback interface(s)
    switchport   Display the modes of the Layer2 interfaces
    tunnel       display a tunnel interface
    tunnels      display all tunnel interfaces
    virtual-access display virtual access interface(s)
```

This command has but one positional parameter, an interface name. Supply a value for the parameter.

Command line errors

If the router does not recognize the command after ENTER is pressed, it displays this message:

```
Router# command-unknown
      ^
Error : Command 'command-unknown' does not exist
```

Some commands are too long for the display line and can wrap in mid-parameter or mid-keyword if necessary:

```
area 10.10.0.18 virtual-link 10.10.0.19 authentication-key
57393
```

Configuration File Operation

By using the configure flash command, you can set the Router system parameters from a configuration file stored in the flash memory. This method is useful if the system configuration differs from the configuration file in flash memory and you want to restore the flash configuration. It is recommended that all configuration files have a .CFG extension.

At the main CLI prompt, type configure flash and press ENTER. Then, type the desired configuration file name (with a .cfg extension) and press ENTER, as shown in the example below.

```
Router# configure flash
filename(path): test.cfg
```

The system configuration can be saved in a file as shown in the following example.

```
Router# save local
```

If you don't give a file name after '*local*', it is saved in the default filename, '*system.cfg*'.

You also can set the Router system parameters from a configuration file on a network server. This method downloads files via the TFTP protocol, then executes the commands from that file without operator intervention. It is recommended to use the *configure network* command if you want to configure one or more Router systems with the same configuration. An example is shown below

```
Router# configure network
      host : testhost
      type(t:tftp, s:scp) : t
      fileName : test.cfg
```

shown below

To save current configuration in a file on a remote server, use the '*save network*' command as in the following example.

```
Router# save network 192.168.0.2 test.cfg
```



This page is intentionally left blank.



CHAPTER 2. Port Numbering

This section describes the port number conventions used by Ubigate routers such as iBG3026, iBG2016, iBG2006, and iBG1000.

Ports on a network module are numbered in a format: *network module slot-number/interface-number*, and ports on a mini-module are numbered in a format: *network module slot-number/mini-module slot number/interface-number*.

Network modules are numbered from right to left, starting with slot number one. If there is more than one row, the bottom row is numbered first, from right to left, starting at slot one, then the next row up is numbered, from right to left, starting with the next slot number based on the lower rows last (left most) numbered slot. The main board is considered as network module slot 0.

Mini modules are numbered from right to left, starting with slot number zero. If there is more than one row, the bottom row is numbered first, from right to left, starting at slot zero, then the next row up is numbered, from right to left, starting with the next slot number based on the lower rows last (left most) numbered slot.

Ports on any mini module or network module are numbered from right to left, starting with port number zero. If there is more than one row of ports on a given module, the bottom row is numbered first, from right to left, starting at port zero, then the next row up is numbered, from right to left, starting with the next port number based on the lower rows last (left most) numbered port.

Main Board Port Numbering

In this Chapter we describe the port number conventions used on the iBG2016. For other models, refer to the corresponding System Description Manual. Ethernet SFP port and four Fast Ethernet UTP ports. They are numbered 0/x *since the main board is considered as network module slot 0*. The SFP port is numbered as 0/0. Then, the Fast Ethernet ports follow the numbering rule and are numbered right to left bottom to top starting with one.

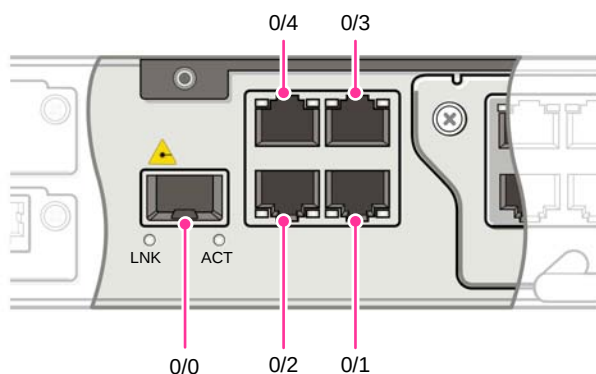


Figure 2.1 LAN Port Numbering

Network Modules Ports Numbering

The network module always resides in the slot #1. The 20-port LAN network module numbering is as follows:

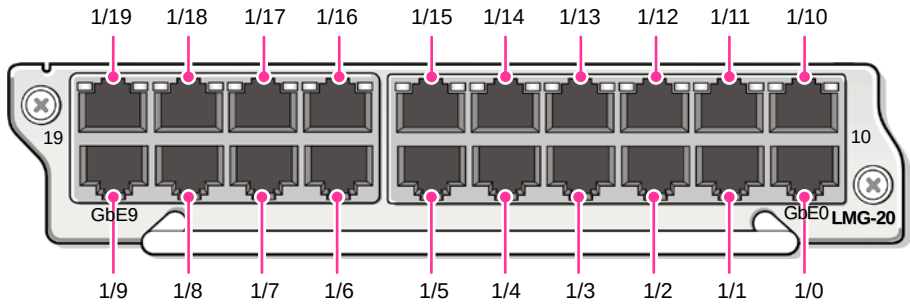


Figure 2.2 20-port Network Module Port Numbering

WAN network modules come in one port or four port configurations. The port numbering is also from right to left starting at port number zero:

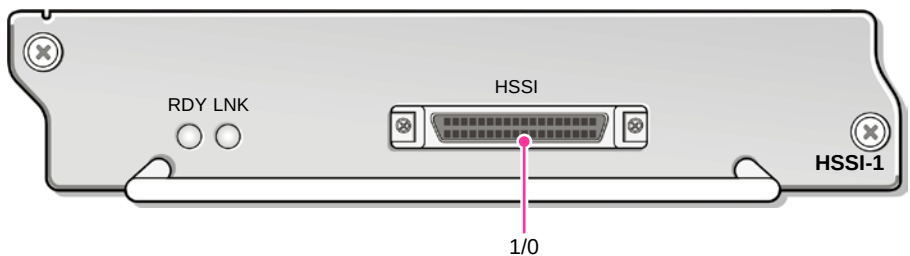


Figure 2.3 1-Port WAN Network Module Port Numbering

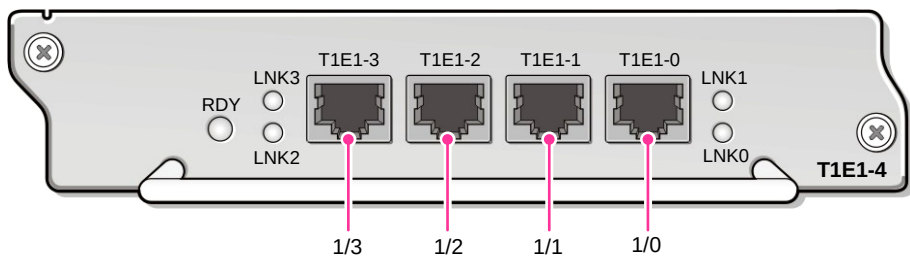


Figure 2.4 4-Port WAN Network Module Port Numbering

Voice carrier Modules can have voice-only mini-modules plugged into them. Here is an example of a voice carrier module in slot 2 with a 4-port mini-module in sub-slot 0, and a 2-port mini-module in sub-slot 1: (X=1 or 2)

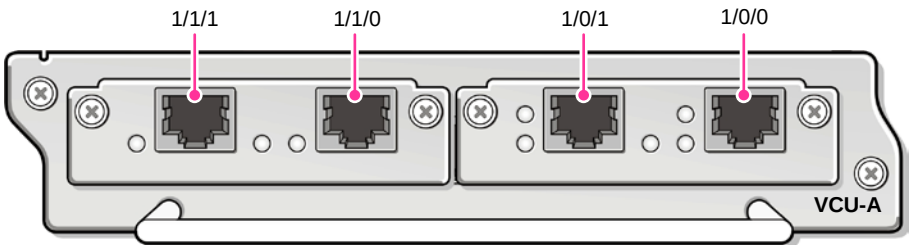


Figure 2.5 Voice Carrier and Mini Module Ports Numbering

Mini Modules Ports Numbering

Mini-modules have one, two or four ports. Port numbering is from right to left starting with port number zero: (X=0, 1, 2, or 3)

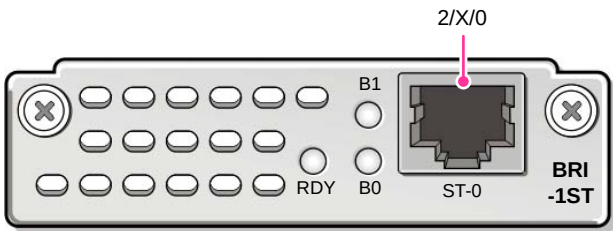


Figure 2.6 1-Port Mini Module Port Numbering

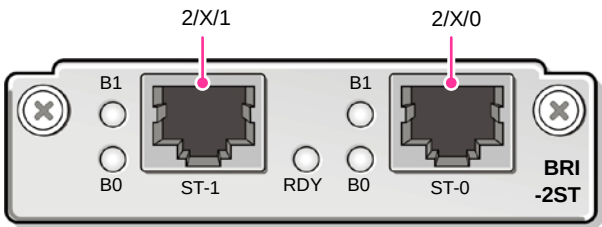


Figure 2.7 2-Port Mini Module Port Numbering

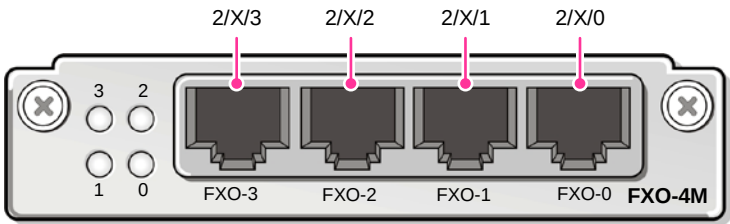


Figure 2.8 4-Port Mini Module Port Numbering

Port Numbering Examples

Port	Numbering	Corresponding Ports
Main board LAN Ports	0/1, 0/2, 0/3 and 0/4	Copper Gigabit Ethernet ports.
	0/5	Optical Gigabit Ethernet port
Mini Module Ports	0/0/0	Port zero on a mini-module in sub-slot zero.
	0/2/3	Port three on a mini-module in sub-slot two in main board in slot zero.
LAN Network Module Port	1/0 thru 1/19	The lower row of Ethernet ports numbered from right to left on the 20-port LAN network module in the network module slot.
WAN Network Module Port	1/0	Right most port on the WAN network module in the network module slot.
	1/3	Left most port of four ports on the WAN network module in the network module slot.
Voice Carrier Module (VCU-A) Port	1/0/0	Right most port on the voice mini-module in the right hand sub-slot in the voice carrier module plugged into the network module slot.
	1/1/3	Left most port on a four port voice mini-module in the left hand sub-slot in the voice carrier module plugged into the network module slot.



This page is intentionally left blank.



CHAPTER 3. Management Configuration

Lets us consider the following Services, Groups and Agents.

Configuring Simple Network Management Protocol

Ubigate iBG router provides two classes of SNMP Management Information Bases (MIBs) to provide you with the ability to manage Ubigate iBG routers. The two MIBs are the Enterprise MIB and the Standard MIB.

Enterprise MIBs

The Enterprise MIBs should be compiled in the following order:

1. SUBMARINE-SMI
2. SUBMARINE-SNMP-MIB.mib
3. SUBMARINE-SYSTEM-MIB.mib
4. SUBMARINE-BUNDLE-MIB.mib
5. SUBMARINE-PPP-MIB.mib
6. SUBMARINE-FR-MIB.mib
7. SUBMARINE-CONFIG-MIB.mib
8. SUBMARINE-DSX-TC.mib
9. SUBMARINE-DSX-TE1-MIB.mib
10. SUBMARINE-DSX-TE3-MIB.mib
11. SUBMARINE-CHASSIS-MIB .mib
12. SUBMARINE-ENVIRON-MIB .mib
13. SUBMARINE-GHDLC-MIB.mib
14. SUBMARINE-IP-MIB.mib
15. SUBMARINE-CLOCKMGR-MIB.mib
16. SUBMARINE-IMC-MIB.mib
17. SUBMARINE-AAA-MIB.mib
18. SUBMARINE-USERS-MIB.mib

19. SUBMARINE-HISTORY-MIB.mib
20. SUBMARINE-ALARM-MIB.mib
21. SUBMARINE-SYSLOG-MIB.mib
22. SUBMARINE-RM-MIB.mib
23. SUBMARINE-QOS-MIB.mib
24. SUBMARINE-VOICE-MIB.mib
25. SUBMARINE-ISM-IPS-MIB.mib

The Enterprise MIB folder includes the following individual MIB.

SUBMARINE-BUNDLE-MIB.mib

Use bundle.mib to manage bundles and links within bundles. Compile bundle.mib before you compile ppp.mib, fr.mib, ghdlc.mib. Use bundle.mib to:

- Be notified when a bundle goes down (bundleDownTrap)
- Be notified when a bundle comes up (bundleUpTrap)
- Be notified when a link goes down (linkDownTrap)
- Be notified when a link comes up (linkUpTrap)

SUBMARINE-CHASSIS-MIB.mib

Use chassis.mib to manage the platform.

SUBMARINE-CONFIG-MIB.mib

Use config.mib to manage configuration data on the router, in memory, or on the network.

Use this MIB to:

- Be notified when the configuration changes (cfgEventChangeNotification)
- Be notified when the configuration is saved (cfgEventSaveNotification)

SUBMARINE-DSX-TC.mib

Compile this MIB before any other DSX MIBs. It does not contain any traps.

SUBMARINE-DSX-TE1-MIB.mib

This MIB manages T1/E1 interfaces. Use this MIB to

- Be notified when an alarm is generated (dsxT1E1AlarmOnTrap)
- Be notified when an alarm is turned off (dsxT1E1AlarmOffTrap)

SUBMARINE-DSX-TE3-MIB.mib

This MIB manages T3/E3 interfaces. Use this MIB to

- Be notified when an alarm is generated (dsxT3E3AlarmOnTrap)
- Be notified when an alarm is turned off (dsxT3E3AlarmOffTrap)

SUBMARINE-ENVIRON-MIB.mib

This MIB manages the chassis environment such as temperature and fan function. Use this MIB to:

- Be notified if the trap is set to true and if temperature reaches a critical level (envTemperatureNotification).
- Be notified if the trap is set to true and the fan state changes (envFanNotification).
- Be notified if the trap is set to true and the specified power supply shuts off (envPowerSupply1DownNotification, envPowerSupply2DownNotification).
- Be notified if the trap is set to true and the specified power supply turns on (envPowerSupply1UpNotification, envPowerSupply2UpNotification).

SUBMARINE-FR-MIB.mib

This MIB manages Frame Relay and Multilink Frame Relay bundles and does not contain any traps.

SUBMARINE-GHDLC-MIB.mib

This MIB manages generic HDLC encapsulated bundles and does not contain any traps.

SUBMARINE-IP-MIB.mib

This MIB manages IP addressable interfaces and static routes and does not contain any traps.

SUBMARINE-PPP-MIB.mib

This MIB manages PPP and MLPPP bundles and does not contain any traps.

SUBMARINE-SMI

This MIB manages internal MIB processes. It must be compiled before any other MIBs are compiled. This does not contain any traps.

SUBMARINE-SNMP-MIB.mib

This MIB defines objects related to SNMP configuration mainly related to community and trap_host configurations. This MIB does not contain any traps. This MIB is obsolete and the information included in this MIB could be found in Standard MIBs, rfc2573.mib and rfc2576.mib.

SUBMARINE-SYSTEM-MIB.mib

This MIB defines system objects such as IP Address, hostName and DNS server. Use this MIB to:

- Be notified when an SNTP client is enabled (sntpEnableNotification).
- Be notified when an SNTP client is disabled (sntpDisableNotification).
- Be notified when an SNTP client is connected to a network time server (sntpSuccessNotification)
- Be notified when an SNTP client is having problems connecting to a network time server (sntpErrorNotification)
- Be notified when there is a system shutdown (shutDownNotification)
- Be notified when a user logs in successfully (userLogInNotification)
- Be notified when a user logs off (userLogOffNotification)
- Be notified when a user is having trouble logging in (userLoginFailNotification)

SUBMARINE-CLOCKMGR-MIB.mib

This MIB defines objects related to managing the network-clocking state of the system. Use this MIB to

- Be notified when the environmental monitoring detects that the network-clock is at a critical state.(clockAllDownNotification)
- Be notified when the environmental monitoring detects that the network-clock is at a normal state.(clockAllUpNotification).

SUBMARINE-IMC-MIB.mib

This MIB defines objects related to manage the inter module communication states. Use this MIB to

- Be notified when an imc communication failure is occurred.
(imcCommFailNotification)
- Be notified when an imc communication failure is recovered.
(imcCommRecoveryNotification)

SUBMARINE-AAA-MIB.mib

This MIB defines objects related to manage the Authentication, Authorization, and Accounting method lists. This MIB does not contain any traps

SUBMARINE-USERS-MIB.mib

This MIB defines objects related to manage the user account and current user lists. This MIB does not contain any traps.

SUBMARINE-HISTORY-MIB.mib

This MIB defines objects related to manage the user login history. This MIB does not contain any traps

SUBMARINE-ALARM-MIB.mib

This MIB defines objects related to manage the current and history alarms. This MIB does not contain any traps.

SUBMARINE-SYSLOG-MIB.mib

This MIB defines objects related to manage the system messages which is logging to console, terminal, buffer and syslog server. This MIB does not contain any traps.

SUBMARINE-RM-MIB.mib

This MIB defines objects related to manage the system resource, such as a CPU and a memory. Use this MIB to

- Be notified when CPU utilization goes over threshold value.
(rmCpuRaiseNotification)
- Be notified when CPU utilization goes down below threshold value.
(rmCpuClearNotification)
- Be notified when Memory utilization goes over threshold value.
(rmMemRaiseNotification)
- Be notified when Memory utilization goes down below threshold value.
(rmMemClearNotification)

SUBMARINE-QOS-MIB.mib

This MIB defines objects related to manage the software QoS. This MIB does not contain any traps.

SUBMARINE-VOICE-MIB.mib

This MIB defines objects related to manage the voice over IP.
Use this MIB to

- Be notified when DSP module initialization fails.
(voiceDspInitNotification)
- Be notified when exceeding a threshold of the system maximum call limit
(voiceMaxCallMajNotification, voiceMaxCallMinNotification)
- Be notified when exceeding a threshold of the DSP channel capacity limit
(voiceDspChanMajNotification, voiceDspChanMinNotification)
- Be notified when connection fails between iBG and SIP entity.
(voiceSipEntityNotification)
- Be notified when the FXO port is connected when using Loop-Start ONLY
(voiceFXOConnNotification)

SUBMARINE-ISM-IPS-MIB.mib

This MIB defines objects related to manage the integrated security module for premium security.

Standard MIBs

The Standard MIBs should be compiled in the following order:

1. rfc1213.mib
2. rfc1471.mib
3. rfc1473.mib
4. rfc1757.mib
5. rfc1406.mib
6. rfc1315.mib
7. rfc1407.mib
8. rfc2787.mib
9. rfc2571.mib
10. rfc2575.mib
11. rfc2572.mib
12. rfc2573.mib
13. rfc2574.mib
14. rfc2576.mib
15. rfc1907.mib
16. iftype.mib
17. rfc2127.mib
18. rfc2620.mib
19. rfc2665.mib
20. rfc2668.mib

The Standard MIB folder contains the following MIBs:

rfc1213.mib

Standard MIB-II objects for TCP/IP networks. This MIB does not contain any traps.

rfc1315.mib

This MIB manages specified Frame Relay DLCI parameters. Use this MIB to:
Be notified when a Virtual Circuit changes state (frDLCIStatusChange)

rfc1406.mib

MIB objects for DS1 interface. This MIB does not contain any traps.

rfc1407.mib

MIB objects for DS3 interface. This MIB does not contain any traps.

rfc1657.mib

This MIB manages specified BGP parameters. This MIB does not contain any traps.

rfc1724.mib

The objects in this MIB manage the RIP2 V2 Protocol in the router.

rfc1850.mib

This MIB manages specified OSPF parameters. This MIB does not contain any traps.

rfc2233.mib

MIB objects for Interface Table extensions including StackTable and ifXTable. The IfStackTable shows the sub-layer relationships of interfaces. This MIB does not contain any traps.

rfc2787.mib

This MIB describes objects used for managing Virtual Router Redundancy Protocol (VRRP) routers.

rfc1471.mib

Implementation of this group is mandatory for all PPP entities.

rfc1473.mib

Implementation of this group is mandatory for all PPP implementations that support operating IP over PPP.

rfc1215.mib

This is really only part of RFC-1215. The other part is built into the Emissary MIB compiler as of Emissary release 4.0.

rfc1757.mib

This MIB defines objects for managing remote network monitoring devices.

rfc2571.mib

This is the SNMP Management Architecture MIB.

rfc2575.mib

The management information definitions for the View-based Access Control Model for SNMP.

rfc2572.mib

The MIB for Message Processing and Dispatching.

rfc2573.mib

This MIB module defines MIB objects which provide mechanisms to remotely configure the parameters used by an SNMP entity for the generation of SNMP messages.

rfc2574.mib

The management information definitions for the SNMP User-based Security Model.

rfc2576.mib

This MIB module defines objects to help support coexistence between SNMPv1, SNMPv2c, and SNMPv3.

rfc1907.mib

The MIB module for SNMPv2 entities.

iftype.mib

This file is maintained by IANA. The latest version can be found at <ftp://ftp.isi.edu/mib/ianaiftype.mib>

This MIB module defines the IANAifType Textual Convention, and thus the enumerated values of the ifType object defined in MIB-II's ifTable.

rfc2127.mib

The MIB module to describe the management of ISDN interfaces.

rfc2618.mib

The MIB module for entities implementing the client side of the Remote Access Dial-In User Service (RADIUS) authentication protocol.

rfc2620.mib

The MIB module for entities implementing the client side of the Remote Access Dial-In User Service (RADIUS) accounting protocol.

rfc2665.mib

MIB objects for Ethernet-like interface. This MIB does not contain any traps.

rfc2668.mib

MIB objects for IEEE 802.3 Medium Attachment Units (MAUs). This MIB does not contain any traps.

SNMP Applications Supported

These SNMP v1 and v2 MIBs can be compiled and used with many popular SNMP managers including, but not limited to:

- HP Openview
- MRTG
- SNMPvC
- NetID
- NetCool

Configuring SNMP

This section describes how to configure Simple Network Management Protocol on a Ubigate iBG router.

snmp-server community

This command sets the SNMP community name and access privileges. This entry is a password string that assigns access privileges to SNMP MIBs.

```
Router/configure/snmp-server# community readuser ro
Router/configure/snmp-server# community writeuser rw
```

snmp-server engineID

This command is for SNMPv3 and changes the local SNMP engine.

```
Router/configure/snmp-server# engineID
00:00:00:ec:00:00:00:16:32:80:43:c0
```



NOTE

Changing the value of engineID has important side effects. A user's password (entered on the command line) is converted to an MD5 or SHA security digest. This digest is based on both the password and the local engine ID. If the local value of engineID changes, the security digests of SNMPv3 users will be invalid, and the users will have to be reconfigured.

snmp-server view

This command is for SNMPv3 and configures the SNMP views. An SNMP view is the mapping between SNMP objects and the access rights available for those objects. Access rights indicate whether the object is accessible by a user.

```
Router/configure/snmp-server# view all 1 1
Router/configure/snmp-server# view ent 1.3.6.1.4.1 1
Router/configure/snmp-server# view one 1.3.6.1.2.1.1 1
Router/configure/snmp-server# view one 1.3.6.1.2.1.2 1
Router/configure/snmp-server# view std 1.3.6.1.4.1 2
```

snmp-server group

This command is for SNMPv3 and configures the SNMP groups. A SNMP group is a collection of SNMP users that belong to common SNMP access rights.

```
Router/configure/snmp-server# group grp v3 noauth readview
std
Router/configure/snmp-server# group grp v3 auth readview
ent writeview std notifyview all
Router/configure/snmp-server# group grp v3 priv readview
all writeview all notifyview all
Router/configure/snmp-server# group initial v3 auth
readview one writeview one notifyview one
Router/configure/snmp-server# group initial v3 priv
readview all writeview all notifyview all
```

snmp-server user

This command is for SNMPv3 and configures an SNMP user to a SNMP group.

```
Router/configure/snmp-server# user noAuthUser grp v3
Router/configure/snmp-server# user authUser grp v3
authProtocol md5 authKey test12345678
Router/configure/snmp-server# user privUser grp v3
authProtocol md5 authKey test12345678 privProtocol des
privKey test12345678
```

snmp-server target

This command configures the recipient of an SNMP trap.

```
Router/configure/snmp-server# target 90.90.90.240 162 v2c
```

For SNOS version 2.0.0 or higher,

```
Router/configure/snmp-server# target 2006:0:0:0:0:0:2 162 v2c
Router/configure/snmp-server# target 2006:0:0:0:0:0:4 162 v3 username privUser secLevel priv
```

snmp-server enable target-traps

This command enables or disables the system to transmit trap groups to a target. If 'all' type is specified, all traps are sent. The 'snmp-server target' command should be configured before the 'snmp-server enable target-traps' command.

Parameter	Description
target <ip_address>	The IP address of the recipient for which the traps are targeted.
trap_group_type	Optional) Type of trap groups to be sent to the target. If 'no' type is specified, the trap group is not sent.
all	Sends all traps.
bgp	Sends bgp group traps
bundle	Sends bundle group traps.
chassis	Sends chassis group traps.
clock	Sends network clock group traps.
config	Sends configuration group traps.
dsx1	Sends dsx1 group traps.
dsx3	Sends dsx3 group traps.
dvmrp	Sends DVMRP group traps.
environ	Sends environment group traps
fr	Sends frame-relay group traps
imc	Sends inter-module communication group traps.
ism	Sends ISM group traps.

(Continued)

Parameter	Description
ospf	Sends OSPF group traps.
pim	Sends PIM group traps.
rm	Sends resource managements group traps
rmon	Sends RMON group traps.
sntp	Sends SNTP group traps.
system	Sends system group traps
voice	Sends voice group traps.
vrrp	Sends VRRP group traps

The following table shows additional parameters for SNOS version 2.0.0 or higher.

Parameter	Description
target <ip_address> <port>	The IP address and the UDP port number of the recipient for which the traps are targeted.
snmp	(default)
	Sends SNMP group trap. Includes coldstart, warmstart, linkdown, linkup, and authfail traps.
	coldstart
	Sends SNMP coldStart trap.
	warmstart
	Sends SNMP warmStart trap.
	linkdown
	Sends SNMP linkDown trap.
	linkup
	Sends SNMP linkUp trap.
	authfail
	Sends SNMP authenticationFailure trap.

```

step1) Router/configure/snmp-server# enable target-traps
165.213.176.232
step2) Router/configure/snmp-server/enable target-traps
165.213.176.232 #all

```

For SNOS version 2.0.0 or higher,

```

step1) Router/configure/snmp-server# enable target-traps
2006:0:0:0:0:0:2 162
step2) Router/configure/snmp-server/enable target-traps
2006:0:0:0:0:0:2 162# all

```

Verifying SNMP configuration

To verify your SNMP configuration use the following commands:

- show snmp community
- show snmp engineID
- show snmp views
- show snmp groups
- show snmp users
- show snmp targets

```
Router# show snmp communities
Community = readuser, privilege = ro.
Community = writeuser, privilege = rw.

Router# show snmp engineID

SNMP engineID : 00:00:00:ec:00:00:00:16:32:80:43:c0

Router# show snmp views

Start of Lists -----
viewname  : all
subtree   : 1
type      : included

viewname  : ent
subtree   : 1.3.6.1.4.1
type      : included

viewname  : one
subtree   : 1.3.6.1.2.1.1
type      : included

viewname  : one
subtree   : 1.3.6.1.2.1.2
type      : included

viewname  : std
subtree   : 1.3.6.1.4.1
type      : excluded

----- End of Lists
Router# show snmp groups
```

```

Start of Lists -----
groupname      : grp
security model : v3      security level : noauth
readview       : std
writeview      : -
notifyview     : -

groupname      : grp
security model : v3      security level : auth
readview       : ent
writeview      : std
notifyview     : all

groupname      : grp
security model : v3      security level : priv
readview       : all
writeview      : all
notifyview     : all

groupname      : initial
security model : v3      security level : auth
readview       : one
writeview      : one
notifyview     : one

groupname      : initial
security model : v3      security level : priv
readview       : all
writeview      : all
notifyview     : all

----- End of Lists
Router# show snmp users

Start of Lists -----
username       : authUser
engine id      : 00:00:00:ec:00:00:00:16:32:80:43:c0
auth-protocol  : md5      priv-protocol : NULL
security model : v3      group name : grp

username : privUser
engine id      : 00:00:00:ec:00:00:00:16:32:80:43:c0
auth-protocol  : md5      priv-protocol : des
security model : v3      group name : grp
username       : noAuthUser
engine id      : 00:00:00:ec:00:00:00:16:32:80:43:c0
auth-protocol  : NULL     priv-protocol : NULL
security model : v3      group name : grp

----- End of Lists

```

Router# **show snmp targets**  for SNOS version 2.0.0 or higher

```

Start of Lists -----
target IP/port : 2006:0:0:0:0:0:4/162
user name      : privUser
security model : v3      security_level : priv
trap group enabled =
    fr          : .1.3.6.1.2.1.10.32
    ospf        : .1.3.6.1.2.1.14.16.2
    bgp         : .1.3.6.1.2.1.15
    rmon        : .1.3.6.1.2.1.16
    vrrp        : .1.3.6.1.2.1.68
pim            : .1.3.6.1.3.61.1
    dvmp        : .1.3.6.1.3.62.1.1.7
    chassis     : .1.3.6.1.4.1.236.4.1.12.2.1.3
    clock       : .1.3.6.1.4.1.236.4.1.12.2.3.3
    imc         : .1.3.6.1.4.1.236.4.1.12.2.9
    rm          : .1.3.6.1.4.1.236.4.1.12.2.22.1
    system      : .1.3.6.1.4.1.236.4.1.12.2.101.4
    snmp        : .1.3.6.1.4.1.236.4.1.12.2.101.12
    environ     : .1.3.6.1.4.1.236.4.1.12.2.103.3
    config      : .1.3.6.1.4.1.236.4.1.12.2.104.4
    dsx1        : .1.3.6.1.4.1.236.4.1.12.2.111.4
    dsx3        : .1.3.6.1.4.1.236.4.1.12.2.112.4
    bundle      : .1.3.6.1.4.1.236.4.1.12.2.113.5
    voice       : .1.3.6.1.4.1.236.4.1.12.2.200.40.1
    ism         : .1.3.6.1.4.1.236.4.1.12.2.300.7
    coldstart   : .1.3.6.1.6.3.1.1.5.1
    warmstart   : .1.3.6.1.6.3.1.1.5.2
    linkdown    : .1.3.6.1.6.3.1.1.5.3
    linkup      : .1.3.6.1.6.3.1.1.5.4
    authfail    : .1.3.6.1.6.3.1.1.5.5

target IP/port : 2006:0:0:0:0:0:2/162
user name      : -
security model : v2c      security_level : noauth
trap group enabled =
    fr          : .1.3.6.1.2.1.10.32
    ospf        : .1.3.6.1.2.1.14.16.2
    bgp         : .1.3.6.1.2.1.15
    rmon        : .1.3.6.1.2.1.16
    vrrp        : .1.3.6.1.2.1.68
pim            : .1.3.6.1.3.61.1
    dvmp        : .1.3.6.1.3.62.1.1.7
    chassis     : .1.3.6.1.4.1.236.4.1.12.2.1.3
    clock       : .1.3.6.1.4.1.236.4.1.12.2.3.3

```

```
imc      : .1.3.6.1.4.1.236.4.1.12.2.9
rm       : .1.3.6.1.4.1.236.4.1.12.2.22.1
system  : .1.3.6.1.4.1.236.4.1.12.2.101.4
snmp     : .1.3.6.1.4.1.236.4.1.12.2.101.12
environ  : .1.3.6.1.4.1.236.4.1.12.2.103.3
config   : .1.3.6.1.4.1.236.4.1.12.2.104.4
dsx1     : .1.3.6.1.4.1.236.4.1.12.2.111.4
dsx3     : .1.3.6.1.4.1.236.4.1.12.2.112.4
bundle   : .1.3.6.1.4.1.236.4.1.12.2.113.5
voice    : .1.3.6.1.4.1.236.4.1.12.2.200.40.1
ism      : .1.3.6.1.4.1.236.4.1.12.2.300.7
coldstart : .1.3.6.1.6.3.1.1.5.1
warmstart : .1.3.6.1.6.3.1.1.5.2
linkdown  : .1.3.6.1.6.3.1.1.5.3
linkup    : .1.3.6.1.6.3.1.1.5.4
authfail  : .1.3.6.1.6.3.1.1.5.5
```

----- End of Lists



CHAPTER 4. System Logging

Logging Commands

The Ubigate iBG router supports event logging as well as the industry-standard syslog logging.

The following commands are useful for configuring event logging on the Ubigate iBG router.

- **system logging**
This command accesses next-level commands for configuring various terminal logging, syslog and event reporting.
- **system logging all_terminal**
This command configures all terminals available on the current system. It has additional arguments for filtering log messages based on severity level.
- **system logging buffered**
This command configures logging buffered in memory. It can set various options like buffering size, severity level for filtering.
- **system logging console**
This command configures severity level for log filtering of log messages printed on console.
- **system logging current_terminal**
This command configures severity level for filtering of log messages on current terminal.
- **system logging email**
This command configures email related setting to send log messages to external email server.

- `system logging logging_on`
This command configures logging enable or not.
- `system logging syslog`
This command configures syslog related settings to send log messages to external syslog server
- `clear cfg_log`
This command clears the system configuration log.
- `clear command_log`
This command clears all information in the command log.
- `event`
This command accesses next-level commands for configuring the event log.
- `ssh_server logevents`
This command enables or disables SSH event logging. SSH logging is disabled by default.
- `show cfg_log`
This command displays the contents of the system configuration log.
- `show system logging buffered`
This command displays the system logging buffered in memory.
- `show system logging commandLog`
This command shows all configuration commands entered by the user.
- `show system logging syslog`
This command shows the current syslog setting.
- `show system logging email`
This command shows the current email related information for log email sending.

Syslog messages' severity

Ubigate iBG router supports logging events to a syslog server. For more information on syslog, see RFC 3164.

The following table shows the different levels of syslog message impact. The first five message levels (Emergency through Warning) have the potential of affecting system performance or normal functionality. The last three message levels (Notification through Debug) report events that do not typically require user monitoring and Samsung recommends that you not configure syslog to log these messages.

The following table lists Message Severity Levels

Level	Meaning
Emergency	The system has become unusable
Alert	Immediate action is needed to restore system stability
Critical	Critical conditions have occurred that may require attention.
Error	Error conditions have occurred that may help track problems
Warning	Warning conditions have occurred that are not severe.
Notification	Normal but significant conditions bear notification
Informational	These informational messages do not require action.
Debugging	These are debugging messages for system troubleshooting only.

For more information of syslog events, refer to the Ubigate iBG Message Reference Manual.

Use the following commands to configure and manage syslog.

- `system logging syslog`
This command accesses next-level commands for configuring syslog on the Router system.
- `show system logging syslog`
Use this command to display configured status related to syslog.

Syslog Configuration

Ubigate provides the following options to configure syslog function.

facility: This option is a kind of log filtering feature. With this setting, an administrator can filter out specific log messages generated by the dedicated facility.

host_ipaddr, host_ipaddrv6: host ip address for external syslog servers

identifier: utc_offset: The time stamp in syslog message is supposed to be local time by Syslog RFC specification. So, there is no time zone information in it. If this option is enabled, the syslog message will include timezone information.

Configure external syslog server

```
Router/configure/system/logging/syslog# ?

    exit          Exit from syslog mode
    facility       set facility type
    host_ipaddr    set syslog host ip address
    host_ipaddrv6  set syslog host ip v6 address
    identifier     set an identifier for syslog messages
    utc_offset     displaying utc offset on/off

    <cr>

Router/configure/system/logging/syslog# host_ipaddr
90.90.1.91
*May 29,2007,17:27:51 #SYS-informational: Logging to syslog
server 90.90.1.91:514 started

Router/configure/system/logging/syslog# no host_ipaddr
90.90.1.91
*May 29,2007,17:27:39 #SYS-informational: Logging to syslog
server 90.90.1.91 stopped
```

Verifying Syslog Configuration

In this section, the method of checking current syslog status is described.

The current syslog status shows the following detailed information.

- Logging enable or disable
- UTC offset on or off
- Severity level to be logged
- The ip address of external syslog servers
- Current facility setting

Verify the current syslog settings and display current log messages in memory buffer

```
Router# show system logging syslog

-----
Syslog Setting
-----

Syslog logging on
  Displaying utc offset: off
  Buffer logging: level debugging, size 2000
  Console logging: level debugging
  Terminal logging: level debugging

Syslog server:
  90.90.1.91 (514)
  90.90.1.148 (514)

Facility Setting:
  Facility type: user
  Facility severity: debug

Identifier Setting:
  Identifier (0xABCD0010): disabled

Router# show system logging buffered
Syslog buffer: 2000 maximum buffer entries,
saving level debugging or higher
4 messages stored, 0 ignored
Log Buffer (792000 bytes):
```

```
*May 29,2007,17:22:35 #PARSER-warning: samsung exit
configuration mode ON TUE MAY 29 17:22:35 2007 FROM SERIAL
*May 29,2007,17:22:33 #PARSER-warning: samsung entered
configuration mode ON TUE MAY 29 17:22:33 2007 FROM SERIAL
*May 29,2007,17:21:56 #AAA-notification: samsung logged in
on Tue May 29 17:21:56 2007 from CONSOLE
*May 29,2007,17:21:29 #SYS-informational: Boot up procedure
completed
```



CHAPTER 5. RMON Configuration

Configuring Remote Monitoring

Remote Monitoring (RMON) is an Internet standard for monitoring network activity. (See RFC 1757 and RFC 2021.) RMON specifies how various network agents collect and exchange data in an SNMP environment.

RMON Version 1 defines the following groups:

1. Statistics-RMON group 1
Used for Ethernet, Fast Ethernet, and Gigabit Ethernet ports.
2. History-RMON group 2
Used for Ethernet, Fast Ethernet, and Gigabit Ethernet ports.
3. Alarm-RMON group 3
4. Event-RMON group 9

The RMON agent does not require monitoring equipment or network analyzers, however, it is useful to collect agent data at Network Management System (which must support RFC 1757 and RFC 2021). Absent an NMS, network administrators can view RMON data using the show commands listed in Verifying RMON Configuration.

Configuring RMON

To enable RMON, enter:

```
Router/configure/rmon# enable
```

To configure RMON statistics (RMON group 1) for a specific interface and owner, enter:

Router/configure/rmon# statistics Ethernet 0/4 owner Manager-1

```
Router/configure/rmon# statistics ethernet0/4 owner Manager-1
```

To configure Ethernet history statistics (RMON group 2) for a specific interface, interval, bucket, and owner, enter:

```
Router/configure/rmon# history ethernet 0/1 interval 100  
buckets 10 owner Manager-1
```

To configure RMON alarms for specified MIB OIDs, alarm entry, index numbers interval, rising/falling alarm threshold, rising/falling event index, alarm sample type (absolute or delta), alarm startup direction (rising/falling alarm, or default), and owner, (RMON group 3), enter:

```
Router/configure/rmon# alarm 1 1.3.6.1.2.1.2.2.1.10.1 300  
1000 0 1 2 type absolute startup rising owner Manager-1
```

To configure an RMON alarm for a variable to be monitored, enter:

```
Router/configure/rmon# alarm 2 ifInoctets 36000 100000 90000  
10 20
```

To configure RMON event (RMON group 9), enter:

```
Router/configure/rmon# event 1
```

To add an RMON event (which can be a log, a trap, or log-trap) enter:

```
Router/configure/rmon# event 1 log
```


To add an RMON events (which can be a log, a trap, or log-trap) with additional information of community for sending traps, event description and owner, enter:

```
Router/configure/rmon# event 2 log community ABC description
"event 2" owner Manager-2
```



Enabling RMON can have a significant impact on performance. When RMON is running, be aware of its impact on data processing and CPU cycles.

Verifying RMON Configuration

To show all RMON alarm configuration information, enter:

```
Router/show/rmon# alarms
RMON Alarms Configured:
Alarm Index    Variable OID    Interval  Startup Type    Or
-----
1      1.3.6.1.2.1.16.1.1.1.5.1  30      Rising or Falling C
2      1.3.6.1.2.1.16.1.1.1.5.1  30      Rising      CLI-Mana
```

To show details of a specific RMON alarm configuration (in this case alarm 1), enter:

```
Router/show/rmon# alarm 1
-----
Alarm Index : 1
-----
Variable OID      : 1.3.6.1.2.1.16.1.1.1.5.1
Last Sample Value : 0
Interval          : 30
Sample Type       : absolute
Alarm Startup     : Rise_Fall(Rising or Falling)
Rising Threshold  : 100
Falling Threshold : 0
Rising Event      : 1
Falling Event     : 1
Alarm Owner       : CLI-Manager
-----
```

To show Ethernet history statistics for the specified Ethernet interface, enter:

```
Router/show/rmon# ethernet_history ethernet0/4

ethernet0/4 Rmon history of History Control With Index 1
-----
ethernet0/4 Rmon history of History Control With Index 2
-----
Sample index:                1 CRC errors:                0
Sample time:      0 days, 0:16: 2 Undersize pkts:          0
Drop events:                0 Oversize pkts:              0
Octets:                     0 Fragments:                 0
Packets:                    0 Jabbers:                    0
Broadcast pkts:              0 Collisions:                0
Multicast Pkts:              0 Utilization:                0
=====
Sample index:                3 CRC errors:                0
Sample time:      0 days, 0:16:22 Undersize pkts:          0
Drop events:                0 Oversize pkts:              0
Octets:                     0 Fragments:                 0
Packets:                    0 Jabbers:                    0
Broadcast pkts:              0 Collisions:                0
Multicast Pkts:              0 Utilization:                0
=====
```

To show specific history control index information, enter:

```
Router/configure/rmon# show rmon history_control ethernet0/0
IndexBucketsInterval Owner
110 1800 CLI-Manager
RMON/configure/rmon#
```

To show the configured RMON events, enter:

```
Router/configure# show rmon events
RMON Events Configured:
Event Event Community Descrip index type
-----
1      log(2)          none      r
2      trap(3)         public   none      r
```

To show RMON statistics for the specified interface, enter:

```
Router/configure/rmon# show rmon statistics ethernet2/19
```

```
-----  
Rmon ethernet statistics of ethernet2/19
```

```
Owner of this Entry: CLI-Manager  
-----
```

```
Drop Events = 0
```

```
Octets = 0
```

```
Packets = 0
```

```
Broadcast Packets = 0
```

```
Multicast Packets = 0
```

```
CRC Error Packets = 0
```

```
Undersize Packets = 0
```

```
Oversize Packets = 0
```

```
Fragments = 0
```

```
Jabbers = 0
```

```
Collisions = 0
```

```
Packets of 64Octets = 0
```

```
Packets of 65to127Octets = 0
```

```
Packets of 128to255Octets = 0
```

```
Packets of 256to511Octets = 0
```

```
Packets of 512to1023Octets = 0
```

```
Packets of 1024to1518Octets = 0  
-----
```

```
RMON/configure/rmon#
```

To show RMON status, enter:

```
Router/configure# show rmon status
```

```
Rmon is ENABLED
```

```
Router/configure# no rmon enable
```

```
Rmon is disabled globally
```

```
Router/configure# show rmon status
```

```
Rmon is DISABLED
```



This page is intentionally left blank.



CHAPTER 6. Image Update

The system contains Ubigate SNOS images. Your system already has an image on it when you receive the system. Nevertheless, you may want to load a different image onto the Ubigate system at some point. For example, you may want to upgrade your software to the latest release, or you may want to use the same SNOS release for all the Ubigate systems in a network. Different system images contain different sets of SNOS features.

SNOS Update Procedure

The following steps presume that the storage media to save the new SNOS image is compact flash.

1. Verify the amount of free space on the flash memory card.
2. Verify that the FTP/TFTP Server has IP Connectivity to the Router.
3. Copy the New Image onto the Flash Memory Card Through the FTP/TFTP Server.
4. Verify SNOS image's validation.
5. Set Boot Parameter to Load the New Image On Startup.
6. Reboot the Router to Load the New Image.
7. Verify the Upgraded Image Version.

Update Step

Step	Command	Purpose
1	Router #file	Enters the file mode.
2	Router /file# ls /cf0	Checks free space in compact flash.
3	Router /file#ping 90.90.90.240	Verify Connectivity to ftp/tftp server
4	Router /file# download 90.90.90.240 ftpboot/mpu81/iBG2016_Advanced_ 2.0.1.Z /cf0/iBG2016_Advanced_2.0.1.Z type ftp	Download from ftp server to compact flash
5	Router /file# ls /cf0	Check downloaded images in compact flash
6	Router /file # version /cf0/iBG2016_Advanced_2.0.1.Z	Verify image's validation
7	Router /file # boot_params	Change boot file name
8	Router# show version	Verify version number

Verify the Amount of Free Space**Command step:****Router #file**

; This command enters file mode.

Router /file# ls /cf0

; This command lists the files in Compact Flash or USB memory.

Command syntax:

ls [device name <d_name>]

Parameter	Definition
device-name	Specifies the device name to list the contents </cf0 /usb0>, default is /cf0

This command displays information of each file in the device. And, it also shows the total bytes of all files and free bytes of the device.

Command example

The following example shows the commands used to verify the amount of free space on the Compact Flash. This Compact Flash has 107916532 byte free space.

```
Router#file
Router /file#ls /cf0

WARNING :
Do not remove Compact Flash or reboot during this process

Contents of /cf0:
```

size	date	time	name
-----	-----	-----	-----
8	APR-01-2007	17:56:44	Certificates.dat
28	APR-01-2007	17:56:44	Keys.dat
51200	APR-02-2007	19:23:18	command.log
20049201	APR-02-2007	19:30:00	iBG2016_Advanced_2.0.0.Z
2534	JAN-21-2000	16:52:14	kyc.cfg
3299	MAR-29-2007	14:43:44	oldsystem.cfg
3305	APR-01-2007	17:56:44	system.cfg

```

Total bytes: 20109575
Bytes Free on /cf0: 107916532

```

Verify that the FTP/TFTP Server Connectivity

Command Step:

Router #ping 90.90.90.200

This command verifies connectivity between a Router system and other network hosts.

Command syntax:

```
ping ip_address [sipaddress <ipaddress>] [pingcnt <n>] [pktsize <n>]
[timeout <n>][fillpattern <n>] [sweepmin<n>] [sweepmax <n>] [tos <n>]
[dfbit <on | off>] [options <none | verbose | validate>] [interval<n>]
```

Parameter	Description
ip_address	destination ip address (A.B.C.D)
sipaddress	source ip address (A.B.C.D)
pingcnt	number of ping packets to send (default: 5)
pktsize	packet size (default: 64)
timeout	time out in seconds (default: 5)
fillpattern	icmp data fill pattern (default: 255)
sweepmin	sweep minimum packet size (default: 36)
sweepmax	sweep maximum packet size (default: 1024)
tos	type of service (default: 0)
dfbit	Turn on DF bit in IP header (default: no)
options	ping options (default: none).
interval	interval between successive transmissions in milliseconds (default: 500 ms)

Symbol	Meaning
!	Receipt of ping echo reply
.	No reply
U	Got reply with destination unreachable
I	User pressed Ctrl + C
&	Got reply with ICMP type 'Time Exceeded'
D	Got reply from different hosts
?	Any other ICMP type. To get more info try ping x.x.x.x verbose

Command example

The following example shows the commands used to verify connectivity to the ftp/tftp server.

```
Router/file# ping 90.90.90.200
Pinging 90.90.90.200 (90.90.90.200): 64 bytes, timeout 5 seconds
!!!!
Ping statistics for 90.90.90.200:
Packets: Transmitted 5, Received 5
Loss Rate 0%, approx. round-trip min/avg/max = 0.367/0.474/0.649
ms.
```

Copy the New Image into the Compact Flash

Command step

Router /file# download 90.90.90.240

ftpboot/mpu81/iBG2016_Advanced_2.0.0.Z

/cf0/iBG2016_Advanced_2.0.0.Z type ftp ftp_mode pasv

; This command downloads a file from a remote host to Compact Flash or USB memory.

Command syntax

download server_ip_address <ip_address> srcfile_path <s_path> dstfile_path <d_path> [type <transfer_type>] [progress <on_off>] [ftp_mode <mode>]

Parameter	Description
server_ip_address <ip_address>	ftp or tftp server IP address
srcfile_path <s_path>	the path name of the source file
dstfile_path <d_path>	the path name of the destination file
type <transfer_type>	the transfer protocol: <ftp tftp (default)>. If ftp is selected, then user login and password will be required.
progress <on_off>	the flag to display progress meter during the file is transfer.: <on off (default)>
ftp_mode <mode>	the mode for opening ftp data connection (only available in ftp).: <port (default) pasv>

Command example

The following example shows the commands used to copy the new image into the flash memory card through the FTP/TFTP server.

```
Router/file# download 90.90.90.240
ftpboot/mpu81/iBG2016_Advanced_2.0.1.Z
/cf0/iBG2016_Advanced_2.0.1.Z type ftp
Handling FTP request !
Continue with the download ? (y/n) : y

WARNING :
Do not remove Compact Flash or reboot during this process
login: common
password:
Transfer complete:      20073685 bytes [100%]

Download successful

Router/file#
```

Verify SNOS image's validation

Command step

Router /file# ls /cf0

; This command lists the files on Compact Flash or USB memory.

Router /file# version /cf0/iBG2016_Advanced_2.0.1.Z

; This command lists versions of the image file on Compact Flash or USB device.

This treats only image type file like SNOS image file or firmware files.

Therefore, using this command with a non-image file will display an error message.

You can get the version name and size from the result of this command.

Command syntax

version [</cf0/filename | /usb0/filename>]

Parameter	Description
/cf0/filename	Image type filename on /cf0
/usb0/filename	Image type filename on /usb0

Command example

The following example shows the commands used for SNOS image's validation.

```
Router/file# ls /cf0
```

WARNING :

Do not remove Compact Flash or reboot during this process

Contents of /cf0:

size	date	time	name
-----	-----	-----	-----
8	APR-01-2007	17:56:44	Certificates.dat
28	APR-01-2007	17:56:44	Keys.dat
51200	APR-02-2007	19:23:18	command.log
20049201	APR-02-2007	19:30:00	iBG2016_Advanced_2.0.0.Z
20073685	APR-02-2007	19:06:52	iBG2016_Advanced_2.0.1.Z
2534	JAN-21-2000	16:52:14	kyc.cfg
3299	MAR-29-2007	14:43:44	oldsystem.cfg
3305	APR-01-2007	17:56:44	system.cfg

Total bytes: 40183260

Bytes Free on /cf0: 87842816

```
Router/file#
```

```
Router/file# version /cf0/iBG2016_Advanced_2.0.1.Z
```

WARNING :

Do not remove Compact Flash or reboot during this process

Checking packed images checksum...

Checksum validation is checked.[OK]

```
/cf0/iBG2016_Advanced_2.0.1.Z Info:
```

```
Image: Type= System Ver= 2.0.1 Size= 17619210 Cksum=
0x337d71ef
```

```
Image: Type= Booting Rom Ver= 1.0.7 Size= 983040 Cksum=
0xfc953da5
```

```
Image: Type= Firmware (DSP) Ver= 50.1.0 Size= 1471367
Cksum= 0x2a1a5a6
```

```
Router /file#
```

Setting Boot Parameter for the New Image

Command step

Router/file#exit

; This command exits file mode.

Router# configure terminal

; This command enters configuration mode.

Router/configure#boot_param

; This command configures the booting related parameters.

The system stores and executes images in the order in which you added them to the boot parameter. If you want to change the order in which images are tried at startup, you can either prepend and clear images from the boot parameter to attain the desired order or you can clear the entire boot parameter and then redefine the list in the desired order.

This command requires system rebooting, however a user can decide when the system reboots.

Command syntax

boot_params

All parameters will be entered interactively. The parameters on each field will display the values typed at the previous time.

Parameter	Description
Boot dev	Device type to get the SNOS image file
Boot file name	Path name and file name. Don't need to prefix the device name
Checksum enable	Flag for checksum of loaded SNOS image If you select 1, then it skips checking checksum values for the image
Show header enable	Flag for showing header information of loaded SNOS image If you select 1, then it will display each header information of the image

(Continued)

Parameter	Description
Save bootrom image	Option for booting ROM update 0: auto update (The Router will update automatically based on the version of booting ROM) 1: update only normal image part 3: force not to update booting ROM
Save Diag Flag	Flag to boot up to diagnostic mode

Command example

The following example shows the commands used to change the boot file name to new SNOS image name and reboot system.

```
Router/file# exit
Router # configure terminal
Router/configure# *Apr 02,2007,19:28:54: #PARSER-warning:
samsung entered config mode ON MON APR 02 19:28:54 2007 FROM
CONSOLE

Router/configure# boot_params
Boot dev  [ftp,active-ftp,tftp,cf0,usb0]: cf0
Boot file name: iBG2016_Advanced_2.0.0.Z
iBG2016_Advanced_2.0.1.Z
Checksum enable      [0:Check ,1:Skip ]: 0
Show header enable  [0:Disalbe,1:Enable]: 1
Save bootrom image  [0:AutoUpdate,1:NormalBTupd,3:NoUpd]: 0
Save Diag Flag      [0:Normal mode,1:Diag mode]: 0

BOOT PARAMETERS HAVE BEEN SAVED.
DO YOU WANT TO REBOOT: (Y/N) ? y
*Apr 02,2007,19:30:29: #PLATFORM-emergency: User types
reboot CLI command, the system will be rebooted.
Router/configure#
```

Verify the Upgraded Image Version

This command is only used for checking the SNOS version after booting the new SNOS version.

Command step

Router #show version

; Use the show version command to show the version of the system currently running.

Command syntax

show version

Command example

The following example shows the commands used verify the updated image version.

```
Router# show version
  Kernel          : WIND version 2.6.
  Boot            : 1.0.7 (NORMAL Boot)
  System          : R2 2.0.1
  Created         : Apr  3 2007, 05:40:10
  Bld Path        : "/home1/build/release/u2rel_2.0.1/src"
  By              : build
  SNOS class      : Advanced SNOS
  Including features: Security Voice
  NorBoot         : 1.0.7
  GolBoot         : 1.0.4
```

Slot/SubSlot	Card-Type	Status	FPGA-Rev	CPLD-Rev
0/-	MPU-A	NORMAL	0x08	0x02
0/0	WTE-2SM	NORMAL	N/A	0x00
0/1	FXS-4M	NORMAL	N/A	0x15
0/2	T1E1-1M	NORMAL	N/A	0x17
1/-	VCU-A	NORMAL	N/A	0x07
1/0	FXS-4M	NORMAL	N/A	0x14
1/1	BRI-2U	NORMAL	N/A	0x0e
2/-	T1E1-4	NORMAL	N/A	0x0c
3/-	ESG-8	NORMAL	N/A	0x06
	LDU-A	NORMAL	N/A	N/A
	VOP-128	NORMAL	N/A	0x35

Router#



CHAPTER 7. Hot Swap

Hot Swap capability allows a network administrator to replace one module with another module of the same type without affecting the rest of the system operation. For example, 4 port T1/E1 module can be replaced by another 4 port T1/E1 module while the system is normally operational.

Hot swap is supported for Voice modules and WAN modules excluding HSSI and CT3 modules. The rest of the system operates normally through the entire period of hot swap action. After the hot swapping is completed, the original configuration for the replaced module can be restored completely.

Hot-Removal of a Module Procedure

A module can be hot-removed according to the following steps:

1. Check the administrative state of a module which you want to remove. The module should be in a normal state.
2. Set the administrative state of the module to admin-down by issuing “slot-disable” command.
3. Check the result of the slot-disable command.
4. Remove the module.

Step-by-Step Configuration

Step	Command	Purpose
1	Router #show chassis	Check the state of module
2	Router #configure terminal	Enters configuration mode
3	Router/configure#slot-disable physlot/physubslot	Disable a module
4	Router # show chassis	Check the result of the slot-disable command

Configuration Example

The following example shows a command used to check the state of a module in a chassis.

```
Router#show chassis
Slot/SubSlot  Card-Type  Admin-Status  Oper-Status  Serial#
-----
0/-           MPU-A      NORMAL        NORMAL
0/0           T1E1-2M    NORMAL        NORMAL        S63A198408
1/-           WT3-1C     NORMAL        NORMAL
2/-           T1E1-4     NORMAL        NORMAL
3/-           ESG-8      NORMAL        NORMAL        ESG-8_SEC_#25
              LDU-A      NORMAL        NORMAL
              VPN-A      NORMAL        NORMAL        S63A198442
              VOP-64     NORMAL        NORMAL        S63A198861
```

The following example shows a command used to enters terminal to configuration mode.

```
Router#configure terminal
Router/configure# *May 06,2001,17:03:25 #PARSER-warning:
samsung entered configuration mode ON SUN MAY 06 17:03:25 2001
FROM SERIAL
```


The following example shows a command used to disable a module.

```
Router/configure# slot-disable 0/0
1 : interface bundle wan1
configuring existing WAN bundle interface wan1
2 : shutdown
3 : exit
4 : no interface bundle wan1
5 : no interface bundle wan2
6 : module e1 0/0/1
7 : exit
8 : module e1 0/0/0
9 : exit
During hotswap-processing, Total commands executed: 6, Total
errors: 0

Router/configure#
```

The following example shows a command used to check the state of a module in a chassis.

```
Router# show chassis
Slot/SubSlot  Card-Type  Admin-Status  Oper-Status  Serial#
-----
0/-           MPU-A       NORMAL        NORMAL
0/0           T1E1-2M     ADMIN-DOWN    OPER-DOWN    S63A198408
1/-           WT3-1C      NORMAL        NORMAL
2/-           T1E1-4      NORMAL        NORMAL
3/-           ESG-8       NORMAL        NORMAL        ESG-8_SEC_#25
              LDU-A       NORMAL        NORMAL
              VPN-A       NORMAL        NORMAL        S63A198442
              VOP-64      NORMAL        NORMAL        S63A198861

Router#
```

Removal of the disabled module

After you verified the status, you can remove the disabled module.

Hot-Insertion of a Module Procedure

A module can be hot-inserted according to the following steps:

1. Check the administrative state and the type of a module which you want to insert. The module should be in an admin-down state and the type should be the same as the new one that you want to replace with.
2. Insert the replacement module.
3. Set the administrative state of the module to normal by issuing “slot-enable” command.
4. Check the result of the “slot-enable” command by issuing “show chassis” command.

Step-by-Step Configuration

Step	Command	Purpose
1	Router #show chassis	Check state and type of module
2	Router #configure terminal	Enters terminal to configuration mode
3	Router/configure#slot-enable physlot/physubslot	Enable a module
4	Router # show chassis	Check the result of slot enable command

Configuration Example

The following example shows a command used to check the state of the replaced module in a chassis.

```
Router#show chassis
Slot/SubSlot  Card-Type  Admin-Status  Oper-Status  Serial#
-----
0/-          MPU-A      NORMAL        NORMAL
0/0          T1E1-2M   ADMIN-DOWN    OPER-DOWN    S63A198408
1/-          WT3-1C    NORMAL        NORMAL
2/-          T1E1-4    NORMAL        NORMAL
3/-          ESG-8     NORMAL        NORMAL        ESG-8_SEC_#25
              LDU-A     NORMAL        NORMAL
              VPN-A     NORMAL        NORMAL        S63A198442
              VOP-64    NORMAL        NORMAL        S63A198861
```

The following example shows a command used to enters configuration mode.

```
Router#configure terminal
Router/configure# *May 06,2001,17:03:25 #PARSER-warning:
samsung entered configuration mode ON SUN MAY 06 17:03:25 2001
FROM SERIAL
```

The following example shows a command used to enable the replaced module.

```
Router/configure# slot-disable 0/0
1 : module e1 0/0/1
2 : exit e1
3 : module e1 0/0/0
4 : exit e1
5 : interface bundle wan1
configuring new WAN bundle interface wan1
6 : link e1 0/0/ encapsulation mlppp
7 : encapsulation mlppp
8 : ppp authentication-database local
9 : ip address 10.10.1.2 255.255.255.0
10 : qos
*May 06,2001,17:25:18 #IPMUXc-notification: <samsung> IP
address(10.10.1.2) is added <OK>
11 : exit qos
12 : exit bundle
13 : interface bundle wan2
configuring new WAN bundle interface wan2
14 : link e1 0/0/1
15 : encapsulation mlppp
16 : ppp authentication-database local
```

```

17 : ip address 10.10.2.2 255.255.255.0
*May 06,2001,17:25:18 #IPMUXc-notification: <samsung> IP
address(10.10.2.2) is added <OK>
18 : ipv6 address 10::2:2/112
*May 06,2001,17:25:19 #IPMUXc-notification: <samsung> IPv6
address(0010::0002:0002) is added <OK>
19 : qos
20 : exit qos
21 : exit bundle
During hotswap-processing, Total commands executed: 51,
Total errors: 0
Router/configure#

```

The following example shows a command used to check the state of the replaced module in a chassis.

```

Router# show chassis
Slot/SubSlot  Card-Type  Admin-Status  Oper-Status  Serial#
-----
0/-           MPU-A      NORMAL        NORMAL
0/0           T1E1-2M    NORMAL        NORMAL        S63A198408
1/-           WT3-1C     NORMAL        NORMAL
2/-           T1E1-4     NORMAL        NORMAL
3/-           ESG-8      NORMAL        NORMAL        ESG-8_SEC_#25
              LDU-A      NORMAL        NORMAL
              VPN-A      NORMAL        NORMAL        S63A198442
              VOP-64     NORMAL        NORMAL        S63A1
Router#

```

PART II. WAN Interface and Protocols



- CHAPTER 1. Serial Interfaces**
- CHAPTER 2. WAN Interfaces**
- CHAPTER 3. PPP, MLPPP and HDLC**
- CHAPTER 4. FR and MFR**
- CHAPTER 5. PPPoFR and MLPPPoFR**



CHAPTER 1. Serial Interfaces

Certain Ubigate iBG routers support High Speed Serial Interface (HSSI) and various serial interfaces such as V.35, RS-232, X.21, 449 and 530.

This document outlines the configuration of module parameters (Layer 1) and, to a lesser degree, the configuration of bundle parameters (Layer 2).

The bundle configuration examples demonstrate linking of physical interfaces (modules) to logical interfaces (bundles). Module configuration occurs within the configure module tree of the Ubigate CLI, and bundle configuration occurs within the configure interface bundle tree.

Serial Interfaces Overview

Multi-Protocol Serial Interface

The Serial Network Module provides four multi-protocol serial interfaces with the ability to support the following serial protocol standards in either DCE or DTE mode: EIA 232C, EIA 449, EIA 530, EIA 530A, V.35 and X.21.

A Multi-Protocol Transceiver in an iBG router constrains all the necessary drivers and receivers for one port to support the appropriate interface types, levels, and termination for the different modes. Each SmartSerial DB26 leaf-contact style connector provides a single cable interface to support any one the different serial standards and modes, all self-configurable depending on which cable type is inserted.

EIA-232C

EIA-232C is a single-ended, asynchronous or synchronous interface. It is equivalent combination of V.24 (connector pin allocation) and V.28 (electrical characteristics) specifications. EIA-232C interface is typically limited to 115kbps, although new ICs can support 230kbps+, and typically limited to 6m (short distance) Both receive and transmit clocks are driven by one end of a connection. Usually, DB-25 connector is used for EIA-232C interface.

EIA-449

EIA-449 interface is a combination of single-ended and differential synchronous interface and also known as V.36. It uses V.11 (EIA-422) electrical characteristics for data and timing (differential) and V.10 (EIA-423) electrical characteristics for link management control signals (single-ended). EIA-449 is typically limited to a maximum throughput of 10Mbps. For the interface, separate clock lines are used for receiving and transmitting data and DB-37 connector are used.

EIA-530/EIA-530A

EIA-530/EIA-530A interface is a combination single-ended/differential synchronous interface. EIA-530/EIA-530A uses V.11 (EIA-422) electrical characteristics for data and timing (differential). It uses V.10 (EIA-423) electrical characteristics for link management control signals (single-ended). For EIA-530, V.11 differential signals of DTR/DSR such as CC(A), CC(B), CD(A), CD(B) are used. For EIA-530A, V.10 single-ended signals of DTR/DSR such as CC, CD are used. EIA-530/EIA-530A interface is typically limited to a maximum throughput of 10Mbps. For the interface, separate clock lines are used for receiving and transmitting data and DB-25 connector is used.

X.21

X.21 is a differential synchronous interface and uses V.11 (EIA-422) electrical characteristics. It is typically limited to a maximum throughput of 10 Mbps. For the interface, a single clock line is used for receiving and transmitting data and DB-15 connector is used.

V.35

V.35 is a combination of single-ended and differential synchronous interface. It uses V.35 electrical characteristics for clock and data (differential) and V.28 (EIA-232) electrical characteristics for control signals (single-ended). It is typically limited to a maximum throughput of 10Mbps. For the interface, separate clock lines are used for receiving and transmitting data and MRAC-34 connector is used.

HSSI Interface

The High-Speed Serial Interface (HSSI) is a DTE/DCE interface and is developed to address the need for high-speed communication over WAN links. HSSI defines both electrical and physical interfaces on DTE and DCE devices. It operates at the physical layer of the OSI reference model.

The maximum signaling rate of HSSI is 52 Mbps. At this rate, HSSI can handle the T3 speeds (45 Mbps) of many of today's fast WAN technologies, as well as the Optical Channel-1 (OC-1) speeds (52 Mbps) of the synchronous digital hierarchy (SDH). In addition, HSSI easily can provide high-speed connectivity between LANs, such as Token Ring and Ethernet.

The use of differential emitter-coupled logic (ECL) helps HSSI achieve high data rates and low noise levels. ECL has been used in Cray computer system interfaces for years and is specified by the ANSI High-Performance Parallel Interface (HIPPI) communications standard for supercomputer LAN communications. ECL is an off-the-shelf technology that permits excellent retiming on the receiver, resulting in reliable timing margins.

HSSI uses a subminiature, FCC-approved 50-pin connector that is smaller than its V.35 counterpart. To reduce the need for male-male and female-female adapters, HSSI cable connectors are specified as male. The HSSI cable uses the same number of pins and wires as the Small Computer Systems Interface 2 (SCSI-2) cable, but the HSSI electrical specification is more concise.

The flexibility of the HSSI clock and data-signaling protocol makes user (or vendor) bandwidth allocation possible. The DCE controls the clock by changing its speed or by deleting clock pulses. In this way, the DCE can allocate bandwidth between applications. For example, a PBX may require a particular amount of bandwidth, a router another amount, and a channel extender a third amount. Bandwidth allocation is a key to making T3 and other broadband services affordable and popular.

HSSI assumes a peer-to-peer intelligence in the DCE and DTE. The control protocol is simplified, with just two control signals required ('DTE available' and 'DCE available'). Both signals must be asserted before the data circuit can become valid. The DCE and DTE are expected to be capable of managing the networks behind their interfaces. Reducing the number of control signals improves circuit reliability by reducing the number of circuits that can fail.



NOTE

The HSSI interface may be operated in either DTE or DCE mode depending on the cable type. For consistency, all signal names and functional definitions use DTE terminology. Thus, Receive Data is data received by the module from the attached piece of equipment, while Transmit Data is data being sent to the attached equipment

Module Configuration

This section describes how to configure serial interfaces of HSSI-1 and WTE-4S modules.

Configuring V.35

This section describes how to configure a serial interface, V.35. The other serial interfaces such as RS-232, X.21, 449 and 530 are to be configured in the similar way.

Configuring V.35 as a DCE

The following steps show how to configure V35 interface for an iBG router where the iBG router is configured as a DCE.

Step-by-Step Configuration

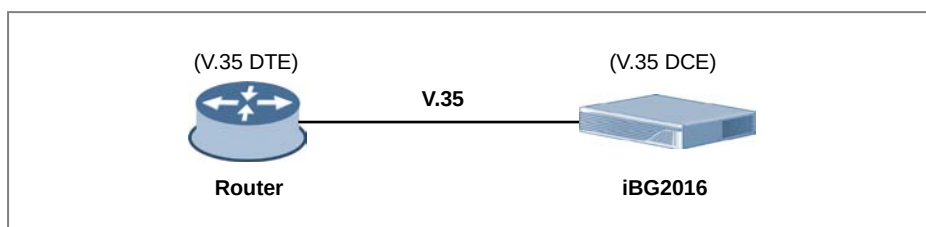
Step	Command	Purpose
1	Router# configure terminal	Enters the terminal configuration mode.
2	Router/configure# module serial [slot /port]	Selects a port to configure as a serial module.
3	Router/configure/module/serial ([slot/port])# mode V.35	Selects a serial interface as a V.35.
4	Router/configure/module/serial ([slot/port])# V35	Enters the V.35 interface.
5	Router/configure/module/serial ([slot/port])/V35# mode dce	Selects V.35 mode as a DCE.
6	Router/configure/module/serial ([slot/port])/V35# clock_rate {56,000 to 52,000,000}	Selects a clock rate.
7	Router/configure/serial ([slot/port])/V35# clock_source {internal line}	Selects a synchronization clock source. As a DTE, the option, 'internal', is recommended.
8	Router/configure/serial ([slot/port])/V35# crc {16 32}	Selects a CRC mode.
9	Router/configure/serial ([slot/port])/V35# data_mode {normal inverted}	Selects a data mode.

(Continued)

Step	Command	Purpose
10	Router/configure/serial ([slot/port])/V35# name {name string}	Name the interface.
11	Router/configure/serial ([slot/port])/V35# end	Returns to the 'Router#' prompt.
12	Router# show module configuration serial [slot/port]	Show configured information of the [slot/port] serial interface.

Configuration Example

The following figure illustrates an example where an iBG router is configured as a DCE.



The following example shows the commands used to configure the connection in The figure.

```
Router# configure terminal
Router/configure# module serial 1/0
Router/configure/module/serial (1/0)# mode V.35
Router/configure/module/serial (1/0)# v35
Router/configure/module/serial (1/0)/v35# mode dce
Router/configure/module/serial (1/0)/v35# clock_rate 2000000
Router/configure/module/serial (1/0)/v35# clock_source
internal
Router/configure/module/serial (1/0)/v35# crc 16
Router/configure/module/serial (1/0)/v35# data_mode normal
Router/configure/module/serial (1/0)/v35# name serial
Router/configure/module/serial (1/0)/v35# end
Router# show module configuration serial 1/0
```

Bundle Configuration

This section describes how to configure a bundle interface. The interface bundle specifies the physical connection to be linked, an encapsulation protocol (Layer 2) and, optionally, Layer 3 parameters.

Configuring a HSSI frame relay bundle

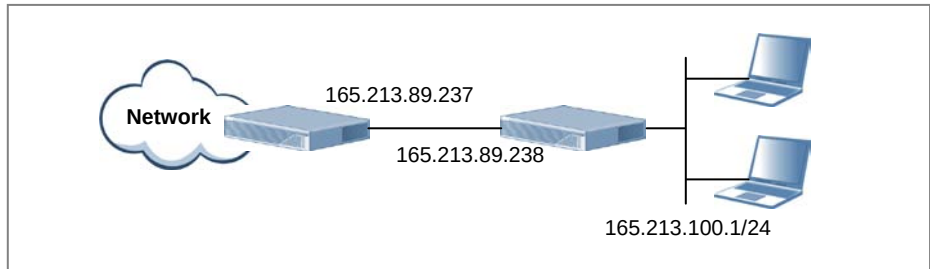
The following example creates a simple interface bundle utilizing the HSSI interface and Frame Relay (Layer 2) parameters.

Step-by-Step Configuration

Step	Command	Purpose
1	Router# configure terminal	Enters the terminal configuration mode.
2	Router/configure# interface bundle [bundle name]	Sets a bundle interface. 'bundle name' represents a specific bundle interface to be configured at the moment.
3	Router/configure/interface/bundle [bundle name]# link hssi 1/0	Links a HSSI interface to a wan interface
4	Router/configure/interface/bundle [bundle name]# encapsulation frrelay	Selects Frame Relay as an encapsulation method.
5	Router/configure/interface/bundle [bundle name]# fr	Enters the frame relay prompt for setting frame relay parameters.
6	Router/configure/interface/bundle [bundle name] /fr#	Selects a clock rate.
7	Router/configure/interface/bundle [bundle name] /fr# pvc [channel number]	Sets a PVC channel number. Channel range: 16 to 1022.
8	Router/configure/interface/bundle [bundle name] /fr/pvc [channel number]# ip address [IP address] { [bit mask] [number of bits for mask] }	Sets an IP address for the PVC.
9	Router/configure/interface/bundle [bundle name] /fr/pvc [channel number]# end	Returns to the 'Router#' prompt.
10	Router# show interface {bundle [bundle name] bundles}	Shows configured information of the bundle interface or all bundle interfaces.

Configuration Example

The following figure illustrates a HSSI bundle configuration.



The following example shows the commands used to configure the connection in the figure.

```
Router# configure terminal
Router/configure# interface bundle wan1
Router/configure/interface/bundle wan1# link hssi 1/0
Router/configure/interface/bundle wan1# encapsulation frelay
Router/configure/interface/bundle wan1# fr
Router/configure/interface/bundle wan1/fr# intf_type dte
Router/configure/interface/bundle wan1/fr# pvc 101
Router/configure/interface/bundle wan1/fr/pvc 101# ip
address 165.213.89.237 24
Router/configure/interface/bundle wan1/fr/pvc 101# end
Router# show interface bundle wan1
```

Configuring a HSSI PPP Bundle

The following example creates a simple interface bundle utilizing the HSSI interface with PPP (Layer 2) parameters.

Step-by-Step Configuration

Step	Command	Purpose
1	Router# configure terminal	Goes into the terminal configuration mode.
2	Router/configure# interface bundle [bundle name]	Sets a bundle interface. 'bundle name' represents a specific bundle interface to be configured at the moment.
3	Router/configure/interface/bundle [bundle name]# link hssi 1/0	Links a HSSI interface to a wan interface
4	Router/configure/interface/bundle [bundle name]# encapsulation ppp	Selects PPP as an encapsulation method.
5	Router/configure/interface/bundle [bundle name]# ip address [IP address] { [bit mask] [number of bits for mask] }	Sets an IP address for the interface.
6	Router/configure/interface/bundle [bundle name] # end	Goes back to the 'Router#' prompt.
7	Router# show interface {bundle [bundle name] bundles}	Shows configured information of the bundle interface or all bundle interfaces.

Configuration Example

The following example shows the commands used to configure the connection in the figure.

```
Router# configure terminal
Router/configure# interface bundle wan1
Router/configure/interface/bundle wan1# link hssi 1/0
Router/configure/interface/bundle wan1# encapsulation ppp
Router/configure/interface/bundle wan1# ip address
165.213.89.237 24
Router/configure/interface/bundle wan1# end
Router# show interface bundle wan1
```

Configuring a V.35 HDLC Bundle

The following example creates a simple interface bundle utilizing the V.35 serial interface with HDLC (layer two) parameters. Before configuring HDLC bundle interface, the serial interface is assumed to be configured as a V.35 in the way described in ‘Configuring V.35 as a DCE.’

Step-by-Step Configuration

Step	Command	Purpose
1	Router# configure terminal	Goes into the terminal configuration mode.
2	Router/configure# interface bundle [bundle name]	Sets a bundle interface. ‘ <i>bundle name</i> ’ represents a specific bundle interface to be configured at the moment.
3	Router/configure/interface/bundle [bundle name]# link serial 1/0	Links a serial interface to a wan interface
4	Router/configure/interface/bundle [bundle name]# encapsulation hdlc	Selects HDLC as an encapsulation method.
5	Router/configure/interface/bundle [bundle name]# ip address [IP address] { [bit mask] [number of bits for mask] }	Sets an IP address for the interface.
6	Router/configure/interface/bundle [bundle name]# end	Returns to the ‘Router#’ prompt.
7	Router# show interface {bundle [bundle name] bundles}	Shows configured information of the bundle interface or all bundle interfaces.

Configuration Example

The following example shows the commands used to configure the connection in the figure.

```
Router# configure terminal
Router/configure# interface bundle wan1
Router/configure/interface/bundle wan1# link serial 1/0
Router/configure/interface/bundle wan1# encapsulation hdlc
Router/configure/interface/bundle wan1# ip address
165.213.89.237 24
Router/configure/interface/bundle wan1# end
Router# show interface bundle wan1
```


Configuring HSSI

The primary use of HSSI is for WAN interfaces such as T3 (45 Mbps), and OC-1 (52 Mbps) of the synchronous digital hierarchy. The HSSI interface can be configured as a DTE or a DCE. Each way to configure HSSI interface is shown in the following.

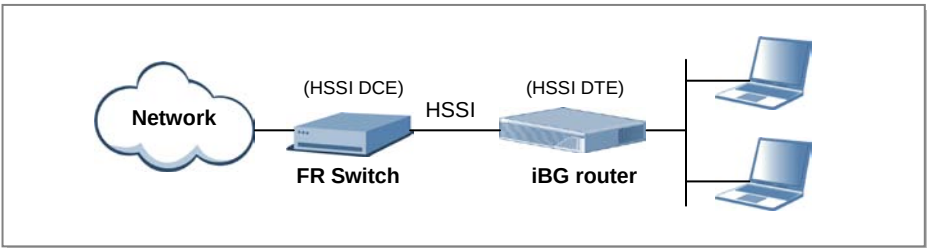
Configuring HSSI as a DTE

Step-by-Step Configuration

Step	Command	Purpose
1	Router# configure terminal	Enters the terminal configuration mode.
2	Router/configure# module hssi [slot /port]	Selects a port to configure as a HSSI module. [slot/port] denotes a specified port in a specified slot.
3	Router/configure/hssi([slot/port])# mode dte	Selects a HSSI mode as a DTE.
4	Router/configure/hssi([slot/port])# clock_source {internal line}	Selects a synchronization clock source. As a DTE, the option, 'line', is recommended.
5	Router/configure/hssi([slot/port])# clock_rate {56,000 to 52,000,000}	Selects a clock rate.
6	Router/configure/hssi([slot/port])# crc {16 32}	Selects a CRC mode.
7	Router/configure/hssi([slot/port])# data_mode {normal inverted}	Selects a data mode.
8	Router/configure/hssi([slot/port])# name {name string}	Name the interface.
9	Router/configure/hssi([slot/port])# end	Returns to the 'Router#' prompt.
10	Router# show module configuration hssi [slot/port]	Show configured information of the [slot/port] HSSI interface.

Configuration Example

The following figure illustrates an example where an iBG router is configured as a HSSI DTE.



The following example shows the commands used to configure the connection in the figure.

```
Router# configure terminal
Router/configure# module hssi 1/0
Router/configure/hssi 1/0)# mode dte
Router/configure/hssi (1/0)# clock_source line
Router/configure/hssi (1/0)# clock_rate 45000000
Router/configure/hssi (1/0)# crc 16
Router/configure/hssi (1/0)# data_mode normal
Router/configure/hssi (1/0)# name hssi1
Router/configure/hssi (1/0)# end
Router# show module configuration hssi 1/0
```

Configuring HSSI as a DCE

Step-by-Step Configuration

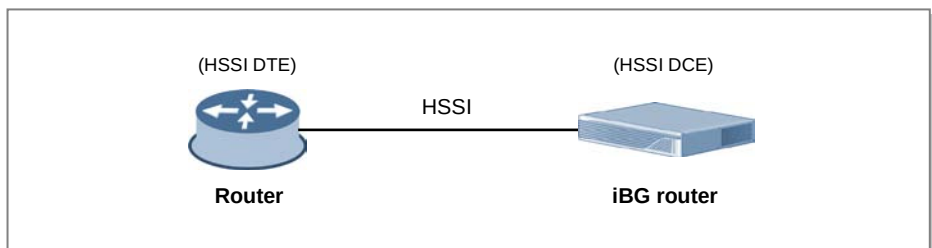
Step	Command	Purpose
1	Router# configure terminal	Enters the terminal configuration mode.
2	Router/configure# module hssi [slot /port]	Selects a port to configure as a HSSI module. [slot/port] denotes a specified port in a specified slot.
3	Router/configure/hssi([slot/port])# mode dce	Selects a HSSI mode as a DCE.
4	Router/configure/hssi([slot/port])# clock_source {internal line}	Selects a synchronization clock source. As a DTE, the option, 'internal', is recommended.

(Continued)

Step	Command	Purpose
5	Router/configure/hssi([slot/port])# clock_rate {56,000 to 52,000,000}	Selects a clock rate.
6	Router/configure/hssi([slot/port])# crc {16 32}	Selects a CRC mode.
7	Router/configure/hssi([slot/port])# data_mode {normal inverted}	Selects a data mode.
8	Router/configure/hssi([slot/port])# name {name string}	Name the interface.
9	Router/configure/hssi([slot/port])# end	Goes back to the 'Router#' prompt.
10	Router# show module configuration hssi [slot/port]	Show configured information of the [slot/port] HSSI interface.

Configuration Example

The following figure illustrates an example where an iBG router is configured as a DCE.



The following example shows the commands used to configure the connection in the figure.

```
Router# configure terminal
Router/configure# module hssi 1/0
Router/configure/hssi (1/0)# mode dce
Router/configure/hssi (1/0)# clock_source internal
Router/configure/hssi (1/0)# clock_rate 45000000
Router/configure/hssi (1/0)# crc 16
Router/configure/hssi (1/0)# data_mode normal
Router/configure/hssi (1/0)# name hssi1
Router/configure/hssi (1/0)# end
Router# show module configuration hssi 1/0
```



This page is intentionally left blank.



CHAPTER 2. WAN Interfaces

iBG routers support T1, Channelized T3, and Clear Channel DS3 WAN interfaces, depending on models. Consult the Ubigate iBG2006/2016/3026 Installation Manuals for details on WAN interface types, cabling, and pinouts. This document outlines the configuration of module parameters (Layer 1) and, to a lesser degree, the configuration of bundle parameters (Layer 2). The bundle configuration examples demonstrate linking of physical interfaces (modules) to logical interfaces (bundles). Module configuration occurs within the configure module tree of the Ubigate CLI, and bundle configuration occurs within the configure interface bundle tree. The T1 and CT3 interfaces support logical interfaces made up of fractional T1, single T1, and multi-link T1 connections.

Module Configuration

This section describes how to configure WAN interfaces of T1E1-2M, T1E1-4 and WT3-1C modules.

Configuring T1 and E1

The following shows simple steps to configure T1 and E1 interfaces respectively.

Configuring T1 Module

The following steps set a few communication modes and port information for a T1 interface.

Step-by-Step Configuration

Step	Command	Purpose
1	Router# configure terminal	Enters the terminal configuration mode.
2	Router/configure# module t1 [slot/subslot/port]	Selects a T1 module port.
3	Router/configure/module/t1(slot/sub slot/port)# circuitId [circuit ID]	Sets a circuit ID.
4	Router/configure/module/t1(slot/sub slot/port)# contactInfo [Contact Information]	Sets contact information such as manager's name or number.
5	Router/configure/module/t1(slot/sub slot/port)# description [Description]	Sets an interface description.
6	Router/configure/module/t1(slot/sub slot/port)# framing {esf d4}	Selects a framing mode
7	Router/configure/module/t1(slot/sub slot/port)# linecode {b8zs ami}	Selects a linecode mode
8	Router/configure/module/t1(slot/sub slot/port)# clock_source {line internal}	Selects a clock source.
9	Router/configure/module/t1(slot/sub slot/port)# end	Returns to the 'Router#' prompt.
10	Router# show module configuration t1 [slot/subslot/port]	Shows T1 module information.

Configuration Example

The following example shows the commands used to configure the connection in the figure.

```
Router# configure terminal
Router/configure# module t1 0/2/0
Router/configure/module/t1 (0/2/0)# circuitId testCircuit
Router/configure/module/t1 (0/2/0)# contactInfo David
Router/configure/module/t1 (0/2/0)# description toSeoul
Router/configure/module/t1 (0/2/0)# framing esf
Router/configure/module/t1 (0/2/0)# linecode b8zs
Router/configure/module/t1 (0/2/0)# clock_source line
Router/configure/module/t1 (0/2/0)# end
Router# show module configuration t1 0/2/0
```

Configuring E1 Module

Before configuring E1 module, the system carrier type must be changed to E1 by using 'system carrier-type' command in the configuration terminal mode. After setting the system carrier type, the system must be rebooted to take effect the changes.

The following steps set a few communication modes and port information for a E1 interface.

Step-by-Step Configuration

Step	Command	Purpose
1	Router# configure terminal	Enters the terminal configuration mode.
2	Router/configure# module e1 [slot/subslot/port]	Selects a E1 module port.
3	Router/configure/module/e1(slot/subslot/port)# circuitId [<i>circuit ID</i>]	Sets a circuit ID.
4	Router/configure/module/e1(slot/subslot/port)# contactInfo [<i>Contact Information</i>]	Sets contact information such as manager's name or number.
5	Router/configure/module/e1(slot/subslot/port)# description [<i>Description</i>]	Sets an interface description.
6	Router/configure/module/e1(slot/subslot/port)# framing {crc noncrc disable}	Selects a framing mode
7	Router/configure/module/e1(slot/subslot/port)# linecode {hdb3 ami}	Selects a linecode mode
8	Router/configure/module/e1(slot/subslot/port)# clock_source {line internal}	Selects a clock source.
9	Router/configure/module/e1(slot/subslot/port)# end	Goes back to the 'Router#' prompt.
10	Router# show module configuration e1 [slot/subslot/port]	Shows E1 module information.

Configuration Example

The following example shows the commands used to configure the connection in the figure.

```
Router# configure terminal
Router/configure# module e1 0/2/0
Router/configure/module/e1 (0/2/0)# circuitId E1234567890
Router/configure/module/e1 (0/2/0)# contactInfo David
Router/configure/module/e1 (0/2/0)# description E1-to-SEOUL
Router/configure/module/e1 (0/2/0)# framing crc
Router/configure/module/e1 (0/2/0)# linecode hdb3
Router/configure/module/e1 (0/2/0)# clock_source line
Router/configure/module/e1 (0/2/0)# end
Router# show module configuration e1 0/2/0
```

Configuring CT3

The following shows simple steps to configure T3 interface module, WT3-1C.

Configuring CT3 interface

The following steps show how to configure communication modes for CT3 interface.

Step-by-Step Configuration

Step	Command	Purpose
1	Router# configure terminal	Enters the terminal configuration mode.
2	Router/configure# module ct3 [slot/port]	Enters CT3 configuration mode
3	Router/configure/module/ct3([slot/port]) # cable_length {1 2}	Sets a cable length - 1: 0 to 225 feet (default) - 2: 226 to 450 feet
4	Router/configure/module/ct3([slot/port]) # framing {c_bit m13}	Sets a framing mode - c_bit: C_BIT format (default) - m13: 226 to 450 feet
5	Router/configure/module/t1(slot/subslot /port)# end	Goes back to the 'Router#' prompt.
6	Router# show module configuration ct3 [slot/port]	Shows CT3 module information.

Configuration Example

The following example shows the commands used to configure the connection in the figure.

```
Router# configure terminal
Router/configure# module ct3 1/0
Router/configure/module/ct3 (1/0)# cable_length 1
Router/configure/module/ct3 (1/0)# framing c_bit
Router/configure/module/ct3 (1/0)# end
Router# show module configuration ct3 1/0
Framing:C-BIT PARITY, LineCode:B3ZS, ClockSource:INTERNAL,
CableLen:0-225ft
LineStatus: RLOS: ON RAIS:OFF RLOF:OFF TAIS:OFF Loop:OFF
```

T1#	FRM	LINE	CLK	Y-ALM	T1#	FRM	LINE	CLK	Y-ALM
---	---	---	---	---	---	---	---	---	---
1	ESF	B8ZS	INT	OFF	15	ESF	B8ZS	INT	OFF
2	ESF	B8ZS	INT	OFF	16	ESF	B8ZS	INT	OFF
3	ESF	B8ZS	INT	OFF	17	ESF	B8ZS	INT	OFF
4	ESF	B8ZS	INT	OFF	18	ESF	B8ZS	INT	OFF
5	ESF	B8ZS	INT	OFF	19	ESF	B8ZS	INT	OFF
6	ESF	B8ZS	INT	OFF	20	ESF	B8ZS	INT	OFF
7	ESF	B8ZS	INT	OFF	21	ESF	B8ZS	INT	OFF
8	ESF	B8ZS	INT	OFF	22	ESF	B8ZS	INT	OFF
9	ESF	B8ZS	INT	OFF	23	ESF	B8ZS	INT	OFF
10	ESF	B8ZS	INT	OFF	24	ESF	B8ZS	INT	OFF
11	ESF	B8ZS	INT	OFF	25	ESF	B8ZS	INT	OFF
12	ESF	B8ZS	INT	OFF	26	ESF	B8ZS	INT	OFF
13	ESF	B8ZS	INT	OFF	27	ESF	B8ZS	INT	OFF
14	ESF	B8ZS	INT	OFF	28	ESF	B8ZS	INT	OFF

FRM = Framing, LINE = Linecode, Y-ALM = Yellow Alarm, CLK = Clock
 DET = Detect, GEN = Generate, D&G = Detect & Generate, INT = Internal

Configuring T1's within CT3

This section shows how to configure T1 channels within CT3 interface.

Step-by-Step Configuration

Step	Command	Purpose
1	Router# configure terminal	Enters the terminal configuration mode.
2	Router/configure# module ct3 [slot/port]	Enters CT3 configuration mode
3	Router/configure/module/ct3([slot/port]) # t1 [T1 number] framing {esf d4}	Sets a T1 interface and its framing mode. T1 number ranges from 1 to 28.
4	Router/configure/module/ct3([slot/port]) # t1 [T1 number] linecode {b8zs ami}	Sets a T1 interface and its linecode mode
5	Router/configure/module/ct3([slot/port]) # t1 [T1 number] yellowalarm {generate detect gen_det disable}	Sets a yellow alarm Configuration
6	Router/configure/module/ct3([slot/port]) # t1 [T1 number] circuitId [Circuit ID]	Sets a Circuit ID.
7	Router/configure/module/ct3([slot/port]) # t1 [T1 number] contactInfo [Contact Info]	Sets a Contact Information.
8	Router/configure/module/ct3([slot/port]) # t1 [T1 number] description [Description]	Sets an interface description.
9	Router/configure/module/ct3([slot/port]) # t1 [T1 number] name [Link Name]	Sets a Link Name.
10	Router/configure/module/ct3([slot/port]) # end	Goes back to the 'Router#' prompt.
11	Router# show module configuration ct3 [slot/port]: [T1 number]	Shows Fractional T1 information.

Configuration Example

The following example shows the commands used to configure the connection in the figure.

```

Router# configure terminal
Router/configuration# module ct3 2/0
Router/configuration/module/ct3 2/0# t1 3 framing esf
Router/configuration/module/ct3 (2/0)# t1 3 linecode b8zs
Router/configuration/module/ct3 (2/0)# t1 3 yellowalarm generate
Router/configuration/module/ct3 (2/0)# t1 3 circuitId CT3_T1_3
Router/configuration/module/ct3 (2/0)# t1 3 contactInfo David
Router/configuration/module/ct3 (2/0)# t1 3 description T1_to_SEOUL
Router/configuration/module/ct3 (2/0)# t1 3 name THIRD_T1_LINK
Router/configuration/module/ct3 (2/0)# end
Router# show module configuration ct3 2/0:3
T1 2/0:3 is ENABLED
Alarm Hierarchy: TRUE,
Yellow Alarm: GENERATE
Framing:ESF, LineCode:B8ZS, ClockSource: INT,
FDL: ANSI Unit Protocol enabled ,ATT Unit Protocol enabled ,
CSUDSUType: CSU & DSU , Loopback Framing (In-band): Overwrite,
CIRCUIT-ID : CT3_T1_3 ,CONTACT-INFO : David ,
DESCRIPTION : T1_to_SEOUL ,LINK NAME : THIRD_T1_LINK ,

Line Status:
    RLOS: ON    RAIS:OFF    RLOF:OFF    RRAI:OFF    TAIS:OFF
    TRAI: ON    TPTrn:OF    Loop:OFF

Timeslot Map:
  1  2  3  4  5  6  7  8  9 10 11 12 13 14 15 16 17 18 19 20 21 22
23 24

|1| |1| |1| |1| |1| |1| |1| |1| |1| |1| |1| |1| |1| |1| |1|
|1| |1| |1| |
|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|
_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|

```

Configuring CT3 bundle

Configuration of an interface bundle is required for WAN interfaces. Multiple physical interfaces may be linked to a single interface bundle; multi-link protocols, including MLPPP and Multilink Frame Relay, make use of NxT1 interfaces to create single logical interfaces. The interface bundle specifies the physical connection(s) to be linked, an encapsulation protocol (Layer 2) and, optionally, Layer 3 parameters.

CT3 Fractional T1

The following example creates a 384 Kbps fractional T1 bundle utilizing DS0s 1-3 and 8-10 of T1 number 3.

```
Router/configure# interface bundle demo
Router/configure/interface/bundle demo# link ct3 2/0/3:1-3
Router/configure/interface/bundle demo# link ct3 2/0/3:8-10
Router/configure/interface/bundle demo# encap hdlc
Router/configure/interface/bundle demo# ip address 10.1.1.9 24
Router/configure/interface/bundle demo# exit
```

CT3 T1

The following example creates a 1536 Kbps T1 bundle utilizing T1 number 4. This bundle uses IP unnumbered.

```
Router/configure# interface bundle demo1
Router/configure/interface/bundle demo1# link ct3 2/0/4
Router/configure/interface/bundle demo1# encap ppp
Router/configure/interface/bundle demo1# ip address 20.1.1.9 24
Router/configure/interface/bundle demo1# exit
```

CT3 NxT1

The following example creates a 4.5 Mbps N x T1 bundle utilizing T1s 6-8. MLPPP is not explicitly specified; a PPP bundle with two or more linked T1s uses the multi-link protocol by definition.

```
Router/configure# interface bundle demo2
Router/configure/interface/bundle demo2# link ct3 2/0/6-8
Router/configure/interface/bundle demo1# encaps mlppp
Router/configure/interface/bundle demo2# ip addr 30.1.1.3
255.255.255.0
Router/configure/interface/bundle demo2# exit
```

Configuring ADSL

An iBG router offers a wide range of WAN interface cards. The new Asymmetric Digital Subscriber Line (ADSL) interface card adds to this offering. This document describes how to configure of the ADSL interface card and provide a configuration example.

This chapter contains the following sections:

- ADSL Interface Card Overview
- How to Configure the ADSL Interface Card
- Configuration Example

ADSL Interface Card Overview

Asymmetric Digital Subscriber Line (ADSL) is a new modem technology that converts existing twisted-pair telephone lines into access paths for high-speed communications of various sorts. It is the most popular protocol among the xDSL technologies (aDSL, hDSL, vDSL and so on). Many home and small offices users can take an advantage of ADSL since ADSL can provide high bandwidth service at much lower price compared to V90 or ISDN.

Current maximum theoretical speeds for various ADSL technologies are as follows:

- ADSL: 1 Mbps upstream / 8 Mbps downstream (G.dmt)
- ADSL2: 1 Mbps upstream / 12 Mbps downstream (ITU G.992.3)
- ADSL2+: 1 Mbps upstream / 24 Mbps downstream (ITU G.992.5)

The ADSL interface card can be plugged into a Mini-Module slot of an iBG router in order to provide ADSL service. The card has one RJ-11 ADSL port and one RJ-45 Ethernet port. The ADSL port should be connected to an ISP's DSLAM. In order to provide WAN connectivity, the ADSL interface card should be connected to one of the fixed Ethernet interfaces in the main chassis of an iBG router. The RJ-45 Ethernet port in the ADSL interface card is used for this purpose.

Figure 1 illustrates a example where an ADSL module is plugged into a Mini-Module slot in Ubigate iBG2016. In order to provide WAN connectivity, one needs to connect the RJ-45 port of the ADSL card and of the fixed Ethernet ports in the main chassis physically. In the example, ethernet 0/4 is used for this purpose.

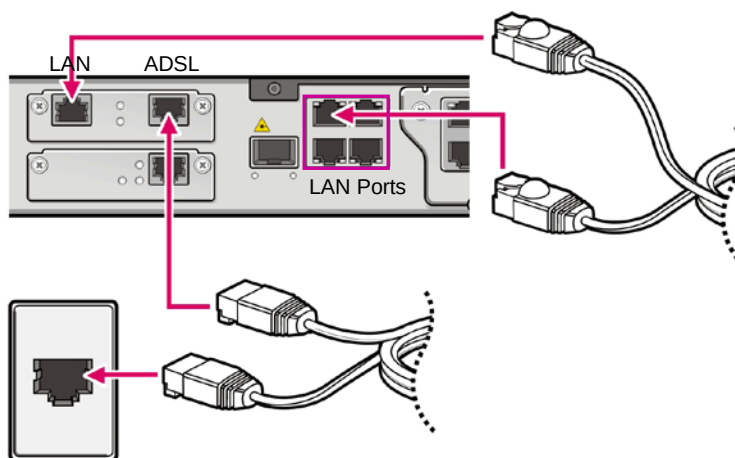


Figure 2.1 ADSL interface card configuration example

The following is a configuration example to enable ADSL interface card in a router.

Step-by-Step Configuration

Step	Command	Purpose
1	Router# configure terminal	Enters the terminal configuration mode.
2	Router/configure# interface ethernet 0/4 [slot/port]	Selects a port to connect with ADSL module.
3	Router/configure/ interface/ethernet (0/4)#connect-dsl 0/0 [slot/sub-slot]	Connect this ethernet port with ADSL module 0/0
4	Router/configure/ interface/ethernet (0/4)#show adsl status	Verify the result.

The following shows how to verify the status of ADSL interface card.

```
Router# show adsl status
```

```
+-----+
| SNOS's ADSL image version : [0.9.8.A] |
+-----+
```

```
ADSL Module      Status      Connected Status  Image Version
=====
| 0/0            Success      [Ethernet 0/4]    [0.9.8.A]
=====
```

Configuring Encapsulation Mode

Figure 2 shows a scenario where iBG3026 is connected with DSLAM.

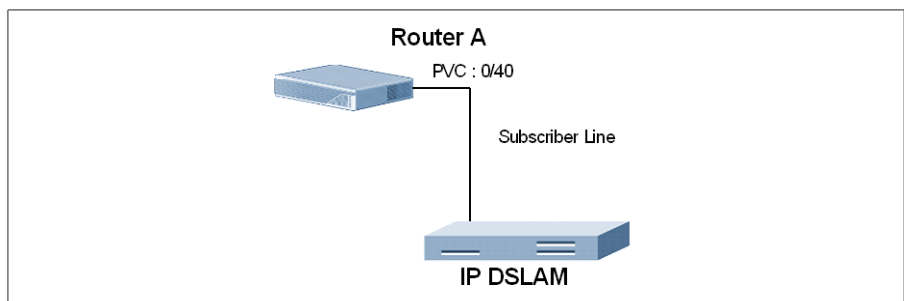


Figure 2.2 ADSL deployment scenario

iBG routers support four modes (adsl, adsl2, adsl2p and auto) for encapsulation mode. By default, encapsulation mode is set to auto mode, then encapsulation mode on iBG router will be trained to the highest possible among the three modes (adsl, adsl2 and adsl2p) allowed by peer DSLAM. The following shows how to set encapsulation mode with adsl2+.

Step-by-Step Configuration

Step	Command	Purpose
1	Router# configure terminal	Enters the terminal configuration mode.
2	Router/configure# module adsl 0/0/0 [slot /sub-slot/port]	Selects a port to configure encapsulation mode.
3	Router/configure/module/adsl(0/0/0) # encap_mode adsl2+	Configure encapsulation mode as ADSL2+.
4	Router# show module configuration adsl 0/0/0	Verify the result.

```

Router# show module configuration adsl 0/0/0

=====
Modem Status      : ShowTime
Mode Selected     : ADSL2p_A [G.992.5]
Latency Type      : Latency Path 0
+-----+
                                     Downstream  Upstream
+-----+-----+
Data Rate          : 27254 kbps           1305 kbps
Maximum Attainable Data Rate : 27304 kbps   1341 kbps
+-----+-----+
Line Attenuation   : 0.00 dB              0.00 dB
Signal Attenuation : 0.00 dB              0.00 dB
Signal-to-Noise Ratio Margin : 7.10 dB      6.10 dB
Actual Aggregate Transmit Power : 10.90 dB   10.00 dB
+-----+-----+
                                     Near End    Far End
+-----+-----+
CRC                : 27                   0
RS_Correction      : 0                    0
HEC Error          : 205                   0

```


Configuring ATM PVC Setting

In order to activate the ADSL interface, one needs to configure the same PVC number as that on DSLAM.

Step-by-Step Configuration

Step	Command	Purpose
1	Router# configure terminal	Enters the terminal configuration mode.
2	Router/configure# module adsl 0/0/0	Selects a port to configure PVC number.
3	Router/configure/module/adsl (0/0/0)# pvc 0 35	Configure PVC number as VPI is 0 and VCI is 35.
4	Router# show adsl pvcs 0/0/0	Verify the result.

The following shows how to verify ADSL PVC configuration.

```
Router# show adsl vc_config 0/0/0

      Adsl VC Configuration
+-----+
VPI  VCI  Encap
=====
  0   40  LLC/SNAP
=====
```

Configuration Example

Figure 3 shows a deployment scenario where an iBG router is connected to an IP DSLAM to get WAN connectivity.

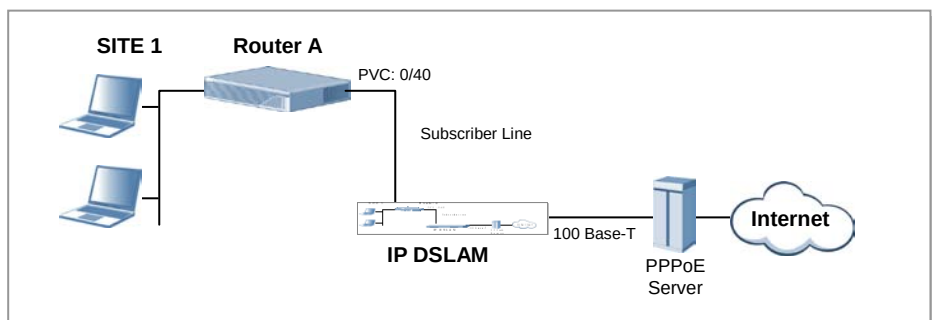


Figure 2.3 ADSL deployment scenario

iBG routers currently support PPPoE only for Layer 2 encapsulation. The following table illustrates a step-by-step configuration to use PPPoE on an ADSL interface.

Step-by-Step Configuration

Step	Command	Purpose
1	Router# configure terminal	Enters the terminal configuration mode.
2	Router/configure# interface ethernet 0/4 [slot/port]	Selects a port to connect with ADSL module.
3	Router/configure/ interface/ethernet (0/4)#connect-dsl 0/0 [slot/sub-slot]	Connect this ethernet port with ADSL module 0/0
4	Router/configure/ interface/ethernet (0/4)#exit	Exit from interface mode
5	Router#show adsl status	Verify the result.
6	Router/configure# module adsl 0/0/0 [slot /sub-slot/port]	Selects a port to configure PVC number.
7	Router/configure/module/adsl(0/0/0) # pvc 0 35	Configure PVC number as VPI is 0 and VCI is 35.
8	Router/configure/module/adsl(0/0/0) #exit	Exit from module mode.
9	Router# show adsl pvcs 0/0/0	Verify the result.
10	Router# show module configuration adsl 0/0/0	Verify the result.
11	Router#interface virtual-access pppoe1	Create virtual interface with name "pppoe1".
12	Router/configure/interface/virtual-access pppoe1#protocol pppoe	Select a tunneling protocol.
13	Router/configure/interface/virtual-access pppoe1/pppoe#ip negotiated	Configure IP address as negotiated over PPP.
14	Router/configure/interface/virtual-access pppoe1/pppoe#pppoe ethernet 0/4	Configure PPPoE ethernet interface.
15	Router/configure/interface/virtual-access pppoe1/pppoe#ppp authentication none	Configure PPP authentication method and parameters.

(Continued)

Step	Command	Purpose
16	Router/configure/interface/virtual-access pppoe1/pppoe#exit	Exit from interface mode.
17	Router/configure# show interface virtual-access pppoe1	Verify the result.

The following shows how to verify the status of virtual interface ‘pppoe1’.

```

Router# show interface virtual-access pppoe1
Virtual Access: pppoe1          Status: up
Internet Address: Negotiated    Subnet Mask:
MTU: 1492 bytes                Ethernet: ethernet0/4
Protocol: PPPoE                Mode: client
Authentication: NONE           Crypto type:
Keep alive time: 10 sec        Access Concentrator:

PPPoE Statistics:
Link Up Time      0 Days 0:01:43
  Bytes Rx      418   Bytes Tx      424
  Packets Rx     28   Packets Tx     28
  Err Packets Rx  0

Router#
Router# show ip interfaces brief
Interface      Type                IP-Address/Mask    Status
ethernet0/0    ETHERNET (802.3)    90.90.9.3/16      Up
ethernet0/2    ETHERNET (802.3)    40.1.1.1/24       Down
ethernet0/4    ETHERNET (802.3)    unassigned         Up
ethernet3/0    ETHERNET (802.3)    unassigned         Down
pppoe1         VIRTUAL ACCESS      143.1.1.10/32     Up
Router#

```



This page is intentionally left blank.



CHAPTER 3. PPP, MLPPP, and HDLC

Ubigate iBG router provides support for point-to-point protocol over WAN interfaces.

The Point-to-Point Protocol (PPP) provides a standard method for transporting multi-protocol datagram over point-to-point links. These links provide full-duplex simultaneous bi-directional operation and are assumed to deliver packets in order. The following figure explains how PPP fits into the Ubigate iBG router software architecture.

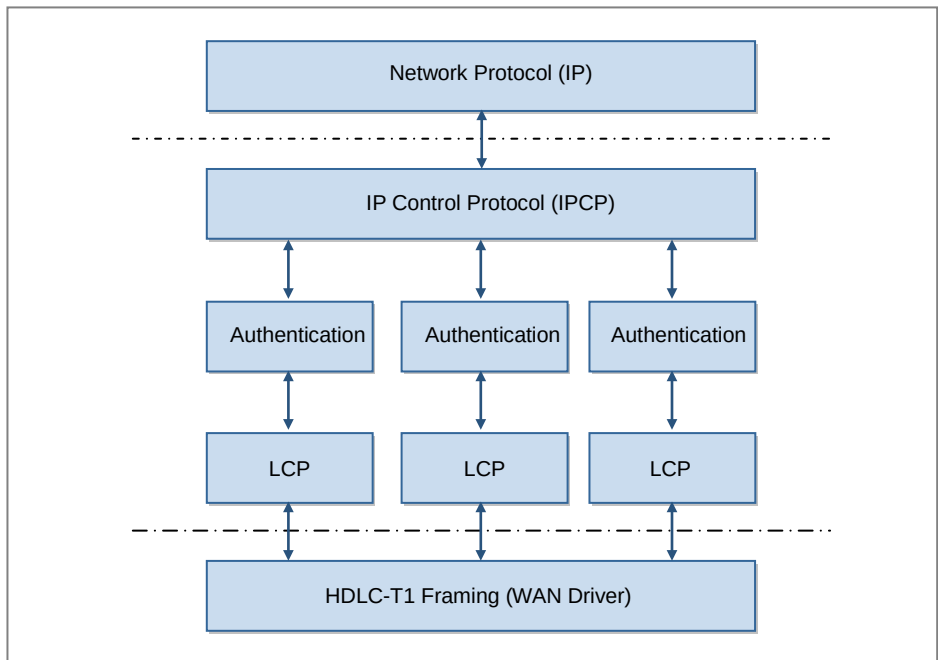


Figure 3.1 Overview of PPP

PPP is comprised of 3 main components: Framing, LCP, and NCP as shown in Figure 3.1.

In an iBG router, PPP is used on the links that use HDLC-like framing (on a WAN side over T1/T3 physical interfaces). The details of the encapsulations can be found in RFC1662 and RFC2516.

A Link Control Protocol (LCP) is used to establish, configure, and test the data-link connection. More detailed information can be found in RFC 1661.

A family of Network Control Protocols (NCPs) are used to establish and configure different network layer protocols. There is an NCP for each network protocol. For example, IPCP is used for IP networks and XNSCP is used for XNS network and so on.

Optionally, before PPP NCP is established, peers may need to authenticate each other and any failure during the authentication process can result in the link termination.

There are two authentication protocols:

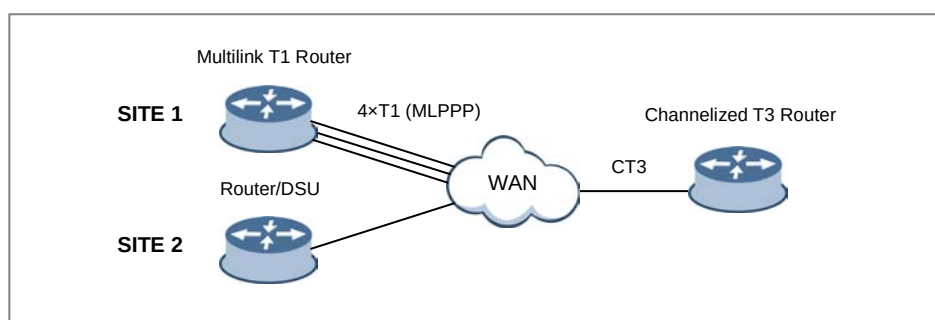
- PAP (Password Authentication Protocol)
- CHAP (Challenge Handshake Authentication Protocol)

The PPP is the most widely used WAN protocol today for internet access and/or leased line connectivity to a remote office. If a bigger bandwidth pipe is needed, one can establish a multilink PPP interface by bundling multiple PPP sessions.

Protocol Configuration

Ubigate iBG routers can accommodate a variety of Layer 2 protocols. This section outlines HDLC, PPP, and Multilink PPP (MLPPP) configurations.

A Ubigate iBG router is often used at POPs (point of presence) to aggregate data for WAN transmission. The following figure shows PPP and multilink PPP connections from two CPE (customer premises equipment) sites to a main site.



1. Site1 uses a multilink T1 router to establish a 6 Mbps MLPPP connection over four T1 lines to the main site.
2. Site2 connects to the main site using a single T1 link with PPP encapsulation.

PPP Configuration

This section shows how to configure the router at site 2 with PPP.

Configuring Ubigate iBG router at Site 2

Step-by-Step Configuration

Step	Command	Purpose
1	Router# configure terminal	Goes into the terminal configuration mode.
2	Router/configure# interface bundle [<i>bundle name</i>]	Sets a bundle interface. ' <i>bundle name</i> ' represents a specific bundle interface to be configured at the moment.
3	Router/configure/bundle/[<i>bundle name</i>]# link t1 1/0-3	Links a channelized T1 interface to a wan interface
4	Router/configure/bundle/[<i>bundle name</i>]# encapsulation ppp	Selects PPP as an encapsulation method.
5	Router/configure/bundle/[<i>bundle name</i>]# ip address [<i>IP address</i>] { [<i>bit mask</i>] [<i>number of bits for mask</i>] }	Sets an IP address for the interface.
6	Router/configure/bundle/[<i>bundle name</i>]# exit	Returns to the upper configuration mode.

Configuration Example

```
R1# configure terminal
R1/configure# interface bundle PPP
R1/configure/interface/bundle PPP# link t1 1/0-3
R1/configure/interface/bundle PPP# encapsulation ppp
R1/configure/interface/bundle PPP# ip address 192.168.1.2 24
R1/configure/interface/bundle PPP# exit
```


MLPPP Configuration

This section shows how to configure interfaces with MLPPP.

Configuring MLPPP for Ubigate iBG router at Main Site

Step-by-Step Configuration

Step	Command	Purpose
1	Router# configure terminal	Goes into the terminal configuration mode.
2	Router/configure# interface bundle [<i>bundle name</i>]	Sets a bundle interface. ' <i>bundle name</i> ' represents a specific bundle interface to be configured at the moment.
3	Router/configure/bundle/[<i>bundle name</i>] # link t1 0/0-3 [<i>slot/port</i>]	Links T1 interfaces to a wan interface
4	Router/configure/bundle/[<i>bundle name</i>] # encapsulation mlppp	Selects MLPPP as an encapsulation method.
5	Router/configure/bundle/[<i>bundle name</i>] # mlppp seg_threshold [64~4500] differential_delay [0~128]	Sets MLPPP segmentation threshold value.
6	Router/configure/bundle/[<i>bundle name</i>] # ip address [<i>IP address</i>] { [<i>bit mask</i>] [<i>number of bits for mask</i>] }	Sets an IP address for the interface.
7	Router/configure/bundle/[<i>bundle name</i>] # exit	Returns to the upper configuration mode.

Configuration Example

```
main# configure terminal
main/configure# interface bundle MLPPP
main/configure/interface/bundle MLPPP# link ct3 1/0/1-4
main/configure/interface/bundle MLPPP# encapsulation mlppp
main/configure/interface/bundle MLPPP# mlppp seg_threshold
1400 differential_delay 50
main/configure/interface/bundle MLPPP# ip address
192.168.1.1 24
main/configure/interface/bundle MLPPP# exit
```

HDLC Configuration

This section shows how to configure interfaces with HDLC.

Configuring HDLC for Ubigate iBG router at Main Site

Step-by-Step Configuration

Step	Command	Purpose
1	Router# configure terminal	Goes into the terminal configuration mode.
2	Router/configure# interface bundle [<i>bundle name</i>]	Sets a bundle interface. ' <i>bundle name</i> ' represents a specific bundle interface to be configured at the moment.
3	Router/configure/bundle/[<i>bundle name</i>] # link ct3 [<i>slot/port/channel</i>]	Links a channelized T3 interface to a wan interface
4	Router/configure/bundle/[<i>bundle name</i>] # encapsulation hdlc	Selects HDLC as an encapsulation method.
5	Router/configure/bundle/[<i>bundle name</i>] # encapsulation hdlc	Selects HDLC as an encapsulation method.
6	Router/configure/bundle/[<i>bundle name</i>] # ip address [<i>IP address</i>] { [<i>bit mask</i>] [<i>number of bits for mask</i>] }	Sets an IP address for the interface.
7	Router/configure/bundle/[<i>bundle name</i>] # end	Return to the 'Router#' prompt.

Configuration Example

```
main# configure terminal
main/configure# interface bundle HDLC
main/configure/interface/bundle HDLC# link ct3 1/0/5
main/configure/interface/bundle HDLC# encapsulation hdlc
main/configure/interface/bundle HDLC# hdlc keepalive 20
main/configure/interface/bundle HDLC# ip address 192.168.2.1 24
main/configure/interface/bundle HDLC# exit
```

Verifying and Troubleshooting Commands

To troubleshoot the PPP configuration and operation, use the following commands:

```
Router# show interface bundle <bundle_name>
```

The following shows how to get a PPP bundle's status information.

```
Router# show interface bundle PPP

bundle PPP
-----
status                               Up

Ipv4 status                          Up
Ipv6 status
number of links                      1
total bandwidth                     1536 kbps

link      speed  bw  inverted  status  diffdelay (msec)
-----
ct3 2/0/5   64   1536   no        up      -

encapsulation                        ppp
  mtu                                100-250-1000
  mru                                100-250-1000
  magic_check                        enable

Negotiated ppp bundle values
  negotiated mru                      250
  negotiated mtu                      250

Authentication parameters
  authentication-database             -- local
  authentication-server               -- none
  accept pap-request                  -- no
  send  pap-request                    -- no
  accept chap-challenge               -- no
  send  chap-challenge                 -- no

Mpls-cp parameters
  mpls-cp is not enabled
  mpls-cp state -- Closed
```

```

ppp-mls-L2Vpn is disabled

Ipv6-cp parameters
  ipv6-cp is not enabled
  ipv6-cp state -- Closed

PPP Timers
  Echo Timer          5
  Restart Timer       3

ip info
  ipaddr              192.168.3.2
  netmask             255.255.255.0

counters since last boot/clear
  Bytes Rx           51712      Bytes Tx           51712
  Packets Rx         4307      Packets Tx           4307
  Err Packets Rx      1
  Up/Down States     0

counters for the last five minutes (updated per 15 sec)
  Bytes Rx           1368      Bytes Tx           1368
  Packets Rx          114      Packets Tx           114
  Err Packets Rx      1
  Up/Down States     0

RED Information
-----
WRED Status: Disabled   DS-RED Status: Disabled

Current queue size = 0      Maximum queue size = 0
Current avg queue size = 0  Maximum avg queue size = 0
Current Q size for WRED = 0
Q overflows = 0

WRED Configuration:
Wq Bias Factor: 5
-----+-----+-----
      color      min      max      mpd
      threshold threshold
-----+-----+-----
      green      16      26      5
      yellow     11      19      5
      red         5      14      5

```

WRED Counters:

Color	Pkts Fwd	Pkts Fwd	Pkts Dropd	Pkts Dropd	Ctrl Pkts
Below Minth	Minth	Minth-Maxth	Minth-Maxth	Above Maxth	
green	0	0	0	0	0
yellow	0	0	0	0	0
red	0	0	0	0	0

Router#

Router# debug ppp ipcp

The following shows how to get IPCP debug information.

```

Router# debug ppp ipcp
WARNING! Enabling PPP Debug can impair system performance.
Do you want to continue?(Y/N)
Icp debug enabled
Router# debug console
LcpSer bundle(PPP) link(0) status updated with "UP"
NcpLyrDown:ncp:0xff020000 NCPEvent:DOWN @S9(St_Opened) ->
S1(St_Starting)

---- dumping PPP packet mp = 0x114b0e00: -----
0x1 0xf 0x0 0xe 0x1 0x4 0x5 0xdc 0x5 0x6 0x70 0x6b 0xb2 0x73
---- msgcnt(1) size(14) dumped-----

---- dumping PPP packet mp = 0x114b0960: -----
0x2 0xb5 0x0 0xe 0x1 0x4 0x0 0xfa 0x5 0x6 0x2c 0x19 0x24 0x93
---- msgcnt(1) size(14) dumped-----
NcpIrc:ncp:0xff020000 NCPEvent:UP @S1(St_Starting) ->
S6(St_ReqSent)
NcpScr:ncp:0xff020000 NCPEvent:UP @S1(St_Starting) ->
S6(St_ReqSent)
O IPCP Configure Request (Sending) :
---- dumping PPP packet mp = 0x114b0e00: -----
0x1 0x3 0x0 0xa 0x3 0x6 0xc0 0xa8 0x3 0x2
---- msgcnt(1) size(10) dumped-----
NcpNullAction:ncp:0xff020000 NCPEvent:OPEN @S6(St_ReqSent) ->
S6(St_ReqSent)
I IPCP Configure Request received:
---- dumping PPP packet mp = 0x11b545d0: -----
0x1 0x5 0x0 0xa 0x3 0x6 0xc0 0xa8 0x3 0x1

```

```

---- msgcnt(1) size(10) dumped-----
I   NcpConverge(ncp:0xff020000,ev:RCR+):IPADDRESS specified:
0xc0a80301
NcpSca:ncp:0xff020000 NCPEvent:RCR+ @S6(St_ReqSent) ->
S8(St_AckSent)
0   IPCP Configure Ack (Sending) :
---- dumping PPP packet mp = 0x114afdd0: -----
0x2 0x5 0x0 0xa 0x3 0x6 0xc0 0xa8 0x3 0x1
---- msgcnt(1) size(10) dumped-----
I   IPCP Configure Ack received:
---- dumping PPP packet mp = 0x11b7cc20: -----
0x2 0x3 0x0 0xa 0x3 0x6 0xc0 0xa8 0x3 0x2
---- msgcnt(1) size(10) dumped-----
ppp-ipc: stopping the ncp-conf-req timer for link 0xff020000
NcpIrc:ncp:0xff020000 NCPEvent:RCA @S8(St_AckSent) ->
S9(St_Opened)
NcpLyrUp:ncp:0xff020000 NCPEvent:RCA @S8(St_AckSent) ->
S9(St_Opened)
Sending an L2_UP event to IPMUX with local addr: c0a80302
peeraddr: c0a80301 mtu: 250
*Oct 19,2000,23:32:43 #PPP-nLcpSerotification: b bundle(undle
UP : PPPPPP) link(0) status updated with "UP"

*Oct 19,2000,23:32:43 #IPMUX-notification: IP received an
L2_UP on bundle PPP mtu 250 peer: 192.168.3.1
LcpSer bundle(PPP) link(0) status updated with "UP"
LcpSer bundle(PPP) link(0) status updated with "UP"

Router#

```

```
Router# debug ppp lcp
```

The following shows how to get LCP debug information

```

Router# debug ppp lcp
WARNING! Enabling PPP Debug can impair system performance.
Do you want to continue?(Y/N)
Lcp debug enabled
Router# debug console
Router# I   LCP Configure Request received on link ff020000:
---- dumping PPP packet mp = 0x11b60ea0: -----
0x1 0x59 0x0 0xe 0x1 0x4 0x0 0xfa 0x5 0x6 0x51 0x66 0xe9 0x40
---- msgcnt(1) size(14) dumped-----

```

```

I LcpConverge(l:0xff020000,ev:RCR+):MRU: 250 bytes requested
***
I MRU (250) suggested by peer is < system Jumbo
Limit..accepting
I LcpConverge(link:0xff020000):setting MRU to 250 bytes
I LcpConverge (MAGIC): Peer magic # 5166E940.
LcpIrc:link:0xff020000 LCPEvent:RCR+ @S3(St_Stopped) ->
S8(St_AckSent)
LcpScr:link:0xff020000 LCPEvent:RCR+ @S3(St_Stopped) ->
S8(St_AckSent)
O LcpPrepareToScr: Link: ff020000, My magic #: 593DA8C8
O Options Sent: Type:1 flag:8 Type:5 flag:8
O LCP Configure Request (Sending) :
---- dumping PPP packet mp = 0x114b0e00: -----
0x1 0xb3 0x0 0xe 0x1 0x4 0x5 0xdc 0x5 0x6 0x59 0x3d 0xa8 0xc8
---- msgcnt(1) size(14) dumped-----
LcpSca:link:0xff020000 LCPEvent:RCR+ @S3(St_Stopped) ->
S8(St_AckSent)
O Options Sent: Type:1 flag:1 Type:5 flag:1
O LCP Configure Ack (Sending) :
---- dumping PPP packet mp = 0x114b0960: -----
0x2 0x59 0x0 0xe 0x1 0x4 0x0 0xfa 0x5 0x6 0x51 0x66 0xe9 0x40
---- msgcnt(1) size(14) dumped-----
I LCP Configure Ack received on link ff020000:
---- dumping PPP packet mp = 0x11b304b0: -----
0x2 0xb3 0x0 0xe 0x1 0x4 0x5 0xdc 0x5 0x6 0x59 0x3d 0xa8 0xc8
---- msgcnt(1) size(14) dumped-----
LcpIrc:link:0xff020000 LCPEvent:RCA @S8(St_AckSent) ->
S9(St_Opened)
LcpLyrUp:link:0xff020000 LCPEvent:RCA @S8(St_AckSent) ->
S9(St_Opened)
O Options Sent: Type:3 flag:8
---- dumping PPP packet mp = 0x114afdd0: -----
0x1 0x4 0x0 0xa 0x3 0x6 0xc0 0xa8 0x3 0x2
---- msgcnt(1) size(10) dumped-----
LcpEcho: Link:0xff020000 rstrtcnt:9
O Link: 0xff020000: Sending LCP Echo Request with id: 180
O Options Sent: Type:3 flag:1

---- dumping PPP packet mp = 0x114b0270: -----
0x2 0x6 0x0 0xa 0x3 0x6 0xc0 0xa8 0x3 0x1
---- msgcnt(1) size(10) dumped-----
LcpSer:link:0xff020000 LCPEvent:RXR @S9(St_Opened) ->
S9(St_Opened)

```

```
*Oct 19,2000,23:47:46 #PLcpRxEchoResPP-notif:link:0xication:
bunff020000dle UP : PPP LCPEvent:
RXR @S9(St_Opened) -> S9(St_Opened)*Oct 19,2000,
23:47:46 #IPMUX-notI Link: 0xificatioff020000n: IP receiv:
Echo Resp rcvd with id: ed an L2_UP on180 bundle PPP mtu
50 peer: 192.168.3LcpIrc.1 :link:0xff020000
LCPEvent:RXR @S9(St_Opened) -> S9(St_Opened)
LcpSer bundle(PPP) link(0) status updated with "UP"
I Link: ff020000: Good echo received
LcpSer:link:0xff020000 LCPEvent:RXR @S9(St_Opened) ->
S9(St_Opened)
LcpEcho: Link:0xff020000 rstcount:9
0 Link: 0xff020000: Sending LCP Echo Request with id: 181
LcpRxEchoRes:link:0xff020000 LCPEvent:RXR @S9(St_Opened) ->
S9(St_Opened)
I Link: 0xff020000: Echo Resp rcvd with id: 181
```

```
Router# debug mlpinf <bundle name>
```

The following shows how to get the MLPPP bundle information.

```
Router# debug ppp mlpinf MLPPP
*****
*****
Bundle #: 2      Structure ptr: 1D7019F0      Last timestamp: 1
Tx sequence #: 0x00000000      Rx begin sequence: 0xFFFFFFFF
Rx begin offset: 0x00000000      Rx end offset: 0x00001000
Rx max sequence: 0xFFFFFFFF      Fragment Mask: 0x00000000
PPP/FR Rx Seq Modulo: 0x00FFFFFF(long)
PPP/FR Tx Seq Modulo: 0x00FFFFFF(long)
Ring buffer modulo: 0x0FFF
Fragment buffer start: 0x1D702FF0 Ring buffer start:
0x1d701fe0
Min. tx size(Seg threshold)=1400, Max_tx_size(Peer MRU)
=1500, Active Links=4
ML Bundle Links Information:
Link #   Link Ptr  Data Xfer OK  Last Seq Recv  Tx Bytes  Frags
-----
00000000 0802F210 Yes          FFFFFFFF      0          0
00000001 0802D0B0 Yes          FFFFFFFF      0          0
00000002 0802B050 Yes          FFFFFFFF      0          0
00000003 0801E9A0 Yes          FFFFFFFF      0          0
Mlp_M: FFFFFFFF
```



```

OutputDrops: 0          InputDrops: 0          Duplicate: 0
TotalOutput: 0          TotalInput: 0
InpSeqAhead: 0          InpSeqLinkAhead: 0
InputOldSeq: 0          InpOldLinkSeq: 0
mlp_discard_loop1: 0    mlp_discard_loop2: 0

    Local EPD(ln:5,class:0x2 addr:0x2 0xc0 0xa8 0x1 0x1 )
    Local MLP Options: 0000001A
    Remote EPD(ln:5,class:0x2 addr:0x2 0xc0 0xa8 0x1 0x2 )
    Remote EPD Clear Count: 0
Router#

```

```

Router# debug negotiation

```

The following shows how to get PPP negotiation debug information.

```

Router# debug ppp negotiation
WARNING! Enabling PPP Debug can impair system performance.
Do you want to continue?(Y/N)
Negotiation debug enabled
Router# debug console
I   LCP Configure Request received on link ff020000:
---- dumping PPP packet mp = 0x11b81b70: -----
0x1 0x92 0x0 0xe 0x1 0x4 0x0 0xfa 0x5 0x6 0x74 0xbb 0x5c 0x40
---- msgcnt(1) size(14) dumped-----
I   LcpConverge(l:0xff020000,ev:RCR+):MRU: 250 bytes requested
***
I MRU (250) suggested by peer is < system Jumbo
Limit..accepting
I     LcpConverge(link:0xff020000):setting MRU to 250 bytes
I   LcpConverge (MAGIC): Peer magic # 74BB5C40.
LcpIrc:link:0xff020000 LCPEvent:RCR+ @S3(St_Stopped) ->
S8(St_AckSent)
LcpScr:link:0xff020000 LCPEvent:RCR+ @S3(St_Stopped) ->
S8(St_AckSent)
O   LcpPrepareToScr: Link: ff020000, My magic #: 38070411
O   LCP Configure Request (Sending) :
---- dumping PPP packet mp = 0x114b0e00: -----
0x1 0xea 0x0 0xe 0x1 0x4 0x5 0xdc 0x5 0x6 0x38 0x7 0x4 0x11
---- msgcnt(1) size(14) dumped-----
LcpSca:link:0xff020000 LCPEvent:RCR+ @S3(St_Stopped) ->
S8(St_AckSent)

```

```

O LCP Configure Ack (Sending) :
---- dumping PPP packet mp = 0x114b0960: -----
0x2 0x92 0x0 0xe 0x1 0x4 0x0 0xfa 0x5 0x6 0x74 0xbb 0x5c 0x40
---- msgcnt(1) size(14) dumped-----
I LCP Configure Ack received on link ff020000:
---- dumping PPP packet mp = 0x11b5f3a0: -----
0x2 0xea 0x0 0xe 0x1 0x4 0x5 0xdc 0x5 0x6 0x38 0x7 0x4 0x11
---- msgcnt(1) size(14) dumped-----
LcpIrc:link:0xff020000 LCPEvent:RCA @S8(St_AckSent) ->
S9(St_Opened)
LcpLyrUp:link:0xff020000 LCPEvent:RCA @S8(St_AckSent) ->
S9(St_Opened)
NcpIrc:ncp:0xff020000 NCPEvent:UP @S1(St_Starting) ->
S6(St_ReqSent)
NcpScr:ncp:0xff020000 NCPEvent:UP @S1(St_Starting) ->
S6(St_ReqSent)
O IPCP Configure Request (Sending) :
---- dumping PPP packet mp = 0x114afdd0: -----
0x1 0x5 0x0 0xa 0x3 0x6 0xc0 0xa8 0x3 0x2
---- msgcnt(1) size(10) dumped-----
NcpNullAction:ncp:0xff020000 NCPEvent:OPEN @S6(St_ReqSent) ->
S6(St_ReqSent)
LcpEcho: Link:0xff020000 rstrtcount:9
O Link: 0xff020000: Sending LCP Echo Request with id: 235
I IPCP Configure Request received:
---- dumping PPP packet mp = 0x11b3ed90: -----
0x1 0x7 0x0 0xa 0x3 0x6 0xc0 0xa8 0x3 0x1
---- msgcnt(1) size(10) dumped-----
I NcpConverge(ncp:0xff020000,ev:RCR+):IPADDRESS specified:
0xc0a80301
NcpSca:ncp:0xff020000 NCPEvent:RCR+ @S6(St_ReqSent) ->
S8(St_AckSent)
O IPCP Configure Ack (Sending) :
---- dumping PPP packet mp = 0x114b0270: -----
0x2 0x7 0x0 0xa 0x3 0x6 0xc0 0xa8 0x3 0x1
---- msgcnt(1) size(10) dumped-----
LcpSer:link:0xff020000 LCPEvent:RXR @S9(St_Opened) ->
S9(St_Opened)
I IPCP Configure Ack received:
---- dumping PPP packet mp = 0x11b46dd0: -----
0x2 0x5 0x0 0xa 0x3 0x6 0xc0 0xa8 0x3 0x2
---- msgcnt(1) size(10) dumped-----
ppp-ipcp: stopping the ncp-conf-req timer for link 0xff020000
NcpIrc:ncp:0xff020000 NCPEvent:RCA @S8(St_AckSent) ->
S9(St_Opened)

```

```

NcpLyrUp:ncp:0xff020000 NCPEvent:RCA @S8(St_AckSent) ->
S9(St_Opened)
*Oct 19,2000,23:54:05 #PPP-notificLcpRxEchoResation:
b:link:0xundle UP : Pff020000PP LCPEvent:RXR
@S9(St_Opened) -> S9(St_Opened)
I Link: 0x*Oct 19,20ff02000000,23:54:05 : Echo Resp rcvd with
id: #IPMUX-notific235ation: IP receive
d an L2_UP on bundLcpIrcle PPP mtu 250:link:0x peer:
192.1ff02000068.3.1 LCPEvent:
RXR @S9(St_Opened) -> S9(St_Opened)
LcpSer bundle(PPP) link(0) status updated with "UP"
I Link: ff020000: Good echo received
LcpSer:link:0xff020000 LCPEvent:RXR @S9(St_Opened) ->
S9(St_Opened)
LcpEcho: Link:0xff020000 rstcount:9
O Link: 0xff020000: Sending LCP Echo Request with id: 236
LcpRxEchoRes:link:0xff020000 LCPEvent:RXR @S9(St_Opened) ->
S9(St_Opened)
I Link: 0xff020000: Echo Resp rcvd with id: 236
LcpIrc:link:0xff020000 LCPEvent:RXR @S9(St_Opened) ->
S9(St_Opened)
LcpSer bundle(PPP) link(0) status updated with "UP"
I Link: ff020000: Good echo received
LcpSer:link:0xff020000 LCPEvent:RXR @S9(St_Opened) ->
S9(St_Opened)

```

```

Router# debug ppp pppstatus <bundle name>

```

The following shows how to get PPP state information.

```

Router# debug ppp pppstates PPP
link          LCP State          Link No
----          -
ct3 1 5      S9(St_Opened)        0xFF020000

IPCP State: S9(St_Opened)

BCP State: S9(St_Opened)

Router#

```

ISDN

Ubigate iBG routers may be configured for ISDN interface bundles. This document outlines ISDN BRI and ISDN PRI interface configurations. The configured interface bundle specifies the physical connection(s) to be linked, an encapsulation protocol (Layer 2) and, optionally, Layer 3 parameters.

Services

BRI Service

BRI (Basic Rate Interface) service possesses two B channels and one D channel (2B+D). BRI B-channel service is operated with 64 Kbps which means User Data. BRI D-channel service is operated with 16 Kbps, transmitting signal information and management information. According to the OSI reference model, D CH ranges from Layer1 to Layer3. BRI is made up of 192 Kbps.

The BRI physical layer specification is International Telecommunication Union-Telecommunications Standards Section (ITU-T) (formerly the Consultative Committee for International Telegraph and Telephone [CCITT]) I.430.

The following figure illustrates a common Ubigate connection using BRI.

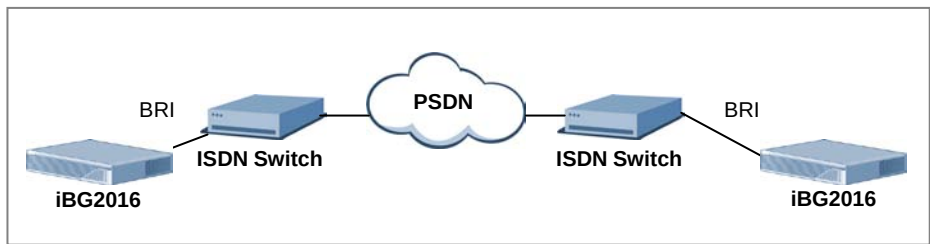


Figure 3.2 ISDN BRI connection with ISDN switches

PRI Service

In America and Japan, PRI (Primary Rate Interface) service is made up of 23 B channel and 1 D channel, which is 1.544 Mbps (the PRI D channel runs at 64 kbps) in total (T1). Countries in Europe and Australia use PRI service made up of 30 B channels plus one 64-kbps D channel, which is 2.048 Mbps in total (E1).

The PRI physical layer specification is ITU-T I.431.

The following figure illustrates a common Ubigate connection using PRI E1. The network topology would be the same for PRI T1.

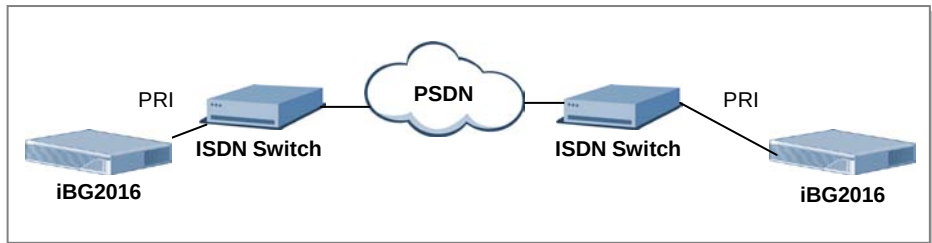


Figure 3.3 ISDN PRI connection with ISDN switches

Configuring ISDN BRI

The following steps show how to configure communication modes for ISDN BRI interface.

Step	Command	Purpose
1	configure terminal	Configures to set up bundle.
2	interface bundle <i>bundle-name</i>	Sets up bundle name.
3	link bri slot/sub-slot/port:timeslot	Sets up the pertinent physical link.
4	Encapsulation [<i>method</i>]	Selects an encapsulation method.
5	Ip address [<i>IP address</i>] { [<i>bit mask</i>] [<i>number of bits for mask</i>] }	Sets an IP address for the interface
6	Isdn	Sets up ISDN
7	switch-type <i>switch-type</i>	Sets up the pertinent switch-type with the content like the following table.
8	Activate	Activates ISDN.
9	Exit	-
10	voice-port <i>slot/sub-slot/port</i>	Configure to set up voice port
11	no shutdown	Turns on the port.

Delete the ISDN BRI

To delete the ISDN, use the following command

Step	Command	Purpose
1	configure terminal	Configures to set up bundle.
2	interface bundle <i>bundle-name</i>	Indicate the ISDN bundle name to delete.
3	Shutdown	Shutdown interface bundle
4	no interface bundle <i>bundleName</i>	Delete interface bundle



NOTE

An existing ISDN interface bundle is should be shutdown before the ISDN bundle is deleted.

Configuration Example

The following example shows the commands used to configure the ISDN BRI

```
Router# configure terminal
Router/configure# interface bundle bri000
configuring new WAN bundle interface bri000
Router/configure/interface/bundle bri000# link bri 0/0/0:2
Router/configure/interface/bundle bri020# encapsulation ppp
Router/configure/interface/bundle bri020# ip address
30.30.30.2 255.255.255.0
Router/configure/interface/bundle bri000# isdn
Router/configure/interface/bundle bri000/isdn# switch-type
basic-euro
Router/configure/interface/bundle bri000/isdn# side USR
Router/configure/interface/bundle bri000/isdn# callednum
5552001
Router/configure/interface/bundle bri000/isdn# activate
Router/configure/ interface/bundle bri000/isdn# end
Router#
```

Configuring ISDN PRI

The following steps show how to configure communication modes for ISDN PRI interface.

Step	Command	Purpose
1	configure terminal	Configures to set up bundle.
2	interface bundle <i>bundle-name</i>	Sets up bundle name.
3	link [pri_t1 pri_e1] slot/sub-slot/port:timeslot	Sets up the pertinent physical link.
4	Encapsulation [method]	Selects an encapsulation method.
5	Ip address [IP address] { [bit mask] [number of bits for mask] }	Sets an IP address for the interface
6	Isdn	Sets up ISDN
7	switch-type <i>switch-type</i>	Sets up the pertinent switch-type with the content like the following table.
8	Side [NET USR]	Sets up for network side.
9	Activate	Activates ISDN.
10	end	-

Delete the ISDN PRI

To delete the ISDN, use the following command

Step	Command	Purpose
1	configure terminal	Configures to set up bundle.
2	interface bundle <i>bundle-name</i>	Indicate the ISDN bundle name to delete.
3	Shutdown	Shutdown interface bundle
4	no interface bundle <i>bundleName</i>	Delete interface bundle



NOTE

An existing ISDN interface bundle is should be shutdown before the ISDN bundle is deleted.

Configuration Example

The following example shows the commands used to configure the ISDN BRI

```
Router# configure terminal
Router/configure# interface bundle pri001
configuring new WAN bundle interface pri001
Router/configure/interface/bundle pri001# link pri_e1 0/0/1
Router/configure/interface/bundle pri001# encapsulation ppp
Router/configure/interface/bundle pri001# ip address
20.20.20.7 255.255.255.0
Router/configure/interface/bundle pri001# isdn
Router/configure/interface/bundle pri001/isdn# switch-type
primary-euro
Router/configure/interface/bundle pri001/isdn# side USR
Router/configure/interface/bundle pri001/isdn# callednum
5551700
Router/configure/interface/bundle pri001/isdn# activate
Router/configure/interface/bundle pri001/isdn# end
```

Verifying ISDN Configuration

The following example shows the commands used to display the information of configured ISDN bundle.

```
Router# show isdn interface pri001
ISDN Information: pri001
-----
caller          -
answer1         -
answer2         -
called-number   5551700
spid1           -
spid2           -
idle-timeout    5
connect delay   15
keep-alive      10000
disconnect-cause 17
switch-type     primary-euro
side            USR
tei-mode        point-to-point
```


The following example shows the commands used to display the information of ISDN bundle status. This example shows the ACTIVE status of PRI bundle.

```
Router# show isdn interface pri001
iBG-04# show isdn status pri10
== USER (0/0/1) side configuration ==
Layer 1 Status:
ACTIVE
Layer 2 Status:
ACTIVE TEI MODE POINT-TO-POINT
Layer 3 Status:
4 Active Calls
```

Troubleshooting ISDN Interfaces

The following figure 3-5 illustrates a common ISDN message flow. Also the debug messages are captured Q931 messages on calling party interface.

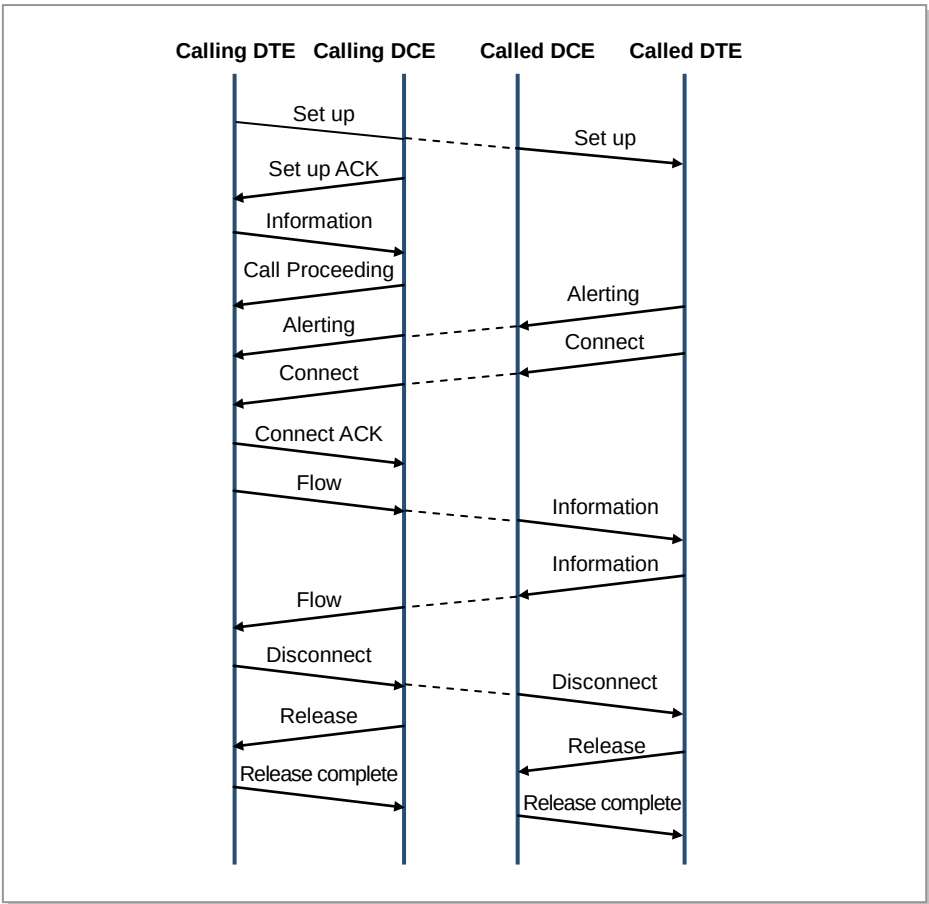


Figure 3.4 Common ISDN message Flow

```
Router# debug isdn q931 pri001
-- 17:10:13.480() -- T --> N (Q931,10) --
MSG          : SETUP
MSGHDR       : 08 02 00 04 05
BEARCAP      : 04 02 88 90
CHANID       : 18 03 a9 83 82
CDPTYNMB     : 70 08 80 35 35 35 34 30 30 30

-- 17:10:13.490() -- N --> T (Q931,10) --
MSG          : CALLPROC
MSGHDR       : 08 02 80 04 02
CHANID       : 18 03 a9 83 82

-- 17:10:13.490() -- N --> T (Q931,10) --
MSG          : CONNECT
MSGHDR       : 08 02 80 04 07

-- 17:10:13.490() -- T --> N (Q931,10) --
MSG          : CONNACK
MSGHDR       : 08 02 00 04 0f

-- 17:15:07.660() -- N --> T (Q931,10) --
MSG          : DISC
MSGHDR       : 08 02 80 04 45
CAUSE        : 08 02 81 90

-- 17:15:07.660() -- T --> N (Q931,10) --
MSG          : RELEASE
MSGHDR       : 08 02 00 04 4d
CAUSE        : 08 02 81 90

-- 17:15:07.670() -- N --> T (Q931,10) --
MSG          : RELCMPLT
MSGHDR       : 08 02 80 04 5a
CAUSE        : 08 02 82 90
```

Message Direction

This example shows the direction field of the ISDN Q931 Message. When the direction field is displayed 'T → N', it means the ISDN message is transmitted from this Gateway to the ISDN network. On the contrary, the direction field is displayed 'N → T' which means that the ISDN message is received from the ISDN network to this Gateway. The following example shows the SETUP message transmitted from the Gateway to the network side (or ISDN switch) of the ISDN interface.

```
-- 18:53:04.240() -- T --> N (Q931,11) --  
MSG      : SETUP  
MSGHDR   : 08 01 02 05  
BEARCAP  : 04 03 80 90 a3  
CHANID   : 18 01 89  
PROGIND  : 1e 02 81 88  
CGPTYNMB : 6c 09 00 80 37 30 30 36 30 30 30  
CDPTYNMB : 70 08 80 35 35 35 33 30 30 30
```

Calling party number and Called party number

The following example shows the calling party number (CGPTYNMB) and called party number (CDPTYNMB) on Q931 messages. The purpose of these information elements is to identify the calling party and called party of a call. In this example, The calling party number is 700-6000 and the called party number is 5553000.

```
-- 18:53:04.240() -- T --> N (Q931,11) --  
MSG      : SETUP  
MSGHDR   : 08 01 02 05  
BEARCAP  : 04 03 80 90 a3  
CHANID   : 18 01 89  
PROGIND  : 1e 02 81 88  
CGPTYNMB : 6c 09 00 80 37 30 30 36 30 30 30  
CDPTYNMB : 70 08 80 35 35 35 33 30 30 30
```

Progress Indicator

The following example shows the Progress indicator information element. The purpose of the Progress indicator information element is to describe an event which has occurred during the life of a call. In this example, The progress description value is 8. The meaning of progress description value is described below table.

```
-- 18:53:04.240() -- T --> N (Q931,11) --
MSG      : SETUP
MSGHDR   : 08 01 02 05
BEARCAP  : 04 03 80 90 a3
CHANID   : 18 01 89
PROGIND  : 1e 02 81 88
CGPTYNMB : 6c 09 00 80 37 30 30 36 30 30 30
CDPTYNMB : 70 08 80 35 35 35 33 30 30 30
```

Value	Mean
1	Call is not end-to-end ISDN; further call progress information may be available in-band
2	Destination address is non-ISDN
3	Origination address is non-ISDN
4	Call has returned to the ISDN
5	Interworking has occurred and has resulted in a telecommunication service change
8	In-band information or an appropriate pattern is now available
All others	Reserved



This page is intentionally left blank.



CHAPTER 4. FR and MFR

Layer Two Configurations

The following figure outlines a Multilink Frame Relay (MFR) configuration with three sites. PVC 16 connects Site 1 to Site 3, while PVC 31 connects Site 2 to Site 3.

The Frame Relay switching equipment is represented simply as a Frame cloud.

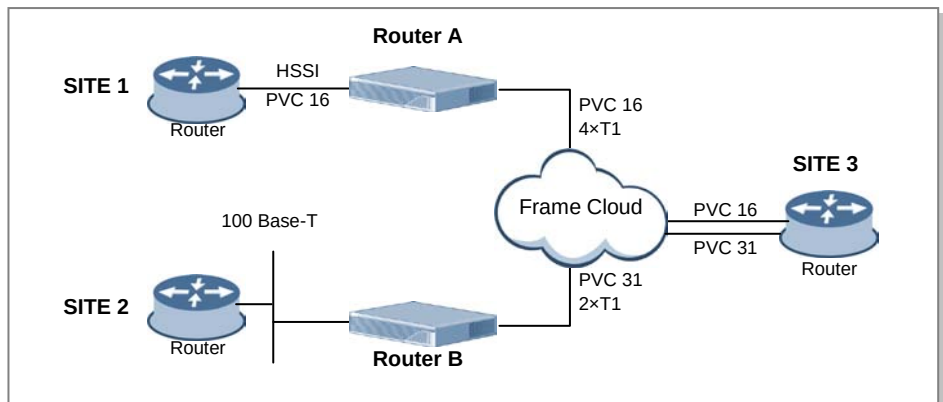


Figure 4.1 Multilink Frame Relay with Three Sites

The following figure provides greater detail, including the use of Router A inside the cloud as a Frame Relay switching device, and Router A, Router B series units at the CPE sites 1 and 2.

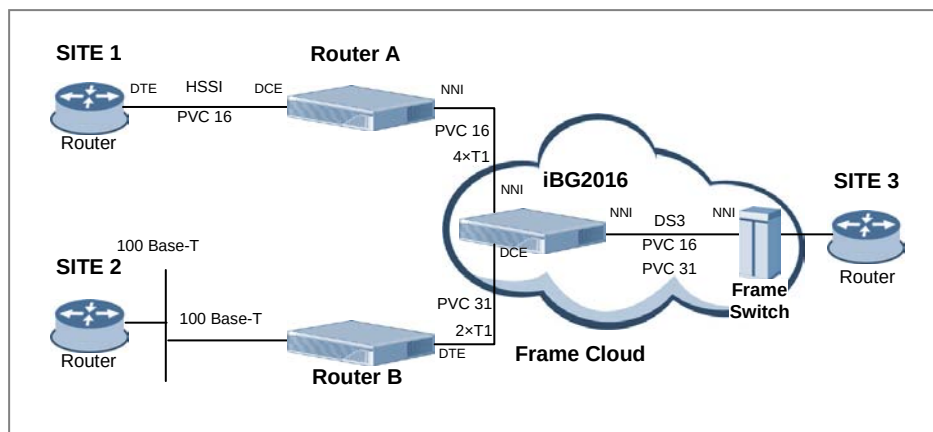


Figure 4.2 Multilink Frame Relay with Three Site Details

FR Configuration

A Router at Site 1 provides Frame Relay switching between a HSSI interface, connecting to the local router, and a 4 x T1 MFR bundle, connecting to the Router. Continuity of PVC 16 is maintained through the Router, though this is not required.

The HSSI connection between the router and the Router is defined as type UNI. The Router serves as Frame Relay DCE and the router as the Frame Relay DTE. Note that the Frame Relay (Layer 2) interface type is independent of, and not necessarily the same as, the HSSI (Layer 1) interface type.

Configure the HSSI Bundle at Site 1

```

Router/configure# interface bundle toRouter
Router/configure/interface/bundle toRouter# link hssi 1/0
Router/configure/interface/bundle toRouter# description
"hssi link to router"
Router/configure/interface/bundle toRouter# encap fr
Router/configure/interface/bundle toRouter# fr
Router/configure/interface/bundle toRouter/fr# intf_type dce
Router/configure/interface/bundle toRouter/fr# lmi ansi
Router/configure/interface/bundle toRouter/fr/lmi# exit
Router/configure/interface/bundle toRouter/fr# pvc 16
Router/configure/interface/bundle toRouter/fr/pvc# shaping
cir 6144000 bcmax 6144000 bcmin 3072000
Router/configure/interface/bundle toRouter/fr/pvc# exit

```

The Router serves as a Frame Relay switch, connecting PVCs 16 and 31 through to another Frame Switch via a Clear Channel DS-3 interface. Note that the Bcmin setting of 3.072 Mbps is maintained across all PVC 16 configurations, to correspond to the Class C setting of the MFR portion of the PVC.

Configure the Clear Channel Bundle on the Router

```

Router/configure# int bundle toFRSwit
Router/configure/interface/bundle toFRSwit# link t3 2/0
Router/configure/interface/bundle toFRSwit# description
"DS-3 bundle to FR Switch"
Router/configure/interface/bundle toFRSwit# encap fr
Router/configure/interface/bundle toFRSwit# fr
Router/configure/interface/bundle toFRSwit/fr# intf_type nni
Router/configure/interface/bundle toFRSwit/fr# lmi ansi
Router/configure/interface/bundle toFRSwit/fr/lmi# exit
Router/configure/interface/bundle toFRSwit/fr# pvc 16
Router/configure/interface/bundle toFRSwit/fr/pvc# shaping
cir 6144000 bcmax 6144000 bcmin 3072000
Router/configure/interface/bundle toFRSwit/fr/pvc# switch 16
toRouter
Router/configure/interface/bundle toFRSwit/fr/pvc# exit
Router/configure/interface/bundle toFRSwit/fr# pvc 31
Router/configure/interface/bundle toFRSwit/fr/pvc# shaping
cir 3072000 bcmax 3072000 bcmin 1536000
Router/configure/interface/bundle toFRSwit/fr/pvc# switch 31
to1400

```

MFR Configuration

The 4 x T1 MFR bundle between the Router and the Router connects two Frame Relay switches, therefore it represents an NNI interface. The sample configuration defines the 4 × T1 bundle to be of Class C; that is, a minimum of 2 T1 links are required to be up in order to keep the bundle up. Settings for Bcmin on the MFR bundle are set to correspond with the Class C configuration; that is, the minimum anticipated bandwidth will be 2 × T1.

Configure the Router A at Site 1

```
Router/configure# int bundle wan1
Router/configure/interface/bundle wan1# link t1 1/0-3
Router/configure/interface/bundle wan1# encap fr
Router/configure/interface/bundle wan1# fr
Router/configure/interface/bundle wan1/fr# intf_type nni
Router/configure/interface/bundle wan1/fr# mfr class C 2
Router/configure/interface/bundle wan1/fr# lmi ansi
Router/configure/interface/bundle wan1/fr/lmi# keepalive 8
Router/configure/interface/bundle wan1/fr/lmi# exit
Router/configure/interface/bundle wan1/fr# pvc 16
Router/configure/interface/bundle wan1/fr/pvc# shaping cir
6144000 bcmax 6144000 bcmin 3072000
```

Configure the Router interface connecting to Router A

```
Router/configure# int bundle toRouter
Router/configure/interface/bundle toRouter# link t1 1/0-3
Router/configure/interface/bundle toRouter# description
"6Mbps MFR to Router"
Router/configure/interface/bundle toRouter# encap fr
Router/configure/interface/bundle toRouter# fr
Router/configure/interface/bundle toRouter/fr# intf_type nni
Router/configure/interface/bundle toRouter/fr# mfr class C 2
Router/configure/interface/bundle toRouter/fr# lmi ansi
Router/configure/interface/bundle toRouter/fr/lmi# keepalive 10
Router/configure/interface/bundle toRouter/fr/lmi# exit
Router/configure/interface/bundle toRouter/fr# pvc 16
Router/configure/interface/bundle toRouter/fr/pvc# shaping
cir 6144000 bcmax 6144000 bcmin 3072000
Router/configure/interface/bundle toRouter/fr/pvc# exit
Router/configure/interface/bundle toRouter/fr# exit 2
```

Router B at Site 2 serves as the Frame Relay termination point, connecting the Site 2 IP network to Router A. This MFR bundle utilizes 2 T1 links for an approximate 3 Mbps bandwidth. Since it is the Frame Relay terminating point and is defined as a DTE frame relay interface, an IP address is assigned to the WAN bundle.

Configure the Router B at Site 2

```
Router/configure# int bundle frame1
Router/configure/interface/bundle frame1# link t1 0/1/0-1
Router/configure/interface/bundle frame1# description "3
Mbps to the Internet"
Router/configure/interface/bundle frame1# encap fr
Router/configure/interface/bundle frame1# fr
Router/configure/interface/bundle frame1/fr# intf_type dte
Router/configure/interface/bundle frame1/fr# lmi ansi
Router/configure/interface/bundle frame1/fr/lmi# keepalive 10
Router/configure/interface/bundle frame1/fr/lmi# exit
Router/configure/interface/bundle frame1/fr# pvc 31
Router/configure/interface/bundle frame1/fr/pvc# shaping cir
3072000 bcmax 3072000 bcmin 1536000
Router/configure/interface/bundle frame1/fr/pvc# ip address
10.0.2.1 255.255.255.0
Router/configure/interface/bundle frame1/fr/pvc# enable
Router/configure/interface/bundle frame1/fr/pvc# exit
```

Configure the Router Interface connecting to Router B

```
Router/configure# int bundle to1400
Router/configure/interface/bundle to1400# link t1 0/2/0-1
Router/configure/interface/bundle to1400# description "3Mbps
MFR to 1400"
Router/configure/interface/bundle to1400# encap fr
Router/configure/interface/bundle to1400# fr
Router/configure/interface/bundle to1400/fr# intf_type dce
Router/configure/interface/bundle to1400/fr# lmi ansi
Router/configure/interface/bundle to1400/fr/lmi# keepalive 10
Router/configure/interface/bundle to1400/fr/lmi# exit
Router/configure/interface/bundle to1400/fr# pvc 31
Router/configure/interface/bundle to1400/fr/pvc# exit 3
```

Verifying and Troubleshooting Commands

The following command shows detailed frame relay bundle interface information.

```
debug# fr bundle-info 'BundleName'
Router/debug# fr bundle-info toRouter
Link State Flags:11100001 00000000 00100001 00100001
Link is Administratively Enabled,Link is Active
LMI is configured
Control Plane is Active
Physical Interface is Up
Bundle is ACTIVE for congestion management
bn_id = 2
bn_name toRouter
bn_state = 2
bn_type = 2
bn_rate = 6144000
bn_no_of_links = 4
bn_no_of_vcs = 2
bn_QmaxCnt = 760
bn_byt_per_tick = 7680
bn_frm_per_tick = 76
bn_bytsent = 0
bn_OFLWcurCnt = 0
bn_rmt_bn_id = wan1
bn_mfr_min_frmsize = 512
bn_mfr_max_frmsize = 1500
bn_mfr_usable_max_frmsize = 1500
bn_mfr_seq_size = 0
bn_class = 3
bn_class_threshold = 2
Router/debug#
```

The following command shows detailed current and max. buffers and other states for all bundles.

```

debug# fr bundle-buffers
Router/debug# fr bundle-buffers

***bundle toRouter,      Tx DE Frames being SENT
      Rx Congestion = none      Tx Congestion = none
Link      MFR State  Rx. Bufs(Max)   Tx Bufs(Cur/Max)
t1 1      Up        0              0/256
t1 2      Up        0              0/256
t1 3      Up        0              0/256
t1 4      Up        0              0/256

***bundle toFRSwit,      Tx DE Frames being SENT
      Rx Congestion = none      Tx Congestion = none
Link      MFR State  Rx. Bufs(Max)   Tx Bufs(Cur/Max)
t1 6      Up        0              0/256
t1 7      Up        0              0/256

***bundle to1400,      Tx DE Frames being SENT
      Rx Congestion = none      Tx Congestion = none
Link      MFR StatRx.   Bufs(Max)   Tx Bufs(Cur/Max)
T3 8      Add Sent    0              0/256

Router/debug#
The following command shows current MFR (FRF.16) states of
links in a bundle.
debug# fr mfr states 'BundleName'
Router/debug# fr mfr states toRouter
Current MFR States for links in Bundle toRouter:
(total links: 4)
t1 1/3      Up
t1 1/2      Up
t1 1/1      Up
t1 1/0      Up
Router/debug#

```

The following command shows dynamic MFR (FRF.16) state machine changes.

```

debug# fr mfr state-machine(enable statemachine changes)
Router/debug# fr mfr state-machine
MFR state machine debug enabled
Router/debug# console
Router/debug# MFR State update on link t1 1/2: OLD state :
Up, event = HELLO, NEW state :Up
MFR State update on link t1 1/3: OLD state : Up, event =
HELLO, NEW state :Up
MFR State update on link t1 1/2: OLD state : Up, event =
HELLO_TIMER_EXP, NEW state :Up
MFR State update on link t1 1/3: OLD state : Up, event =
HELLO_TIMER_EXP, NEW state :Up
MFR State update on link t1 1/2: OLD state : Up, event =
HELLO_ACK, NEW state :Up
MFR State update on link t1 1/3: OLD state : Up, event =
HELLO_ACK, NEW state :Up
MFR State update on link t1 1/1: OLD state : Up, event =
MFR State updHELLOate on link , t1 1/0NEW state :: 0UpLD
state :
UpMFR , event = State updaHELLO_TIMER_EXPte on, NEW state :
link Upt1 1/0
: OLD stateMFR State update on : link Upt1 1/1, ev: OLD
state : ent = UpHELLO, event = , HELLO_TIMER_EXPNEW s,
NEW state :tatep

MFR State update on link t1 1/0: OLD state : Up, event =
HELLO_ACK, NEW state :Up
MFR State update on link t1 1/1: OLD state : Up, event =
HELLO_ACK, NEW state :Up
MFR State update on link t1 0/1/1: OLD state : Add Sent,
event = ACK_TIMER_EXP, NEW state :Add Sent
MFR State update on link t1 0/1/0: OLD state : Add Sent,
event = ACK_TIMER_EXP, NEW state :Add Sent
MFR State update on link t1 1/2: OLD state : Up, event =
HELLO, NEW state :Up
MFR State update on link t1 1/3: OLD state : Up, event =
HELLO, NEW state :Up
MFR State update on link t1 1/2: OLD state : Up, event =
HELLO_TIMER_EXP, NEW state :Up
MFR State update on link t1 1/3: OLD state : Up, event =
HELLO_TIMER_EXP, NEW state :Up
MFR State update on link t1 1/2: OLD state : Up, event =
HELLO_ACK, NEW state :Up

```

```

MFR State update on link t1 1/3: OLD state : Up, event =
HELLO_ACK, NEW state :Up
MFR State update on link t1 1/1: OLD state : Up, event =
HELLO, NEW state :Up
MFR State update on link t1 1/0: OLD state : Up, event =
HELLO, NEW state :Up
MFR State update on link t1 1/0: OLD state : Up, event =
HELLO_TIMER_EXP, NEW state :Up
MFR State update on link t1 1/0: OLD state : Up, event =
HELLO_ACK, NEW state :Up
MFR State update on link t1 1/1: OLD state : Up, event =
HELLO_TIMER_EXP, NEW state :Up
MFR State update on link t1 1/1: OLD state : Up, event =
HELLO_ACK, NEW state :Up
MFR State update on link t1 0/1/1: OLD state : Add Sent,
event = HELLO_TIMER_EXP, NEW state :Add Sent
MFR State update on link t1 0/1/0: OLD state : Add Sent,
event = HELLO_TIMER_EXP, NEW state :Add Sent

```

The following command dumps the lmi packet.

```

debug# fr packet lmi(dump the lmi packets)
Router/debug# fr packet lmi
Router/debug#
>>>RX LMI PKT, MFR bundle: toRouter, link: 64, size = 16

=====START OF PKT DUMP=====
total length of packet = 16

Buf : bp = 0x13398ef0,size = 16,db_ref = 1,rptr = 0x14c2e960
wptr = 0x14c2e970, db_base = 0x14c2e8a8, db_lim=0x14c2f012
( 1)0xc3 ( 2)0x19 ( 3)0x0 ( 4)0x1 ( 5)0x3 ( 6)0x8 ( 7)0x0
( 8)0x75 ( 9)0x95 (10)0x1 (11)0x1 (12)0x1 (13)0x3 (14)0x2
(15)0x8d (16)6

=====END OF PKT DUMP=====

<<<TX LMI PKT, MFR Bundle:toRouter, link: 96, size = 16

```

```

=====START OF PKT DUMP=====
total length of packet = 16

Buf : bp = 0x12cfce40,size = 4,db_ref = 1,rptr = 0x12cfd00c
wptr = 0x
<<<TX LMI12cfd010 PKT, MFR Bu, db_base =
0xndle:1toRouter2cfd00c, lin, db_lim=0xk: 12cfd004c, size =
16(

=1=====STAR)0xT OF PKT DUMP=====c3=====
tot(al length of packet = 216)0x
b2
Buf : bp = 0x(12cfd280 ,s3size = )0x40,db_ref = (1 ,rptr =
0x412c)0xfd44c1
wptr = 0x 12cfd450
Buf : bp = , db_base = 0x0x12cf12cfcc20d44c,size = ,
db_lim=0x1212cfd48,db_ref = c1
,rptr =( 0x 12cfcdee1
wptr )0x= 0xc312cfdfa , (db_base = 0x 12cfd2ec)0x,
db_lim=0xb21 2cfce2c(
(3 )0x50) 0x(3 4)0x 16 )0x
8Buf : bp = 0x 12cfd(060 ,size = 712)0x,0db_ref = 1(rptr =
0x812cfd22e)0x
wpt7dr = 0x 12cfd23a(, db_base = 0x912cfd2)0x2c95,
db_lim=0x 1(2cfd26c10
)0x(1 5)0x113)0x 1( (612)0)0xx18 ((13 )0x73)0 x(014 )0x(2
8)0x1755 )0x(8d 9)0x169)0x58d (len == 1016)0x
1
===== ==END OF PKT DUMP(=====11
)0x1 (12)0x1 (13)0x3 (14)0x2 (15)0x8d (16)0x8c len == 16

=====END OF PKT DUMP=====

<<<TX LMI PKT, FR bundle: toFRSwit, link 2, size = 14

=====START OF PKT DUMP=====
total length of packet = 14

Buf : bp = 0x12cfd280,size = 14,db_ref = 1,rptr = 0x12cfd44c
wptr = 0x12cfd45a, db_base = 0x12cfd44c, db_lim=0x12cfd48c
( 1)0x0 ( 2)0x1 ( 3)0x3 ( 4)0x8 ( 5)0x0 ( 6)0x75 ( 7)0x95
( 8)0x1 ( 9)0x1 (10)0x0 (11)0x3 (12)0x2 (13)0x5 (14)0x0 len
== 14

=====END OF PKT DUMP=====

```



```
Router/debug# fr packet lmi
>>>RX LMI PKT, MFR bundle: toRouter, link: 96, size = 16

=====START OF PKT DUMP=====
total length of packet = 16

Buf : bp = 0x1339c370,size = 16,db_ref = 1,rptra = 0x14c3f440
wptr = 0x14c3f450, db_base = 0x14c3f388, db_lim=0x14c3faf2
( 1)0xc3 ( 2)0x1a ( 3)0x0 ( 4)0x1 ( 5)0x3 ( 6)0x8 ( 7)0x0
( 8)0x75 ( 9)0x95 (10)0x1 (11)0x1 (12)0x1 (13)0x3 (14)0x2
(15)0x8e (16)6

=====END OF PKT DUMP=====
```

The following command dumps FRF.16.1 UNI/NNI MFR control packets.

```
debug# fr packet mfr
Router/debug# fr packet mfr
MFR control packet debug enabled
Router/debug#
Received MFR Control Msg on link t1 1 , current local State:
Up, Rcvd Msg: HELLO

=====START OF PKT DUMP=====
total length of packet = 12

Buf : bp = 0x133a1470,size = 12,db_ref = 1,rptra = 0x14c59003
wptr = 0x14c5900f, db_base = 0x14c58f48, db_lim=0x14c596b2
( 1)0x3 ( 2)0x6 ( 3)0x15 ( 4)0x78 ( 5)0xd3 ( 6)0x54 ( 7)0x5
( 8)0x6 ( 9)0xb6 (10)0x3f (11)0xd (12)0x5f len == 12

=====END OF PKT DUMP=====

Sending MFR Control Msg on link t1 1 , current local State:
Up, Msg type
Sending HELLO_ACKMFR Control
Msg on link
=====t1 2 =====STAR, current local StatT OF PKT
DUMP=====e: =====
Uptota, Msg type l length HELLOof packet =
15
=====STA
RT OF PKT DUMP=====
```

```

Buf : bp = 0x=====12cbbac0=====
,sizetotal length of pack = et = 1515,db_ref
=
Buf : bp = 0x112,rptr = 0xcbb22012cb,size = bc8c15
wptr ,db_ref = = 0x112cbb,rptr = 0xc9b12cbb3e, db_base =
0xc12cbb
wptr = 0xc8c12cbb3f, db_lim=0xb12cbbd8c, db_base = 0x
12cbb(3ec , db_lim=0x112c)0xbb4ece1
(( 12)0)0xx0e1 (( 32)0x)05x 0( (4 )0x33)0x
4( (5 )0x46)0x 3( (6 )0x515)0x 6( (7 )60x)0x5d31
(( 87)0)0xx163a (( 89)0x)x
ea
===== END OF PKT len ==
DUMP=====15=====

Recei
=====Eved MFR Control Msg ND OF PKT
DUMP=====on link =====t1 2 =
, current loc
Sending MFR Controlal State: Msg on liUpnk , Rcvd Msg: t1
HELL01
, current lo
=====STAcac State: RT OF PKTUp DUMP=====,
Msg type ====
HELLtotal length of pack0et =
12
=====
=====START OF PKT
Buf : bp = 0xDUMP==1339aff0=====,size = ==
12total ,db_ref = length of 1packet = ,rptr = 0x1514c39123

wptr = 0
Buf : bp = 0xx12cbb14c3912f7e0, db_base,size = =
0x1514c39,db_ref = 0681, db_l,rptr = 0xim=0x12cbb14c397d29ac

wptr = (0x 12cbb9bb1, db_ba)0xse = 0x312cbb9ac ,
db_lim=0x(12cbbaac
2()0x 61 )0x(e1 3()0x 3a2 )0x(0 4()0 x356)0x
4( (5 )0x498)0x 3( (6 )0x589) 0x(6 7()0x 56 )0x(15 8()0x
67 )0x(5d 9()0x b68 6

=(=====EN12D OF PKT DUMP=====)0x=====

```

The following command shows detailed frame relay virtual circuit information.

```
debug# fr pvc-info 'bundlename' DLCI
Router/debug# fr pvc-info toRouter 16
Bundle status: Enabled
Link is Active
Circuit State Flags:11000000 00000000 00100001 00100001
Circuit : Enabled, InactiveLocally switched, Fwd Node = 0,
Fwd Link = 4, Fwd Dlci = 16
      Rx: Active, Tx: Inactive
      Egress traffic : enabled
      Circuit will FALLBACK upon receiving BECN

Tx Counters:
      Normal      Excess      Hold      Dropped
Packets :
      0            0            0            0
      0            0            0            0
Congestion State : NORMAL ( max rate - fallback if BECN )
  total_fallbacks = 0, total_fallforwards = 0
  cir = 6144000 bc_cur = 6144000, bcmin = 3072000, be = 0
  Tc =      1000, Congestion Monitor Period Timer = 7
  bytes_written_in_current_tc =      0
Router/debug#
```

The following command shows detailed frame relay PVC information.
show inter bundle 'bundlename' DLCI

```
Router# show interface bundle toRouter 16

bundle toRouter
-----
status                up
description            6Mbps MFR to Router
number of links        4
total bandwidth        6144 kbps, utilized : 6144 kbps
link restoral type     automatic
link restoral time     10

link      speed  bw      inverted  status    diffdelay(msec)
-----
t1 1/3    64     1536    no        up        0
t1 1/2    64     1536    no        up        0
t1 1/1    64     1536    no        up        0
t1 1/0    64     1536    no        up        0
```

```

encapsulation          frame relay
  mfr fragment size    1500
  seg. threshold        512
  sequence              short
  differential delay    feature turned off
  bandwidth class      class C, threshold links 2
  hello Timer           10
  ack Timer             7
  ack Retry             5
  mtu                   4096
  RFC1490 fragmentation enabled
  LMI                   ansi(ANSI T1.617 Annex D)
                        dte: keepalive(t391) 10 n392 9
n393 10

                        n391 6
                        dce: t392 15 n392 9 n393 10

  interface type        NNI

Bundle/Interface Counters since last boot/clear
  Rx Frames             503    Rx Invalid Frames      0
  Rx FECNS              0      Rx BECNs           0
  Rx Short Frames       0      Rx Long Frames      0
  Rx Invalid DLCIs      0      Rx Unknown DLCIs   0

  Tx Frames             502

PVC 16
-----
  status                down, pvc's operationally down
  FRF20 Status          frf20 disabled
  shaping(cir-bcmax-bcmin-be) 6144000-6144000-3072000-0
  policing(de-cir-bc-be)  D-6144000-6144000-0
  protocol(s) support    none
switching info
  bundle                toFRSwit
  pvc                   16

counters since last boot/clear
  Bytes Rx              0      Bytes Tx           0
  Packets Rx            0      Packets Tx         0
  Err Packets Rx        0
  Up/Down States        0

```

```

counters for the last five minutes(updated per 15 sec)
  Bytes Rx          0      Bytes Tx          0
  Packets Rx        0      Packets Tx          0
  Err Packets Rx    0
  Up/Down States    0

Router#

```

The following command shows detailed frame relay lmi statistics.
show fr lmistats 'bundlename'

```

Router# show fr lmistats toRouter

LMI Statistics for the DCE Side
  local seq. number: 187, remote seq. number: 187
  RX Status Enquiries          264
  RX Full Status Enquiries     45
  TX Status                    264
  TX Full Status               45

RX Errors:
  Invalid Frame Header         0
  Proto Err In Frame           0
  Unknown LMI Msg              0
  No Report Type IE            0
  No Keep Alive IE             0
  Keep Alive Seq. Loss         0
  Unknown Type IE              0
  Stat. Enq. Poll Rate Too High 0
  Timeout                      0

LMI Statistics for the DTE side
  local seq. number: 187, remote seq. number: 186
  TX Status Enquiries          264
  TX Full Status Enquiries     45
  RX Status                    265
  RX Full Status               45
  RX Updates                   2

RX Errors:
  Invalid Frame Header         0
  Proto Err In Frame           0
  Unknown LMI Msg              0
  No Report Type IE            0

```

No Keep Alive IE	0
Keep Alive Seq. Loss	0
Unknown Type IE	0
Timeout	1
General LMI Error Statistics:	
TX LMI Frame Too Big	0
RX Invalid Frame Headers	0
RX Invalid Info. Frame	0
RX Invalid Msg. Rcvd	0
RX Unexpected PVC Stat. IE	0
Router#	

The following command shows detailed frame relay PVC statistics.
show fr vcstats 'bundlename' DLCI

```
Router# show fr vcstats toRouter 16
```

RX Normal Frames	0
RX Octets normal	0
RX Framesin excess of Bc	0
RX Octets in excess of Bc	0
RX Frames over Bc + Be	0
RX Octets over Bc + Be	0
Frames dropped	0
Octets dropped	0
Frames dropped with DE bit set	0
Octets dropped with DE bit set	0
Frames with DE bit set	0
Octets with DE bit set	0
Frames in which RX set the DE bit	0
Octets in which RX set the DE bit	0

```
Router#
```



CHAPTER 5. PPPoFR and MLPPPoFR

The PPP over Frame Relay (PPPoFR) feature allows a router to establish end-to-end Point-to-Point Protocol (PPP) sessions over Frame Relay regardless of media type in the middle of network. IP datagrams are transported over the PPP layer using RFC 1973 compliant Frame Relay framing. This feature is useful for remote users running PPP to access their corporate networks through Frame Relay networks.

A PPP connection is established over a Frame Relay permanent virtual circuit (PVC). The PPP session will not be in an 'UP' state unless the associated Frame Relay PVC is in an 'UP' state. The Frame Relay PVC can coexist with other circuits using different Frame Relay encapsulation methods, such as RFC 1490 and bridging mode over the same Frame Relay link. One can establish a bigger bandwidth pipe by using multi-link PPP over Frame Relay (MLPPPoFR) as well.



NOTE

Restrictions:

- Only Frame Relay PVCs are supported.
- Only the Internet Protocol (IP) is supported.
- Up to 100 PPP over Frame Relay Interface are supported in an iBG router.
- Up to 30 PVCs can be bound to a MLPPPoFR interface.

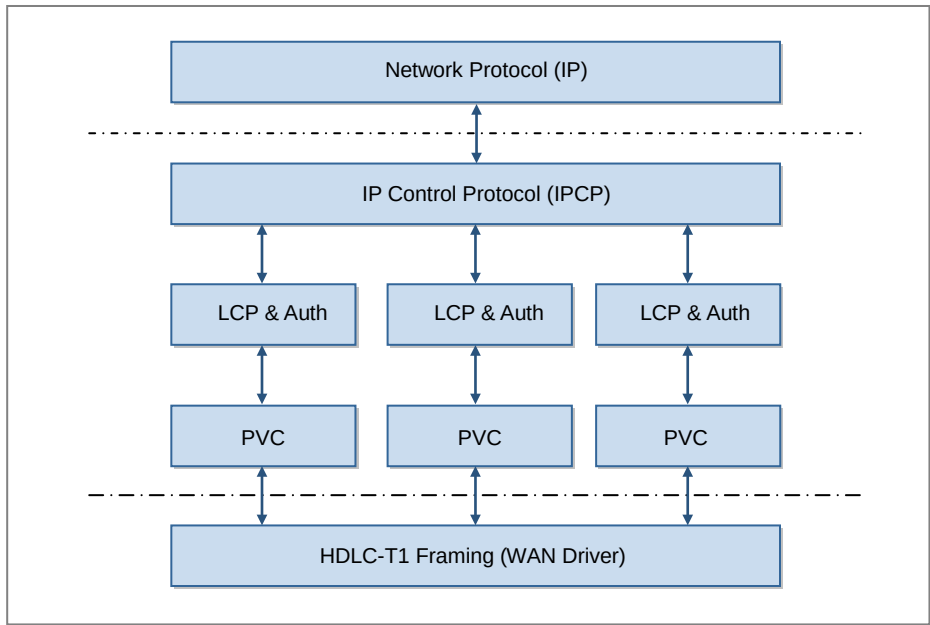


Figure 5.1 Overview of PPPoFR

PPPoFR is comprised of 3 main components: Framing, LCP, and NCP as shown in Figure 5.1.

PVC indicates a Frame Relay circuit.

A Link Control Protocol (LCP) is used to establish, configure and test a data-link connection. More detailed information can be found in RFC 1661.

A family of Network Control Protocols (NCPs) are used to establish and configure different network layer protocols. For each network protocol, a corresponding NCP should be used. For example, IPCP is used for IP networks and XNSCP is used for XNS network.

Optionally, before PPP NCP is established, peers may need to authenticate each other and in such a case an authentication failure may result in the link termination.

There are two authentication protocols:

- PAP (Password Authentication Protocol)
- CHAP (Challenge Handshake Authentication Protocol)

Protocol Configuration

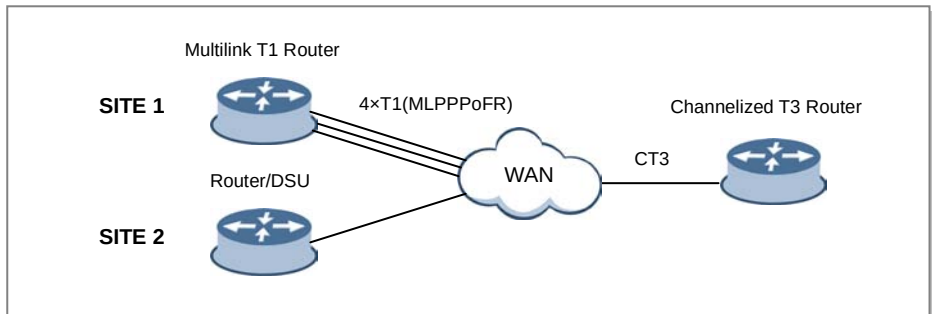


Figure 5.2 MLPPPoFR deployment scenario

1. Site 1 uses a multilink T1 router to establish a 6 Mbps MLPPP connection over four T1 PVC lines to the main site. Each PVC is a Frame Relay circuit.
2. Site 2 uses a router to connect to the main site over a single T1 PVC link with PPP encapsulation. The PVC is a Frame Relay circuit.

PPPoFR Configuration

This section shows how to configure the router at Site 2 with PPPoFR.

Configuring Ubigate iBG router at Site 2

Step-by-Step Configuration

Step	Command	Purpose
1	Router# configure terminal	Goes into the terminal configuration mode.
2	Router/configure# interface bundle [<i>bundle name</i>]	Sets a bundle interface. ' <i>bundle name</i> ' represents a specific bundle interface to be configured at the moment. It means Frame Relay bundle.
3	Router/configure/bundle/[<i>bundle name</i>]# link t1 0/0	Links a channelized T1 interface to a Frame Relay bundle interface
4	Router/configure/bundle/[<i>bundle name</i>]# encapsulation fr	Selects Frame Relay as an encapsulation method.

(Continued)

Step	Command	Purpose
5	Router/configure# interface pppofr [pppofr name]	Sets a pppofr interface. 'pppofr name' represents a specific pppofr interface to be configured at the moment
6	Router/configure/pppofr/[pppofr name]# add_vc [DLCI] [bundle name]	Binds a PVC to pppofr Interface. 'bundle name' represents a Frame Relay bundle.
7	Router/configure/pppofr/[pppofr name]# ppp_type [PPP TYPE]	'PPP TYPE' can be ppp or mlppp as an encapsulation method.
8	Router/configure/pppofr/[pppofr name]# ip address [IP address] { [bit mask] [number of bits for mask] }	Sets an IP address for the interface.
9	Router/configure/pppofr/[pppofr name]# ip negotiated	Sets an IP address on the pppofr interface after acquiring the IP address from the peer.
10	Router/configure/pppofr/[pppofr name]# exit	Returns to the upper configuration mode.

Configuration Example

```

DUT10/configure# interface bundle fr1
configuring new WAN bundle interface fr1
DUT10/configure/interface/bundle fr1# link t1 0/0
DUT10/configure/interface/bundle fr1# encapsulation frelay
DUT10/configure/interface/bundle fr1# fr
DUT10/configure/interface/bundle fr1/fr# intf_type dce
DUT10/configure/interface/bundle fr1/fr# pvc 100
new pvc created
pvc's default cir set to 1536000 bps
DUT10/configure/interface/bundle fr1/fr/pvc 100# exit
DUT10/configure/interface/bundle fr1/fr# exit 3
DUT10/configure# interface pppofr pppofr1
configuring new pppofr interface pppofr1
DUT10/configure/interface/pppofr pppofr1# add_vc 100 fr1
DUT10/configure/interface/pppofr pppofr1# ppp_type ppp
DUT10/configure/interface/pppofr pppofr1# ip address
143.23.12.2 255.255.255.0
*Jan 11,2000,03:14:09 #IPMUXc-notification: <samsung> IP
address(143.23.12.2) is added <OK>
DUT10/configure/interface/pppofr pppofr1#
DUT10/configure/interface/pppofr pppofr1# ip negotiated
DUT10/configure/interface/pppofr pppofr1#

```

MLPPPoFR Configuration

This section shows how to configure the router at site 1 with MLPPPoFR.

Configuring Ubigate iBG router at Site 1

Step-by-Step Configuration

Step	Command	Purpose
1	Router# configure terminal	Goes into the terminal configuration mode.
2	Router/configure# interface bundle [<i>bundle name</i>]	Sets a bundle interface. ' <i>bundle name</i> ' represents a specific bundle interface to be configured at the moment. It means Frame Relay bundle.
3	Router/configure/bundle/[<i>bundle name</i>]# link t1 0/0	Links a channelized T1 interface to a Frame Relay bundle interface
4	Router/configure/bundle/[<i>bundle name</i>]# encapsulation fr	Selects Frame Relay as an encapsulation method.
5	Router/configure# interface pppofr [<i>pppofr name</i>]	Sets a pppofr interface. ' <i>pppofr name</i> ' represents a specific pppofr interface to be configured at the moment
6	Router/configure/pppofr/[<i>pppofr name</i>]# add_vc [DLCI] [<i>bundle name</i>]	Binds a PVC to pppofr Interface. ' <i>bundle name</i> ' represents a Frame Relay bundle.
7	Router/configure/pppofr/[<i>pppofr name</i>]# ppp_type [PPP TYPE]	'PPP TYPE' can be ppp or mlppp as an encapsulation method.
8	Router/configure/pppofr/[<i>pppofr name</i>]# ip address [IP address] { [bit mask] [number of bits for mask] }	Sets an IP address for the interface.
9	Router/configure/pppofr/[<i>pppofr name</i>]# ip negotiated	Sets an IP address on the pppofr interface after acquiring the IP address from the peer.
10	Router/configure/pppofr/[<i>pppofr name</i>]# exit	Returns to the upper configuration mode.

Configuration Example

```
DUT10/configure# interface bundle fr1
configuring new WAN bundle interface fr1
DUT10/configure/interface/bundle fr1# link t1 0/0
DUT10/configure/interface/bundle fr1# encapsulation frelay
DUT10/configure/interface/bundle fr1# fr
DUT10/configure/interface/bundle fr1/fr# intf_type dce
DUT10/configure/interface/bundle fr1/fr# pvc 100
new pvc created
pvc's default cir set to 1536000 bps
DUT10/configure/interface/bundle fr1/fr/pvc 100# exit 3
DUT10/configure# interface bundle fr2
configuring new WAN bundle interface fr2
DUT10/configure/interface/bundle fr2# link t1 0/1
DUT10/configure/interface/bundle fr2# encapsulation frelay
DUT10/configure/interface/bundle fr2# fr
DUT10/configure/interface/bundle fr2/fr# intf_type dce
DUT10/configure/interface/bundle fr2/fr# pvc 200
new pvc created
pvc's default cir set to 1536000 bps
DUT10/configure/interface/bundle fr2/fr/pvc 200# exit 3
DUT10/configure# interface bundle fr3
configuring new WAN bundle interface fr3
DUT10/configure/interface/bundle fr3# link t1 0/2
DUT10/configure/interface/bundle fr3# encapsulation frelay
DUT10/configure/interface/bundle fr3# fr
DUT10/configure/interface/bundle fr3/fr# intf_type dce
DUT10/configure/interface/bundle fr3/fr# pvc 300
new pvc created
pvc's default cir set to 1536000 bps
DUT10/configure/interface/bundle fr3/fr/pvc 300# exit 3
DUT10/configure# interface bundle fr4
configuring new WAN bundle interface fr4
DUT10/configure/interface/bundle fr4# link t1 0/3
DUT10/configure/interface/bundle fr4# encapsulation frelay
DUT10/configure/interface/bundle fr4# fr
DUT10/configure/interface/bundle fr4/fr# intf_type dce
DUT10/configure/interface/bundle fr4/fr# pvc 400
new pvc created
pvc's default cir set to 1536000 bps
DUT10/configure/interface/bundle fr4/fr/pvc 400#
DUT10/configure/interface/bundle fr4/fr/pvc 400# exit 4
DUT10/configure# interface pppofr mlpppofr
configuring new pppofr interface mlpppofr
DUT10/configure/interface/pppofr mlpppofr# add_vc 100 fr1
DUT10/configure/interface/pppofr mlpppofr# add_vc 200 fr2
DUT10/configure/interface/pppofr mlpppofr# add_vc 300 fr3
DUT10/configure/interface/pppofr mlpppofr# add_vc 400 fr4
DUT10/configure/interface/pppofr mlpppofr# ppp_type mlppp
DUT10/configure/interface/pppofr mlpppofr# ip negotiated
```

Verifying and Troubleshooting Commands

To troubleshoot a PPPoFR configuration and operation, use the following commands:

```
Router# show interface pppofr <pppofr_name>
Router# show interface bundle <bundle_name>
Router# show interface pppofrs
```

The following shows how to get information about a pppofr interface and a Frame Relay bundle.

```
DUT10# show interface pppofr mlpppofr

pppofr mlpppofr
-----
status                               Down

Ipv4 status                          Down

number of pvcs                       4
total bandwidth                      6144 kbps

Bound PVCs Info : 4 PVCs

VC(DLCI)   BUNDLE   STATUS   BANDWIDTH(bps)
-----
    100     fr1      DOWN    1536000
    200     fr2      DOWN    1536000
    300     fr3      DOWN    1536000
    400     fr4      DOWN    1536000

encapsulation                          mlppp
  mtu                                64-1500-8192
  mru                                64-1500-8192
  mrru                              1500-1524-8192
  sequence                          long
  seg_threshold                      512
  differential delay                 0
  discriminator                     2013695163
  minimum_pvcs                       1
```

```

Negotiated ppp pppofrbundle values
    negotiated mru          1500
    negotiated mrru         1524
    negotiated mtu          1524

LFI parameters configured
    interleave -- no

Authentication parameters
    authentication-database -- local
    authentication-server -- none
    accept pap-request -- no
    send  pap-request -- no
    accept chap-challenge -- no
    send  chap-challenge -- no

PPP Timers
    Echo Timer              5
    Restart Timer           3

ip info
    ipaddr                  0.0.0.0
    netmask                  255.255.255.254

RED Information
-----
WRED Status: Disabled    DS-RED Status: Disabled

Current queue size      = 0          Maximum queue size      = 0
Current avg queue size = 0          Maximum avg queue size = 0
Current Q size for WRED= 0
Q overflows = 0

WRED Configuration:
Wq Bias Factor : 5
-----+-----+-----
      color      min      max      mpd
      threshold threshold
-----+-----+-----
      green      69      109      5
      yellow     46      80      5
      red        23      57      5

```

WRED Counters:

Color	Pkts Fwd Below Minth	Pkts Fwd Minth-Maxth	Pkts Dropd Minth-Maxth	Pkts Dropd Above Maxth	Ctrl Pkts
green	0	0	0	0	0
yellow	0	0	0	0	0
red	0	0	0	0	0

DUT10# show interface bundle fr1

bundle fr1

```

-----
status                               down
number of links                      1
total bandwidth                      1536 kbps, utilized : 1536 kbps

```

```

link          speed bw    inverted status
diffdelay(msec)
-----
t1            0/0   64    1536   no    down    -
                                     fr negotiation failed

```

```

encapsulation          frame relay
  mtu                  1500
  fragmentation_len    1500
  fragmentation        disabled
  shaping              disabled
  pvc-priority         disabled
  LMI                  ansi(ANSI T1.617 Annex D)
                     keepalive(t392) 15 n392 3 n393 4
  interface type       DCE

```

Bundle/Interface Counters since last boot/clear

```

Rx Frames              0    Rx Invalid Frames    0
Rx FECNS               0    Rx BECNS           0
Rx Short Frames        0    Rx Long Frames    0
Rx Invalid DLCIs       0    Rx Unknown DLCIs  0

Tx Frames              0

```

```

PVC 100
-----
    status                down, pvc's operationally down
    FRF20 Status          frf20 disabled
    shaping(cir-bcmax-bcmin-be) 1536000-768000-65536-0
    queue size for shaping    0
    policing              disabled
    priority              none
    protocol(s) support     none
counters since last boot/clear
    Bytes Rx              0    Bytes Tx              0
    Packets Rx            0    Packets Tx            0
    Err Packets Rx        0
    Up/Down States        0

counters for the last five minutes(updated per 15 sec)
    Bytes Rx              0    Bytes Tx              0
    Packets Rx            0    Packets Tx            0
    Err Packets Rx        0
    Up/Down States        0

DUT10# show interface pppofrs
pppofr  bw(kbps) availbw(kbps) NumOfPvcs ppp_type status
=====
mlpppofr 6144    0            4            MLPPP    DOWN

-----
In total 1 pppofr exists in system
DUT10#

```

```

Router# debug ppp negotiation

```


The following shows how to get the LCP and IPCP debug information.

```
DUT10# debug ppp negotiation
WARNING! Enabling PPP Debug can impair system performance.
Do you want to continue?(Y/N)
Negotiation debug enabled
DUT10# debug console
---- msgcnt(1) size(25) dumped-----
LcpTimeout: Link:0x980005 rstrtcount:14431
LcpScr:link:0x980005 LCPEvent:T0+ @S6(St_ReqSent) ->
S6(St_ReqSent)
0 LcpPrepareToScr: Link: 980005, My magic #: 4CD07653
0 LcpPrepareToScr: Link: 980005, EPD len:7 class:2 0x78 0x6
0x8c 0xbb
t:0x1 l:4 v:0x5:0xdc:0x5:0x6
t:0x5 l:6 v:0x4c:0xd0:0x76:0x53
t:0x11 l:4 v:0x5:0xf4:0x13:0x7
t:0x13 l:7 v:0x2:0x78:0x6:0x8c
0 LCP Configure Request (Sending) :
---- dumping PPP packet mp = 0x17c17620: -----
0x1 0x2 0x0 0x19 0x1 0x4 0x5 0xdc 0x5 0x6 0x4c 0xd0 0x76 0x53
0x11 0x4 0x5 0xf4 0x13 0x7 0x2 0x78 0x6 0x8c 0xbb
---- msgcnt(1) size(25) dumped-----
LcpTimeout: Link:0x980002 rstrtcount:14430
LcpScr:link:0x980002 LCPEvent:T0+ @S6(St_ReqSent) ->
S6(St_ReqSent)
0 LcpPrepareToScr: Link: 980002, My magic #: 05CB5DA1
0 LcpPrepareToScr: Link: 980002, EPD len:7 class:2 0x78 0x6
0x8c 0xbb
t:0x1 l:4 v:0x5:0xdc:0x5:0x6
t:0x5 l:6 v:0x5:0xcb:0x5d:0xa1
t:0x11 l:4 v:0x5:0xf4:0x13:0x7
t:0x13 l:7 v:0x2:0x78:0x6:0x8c
0 LCP Configure Request (Sending) :
---- dumping PPP packet mp = 0x17c17620: -----
0x1 0x2 0x0 0x19 0x1 0x4 0x5 0xdc 0x5 0x6 0x5 0xcb 0x5d 0xa1
0x11 0x4 0x5 0xf4 0x13 0x7 0x2 0x78 0x6 0x8c 0xbb
---- msgcnt(1) size(25) dumped-----
LcpTimeout: Link:0x980003 rstrtcount:14430
LcpScr:link:0x980003 LCPEvent:T0+ @S6(St_ReqSent) ->
S6(St_ReqSent)
0 LcpPrepareToScr: Link: 980003, My magic #: 24C10A34
0 LcpPrepareToScr: Link: 980003, EPD len:7 class:2 0x78 0x6
0x8c 0xbb
t:0x1 l:4 v:0x5:0xdc:0x5:0x6
t:0x5 l:6 v:0x24:0xc1:0xa:0x34
t:0x11 l:4 v:0x5:0xf4:0x13:0x7
t:0x13 l:7 v:0x2:0x78:0x6:0x8c
```

```

0 LCP Configure Request (Sending) :
---- dumping PPP packet mp = 0x17c17620: -----
0x1 0x2 0x0 0x19 0x1 0x4 0x5 0xdc 0x5 0x6 0x24 0xc1 0xa 0x34
0x11 0x4 0x5 0xf4 0x13 0x7 0x2 0x78 0x6 0x8c 0xbb
---- msgcnt(1) size(25) dumped-----
LcpTimeout: Link:0x980004 rstrtcount:14430
LcpScr:link:0x980004 LCPEvent:T0+ @S6(St_ReqSent) ->
S6(St_ReqSent)
0 LcpPrepareToScr: Link: 980004, My magic #: 115E44B2
0 LcpPrepareToScr: Link: 980004, EPD len:7 class:2 0x78 0x6
0x8c 0xbb
t:0x1 l:4 v:0x5:0xdc:0x5:0x6
t:0x5 l:6 v:0x11:0x5e:0x44:0xb2
t:0x11 l:4 v:0x5:0xf4:0x13:0x7
t:0x13 l:7 v:0x2:0x78:0x6:0x8c
0 LCP Configure Request (Sending) :
---- dumping PPP packet mp = 0x17c17620: -----
0x1 0x2 0x0 0x19 0x1 0x4 0x5 0xdc 0x5 0x6 0x11 0x5e 0x44 0xb2
0x11 0x4 0x5 0xf4 0x13 0x7 0x2 0x78 0x6 0x8c 0xbb
---- msgcnt(1) size(25) dumped-----
LcpTimeout: Link:0x980005 rstrtcount:14430
LcpScr:link:0x980005 LCPEvent:T0+ @S6(St_ReqSent) ->
S6(St_ReqSent)
0 LcpPrepareToScr: Link: 980005, My magic #: 03C48B38
0 LcpPrepareToScr: Link: 980005, EPD len:7 class:2 0x78 0x6
0x8c 0xbb
t:0x1 l:4 v:0x5:0xdc:0x5:0x6
t:0x5 l:6 v:0x3:0xc4:0x8b:0x38
t:0x11 l:4 v:0x5:0xf4:0x13:0x7
t:0x13 l:7 v:0x2:0x78:0x6:0x8c
0 LCP Configure Request (Sending) :
---- dumping PPP packet mp = 0x17c17620: -----
0x1 0x2 0x0 0x19 0x1 0x4 0x5 0xdc 0x5 0x6 0x3 0xc4 0x8b 0x38
0x11 0x4 0x5 0xf4 0x13 0x7 0x2 0x78 0x6 0x8c 0xbb
---- msgcnt(1) size(25) dumped-----
LcpTimeout: Link:0x980002 rstrtcount:14429
LcpScr:link:0x980002 LCPEvent:T0+ @S6(St_ReqSent) ->
S6(St_ReqSent)
0 LcpPrepareToScr: Link: 980002, My magic #: 7B1406D1
0 LcpPrepareToScr: Link: 980002, EPD len:7 class:2 0x78 0x6
0x8c 0xbb
t:0x1 l:4 v:0x5:0xdc:0x5:0x6
t:0x5 l:6 v:0x7b:0x14:0x6:0xd1
t:0x11 l:4 v:0x5:0xf4:0x13:0x7
t:0x13 l:7 v:0x2:0x78:0x6:0x8c
0 LCP Configure Request (Sending) :
---- dumping PPP packet mp = 0x17c17620: -----
0x1 0x2 0x0 0x19 0x1 0x4 0x5 0xdc 0x5 0x6 0x7b 0x14 0x6 0xd1

```

```

0x11 0x4 0x5 0xf4 0x13 0x7 0x2 0x78 0x6 0x8c 0xbb
---- msgcnt(1) size(25) dumped-----
LcpTimeout: Link:0x980003 rstrtcount:14429
LcpScr:link:0x980003 LCPEvent:T0+ @S6(St_ReqSent) ->
S6(St_ReqSent)
0 LcpPrepareToScr: Link: 980003, My magic #: 17C4C973
0 LcpPrepareToScr: Link: 980003, EPD len:7 class:2 0x78 0x6
0x8c 0xbb
t:0x1 l:4 v:0x5:0xdc:0x5:0x6
t:0x5 l:6 v:0x17:0xc4:0xc9:0x73
t:0x11 l:4 v:0x5:0xf4:0x13:0x7
t:0x13 l:7 v:0x2:0x78:0x6:0x8c
0 LCP Configure Request (Sending) :
---- dumping PPP packet mp = 0x17c17620: -----
0x1 0x2 0x0 0x19 0x1 0x4 0x5 0xdc 0x5 0x6 0x17 0xc4 0xc9 0x73
0x11 0x4 0x5 0xf4 0x13 0x7 0x2 0x78 0x6 0x8c 0xbb
---- msgcnt(1) size(25) dumped-----
LcpTimeout: Link:0x980004 rstrtcount:14429
LcpScr:link:0x980004 LCPEvent:T0+ @S6(St_ReqSent) ->
S6(St_ReqSent)
0 LcpPrepareToScr: Link: 980004, My magic #: 2755800A
0 LcpPrepareToScr: Link: 980004, EPD len:7 class:2 0x78 0x6
0x8c 0xbb
t:0x1 l:4 v:0x5:0xdc:0x5:0x6
t:0x5 l:6 v:0x27:0x55:0x80:0xa
t:0x11 l:4 v:0x5:0xf4:0x13:0x7
t:0x13 l:7 v:0x2:0x78:0x6:0x8c
0 LCP Configure Request (Sending) :
---- dumping PPP packet mp = 0x17c17620: -----
0x1 0x2 0x0 0x19 0x1 0x4 0x5 0xdc 0x5 0x6 0x27 0x55 0x80 0xa
0x11 0x4 0x5 0xf4 0x13 0x7 0x2 0x78 0x6 0x8c 0xbb
---- msgcnt(1) size(25) dumped-----
LcpTimeout: Link:0x980005 rstrtcount:14429
LcpScr:link:0x980005 LCPEvent:T0+ @S6(St_ReqSent) ->
S6(St_ReqSent)
0 LcpPrepareToScr: Link: 980005, My magic #: 3E6EDA23
0 LcpPrepareToScr: Link: 980005, EPD len:7 class:2 0x78 0x6
0x8c 0xbb
t:0x1 l:4 v:0x5:0xdc:0x5:0x6
t:0x5 l:6 v:0x3e:0x6e:0xda:0x23
t:0x11 l:4 v:0x5:0xf4:0x13:0x7
t:0x13 l:7 v:0x2:0x78:0x6:0x8c
0 LCP Configure Request (Sending) :
---- dumping PPP packet mp = 0x17c17620: -----
0x1 0x2 0x0 0x19 0x1 0x4 0x5 0xdc 0x5 0x6 0x3e 0x6e 0xda 0x23
0x11 0x4 0x5 0xf4 0x13 0x7 0x2 0x78 0x6 0x8c 0xbb
---- msgcnt(1) size(25) dumped-----
LcpTimeout: Link:0x980002 rstrtcount:14428

```

```

LcpScr:link:0x980002 LCPEvent:T0+ @S6(St_ReqSent) ->
S6(St_ReqSent)
0 LcpPrepareToScr: Link: 980002, My magic #: 388094D5
0 LcpPrepareToScr: Link: 980002, EPD len:7 class:2 0x78 0x6
0x8c 0xbb
t:0x1 l:4 v:0x5:0xdc:0x5:0x6
t:0x5 l:6 v:0x38:0x80:0x94:0xd5
t:0x11 l:4 v:0x5:0xf4:0x13:0x7
t:0x13 l:7 v:0x2:0x78:0x6:0x8c
0 LCP Configure Request (Sending) :
---- dumping PPP packet mp = 0x17c17620: -----
0x1 0x2 0x0 0x19 0x1 0x4 0x5 0xdc 0x5
---- msgcnt(1) size(10) dumped-----
I NcpConverge(ncp:0xff020000,ev:RCR+):IPADDRESS specified:
0xc0a80301
NcpSca:ncp:0xff020000 NCPEvent:RCR+ @S6(St_ReqSent) ->
S8(St_AckSent)
0 IPCP Configure Ack (Sending) :
---- dumping PPP packet mp = 0x114afdd0: -----
0x2 0x5 0x0 0xa 0x3 0x6 0xc0 0xa8 0x3 0x1
---- msgcnt(1) size(10) dumped-----
I IPCP Configure Ack received:
---- dumping PPP packet mp = 0x11b7cc20: -----
0x2 0x3 0x0 0xa 0x3 0x6 0xc0 0xa8 0x3 0x2
---- msgcnt(1) size(10) dumped-----
ppp-ipcp: stopping the ncp-conf-req timer for link 0xff020000
NcpIrc:ncp:0xff020000 NCPEvent:RCA @S8(St_AckSent) ->
S9(St_Opened)
NcpLyrUp:ncp:0xff020000 NCPEvent:RCA @S8(St_AckSent) ->
S9(St_Opened)
Sending an L2_UP event to IPMUX with local addr: c0a80302
peeraddr: c0a80301 mtu: 250
*Oct 19,2000,23:32:43 #PPP-nLcpSerotification: b bundle(undle
UP : PPPPPP) link(0) status updated with "UP"

*Oct 19,2000,23:32:43 #IPMUX-notification: IP received an
L2_UP on bundle PPP mtu 250 peer: 192.168.3.1
LcpSer bundle(PPP) link(0) status updated with "UP"
LcpSer bundle(PPP) link(0) status updated with "UP"

Router#

```

```
Router# debug mlpinf <pppofr name>
```

The following shows how to get MLPPP debug Information

```
Router# debug ppp mlpinfo MLPPP
*****
*****
Bundle #: 2      Structure ptr: 1D7019F0      Last timestamp: 1
Tx sequence #: 0x00000000      Rx begin sequence:
0xFFFFFFFF
Rx begin offset: 0x00000000      Rx end offset: 0x00001000
Rx max sequence: 0xFFFFFFFF      Fragment Mask: 0x00000000
PPP/FR Rx Seq Modulo: 0x00FFFFFF(long)
PPP/FR Tx Seq Modulo: 0x00FFFFFF(long)
Ring buffer modulo: 0x0FFF
Fragment buffer start: 0x1D702FF0  Ring buffer start:
0x1d701fe0
Min. tx size(Seg threshold)=1400, Max_tx_size(Peer MRU)
=1500, Active Links=4
ML Bundle Links Information:
  Link #   Link Ptr  Data Xfer OK  Last Seq Recv  Tx Bytes
  Frags
-----
00000000  0802F210  Yes           FFFFFFFF      0             0
00000001  0802D0B0  Yes           FFFFFFFF      0             0
00000002  0802B050  Yes           FFFFFFFF      0             0
00000003  0801E9A0  Yes           FFFFFFFF      0             0
```



This page is intentionally left blank.

PART III. Switching and Routing Protocols



- CHAPTER 1. Layer-2 Switching
- CHAPTER 2. DHCP Relay
- CHAPTER 3. Static Routing
- CHAPTER 4. RIP
- CHAPTER 5. RIPng
- CHAPTER 6. OSPF
- CHAPTER 7. OSPFv3
- CHAPTER 8. BGP
- CHAPTER. 9. BGP4+
- CHAPTER 10. Multicast Protocols
- CHAPTER 11. VRRP
- CHAPTER 12. QoS



CHAPTER 1. Layer-2 Switching

Layer 2 LAN Switching and Bridging

Local Area Network (LAN) is a data communications network connecting terminals, computers and printers within a building or other geographically limited areas. These devices could be connected through wired cables or wireless links. Ethernet and Token Ring are examples of standard LAN technologies. LAN switching involves examining of physical network addresses that uniquely identifies a device in the network. LAN bridging allows extension of LAN by supporting connection of multiple LAN segments. MAC addresses of the datagram that flow through bridges are examined to build a table of known destinations. If the destination of a datagram is on the same segment as the source of the datagram, the bridge drops the datagram because forwarding is not required. However, if the destination is on another segment, the bridge transmits the datagram on that segment only. If the bridge does not know the destination segment, it transmits the datagram on all segments except the source segment (a technique known as flooding).

IEEE 802.1d-Media Access Control (MAC) Bridging and Spanning-Tree Protocol

Mac Bridging allows multiple Local Area Networks (LANs) to be connected together. Transparent bridging involves the creation of MAC address tables, and limits the Ethernet collision domain by filtering data sent between LAN segments. This reduces network congestion and allows networks to be partitioned for administrative purposes.

The Spanning Tree Protocol (STP) calculates the best path between 2 stations while preventing loops when multiple paths are available. Multiple paths among LAN switches are desirable for redundancy purpose. However, with multiple paths messages will be duplicated if loops are not care for.

STP defines a tree that spans all switches in an extended network.

All participating switches in an extended LAN sends Bridge Protocol Data Unit (BPDU) messages that communicate information on ports, addresses, priorities and costs. A switch is elected as the root bridge based on MAC address and priority value. All ports on the root bridge are assigned as designated ports. All other bridges determine the lowest cost path (the best path) to get to the root bridge, and assign that port as designated port. On non-root bridges only one port can be designated. The designated port is moved into Forwarding State while all remaining switch ports are considered as redundant and are placed in Blocking State. The spanning tree algorithm reconfigures the spanning tree topology if STP costs change, or if one network segment in the STP becomes unreachable.

IEEE 802.1s-Multiple Spanning Tree

In a network where multiple links are used to separate VLAN traffic, the use of STP could cause certain data paths to be disabled. 802.1S Multiple Spanning Tree Protocol (MSTP) resolves the problem by supporting multiple spanning trees within a network. The standard lets administrators assign VLAN traffic to unique paths. With this feature load balancing can be achieved through assigning multiple VLANs to 2 distinct paths.

With MSTP each VLAN is mapped to an instance of a MSTP. Moving bridge ports into blocking state will cause blocking of specific VLAN traffic and not the entire link.

VLAN (Virtual LAN)

VLAN is a logical group of LAN segments, independent of physical location, with a common set of requirements. Broadcast traffic is only propagated in a same the VLAN. The VLAN forwarding feature has the added benefit of being able to support non-IP traffic since all traffic is forwarded based only on the Layer 2 VLAN tag. Although iBG routers do not communicate using non-IP Layer 3 protocols, they can forward these protocols using VLAN tag.

The VLAN interface provides in-band communication with the iBG router as well as the Ethernet switches while remaining separate from customer traffic. An iBG router will examine the destination IP address of any packets received on the management VLAN. If the destination is an iBG router, the address of the packet will be forwarded to the IP layer for local processing. If the address does not match the address of the iBG router, the packet will be forwarded to all configured interfaces for the VLAN with the exception of the interface where it was received. This allows all transmission equipment to be managed in a single, flat VLAN.

The routing protocol, IP switching and other high-level applications are supported on the VLAN interface which are also supported on other interfaces. iBG router supports VLAN-based data forwarding. Essentially, this feature forwards the packets from one network to another based on the VLAN identifier (rather than routing) contained in the VLAN header, as defined by IEEE 802.1q. The VLAN packets are generally termed as tagged packets referring to the VLAN encapsulation of the Ethernet packets.

IGMP Snooping

The Internet Group Management Protocol (IGMP) is a layer-3 protocol used by IP hosts to report multicast information to neighboring multicast routers. IGMP snooping allows a Layer-2 router or switch to read (snoop) IGMP packets transferred between IP Multicast Routers and IP Multicast hosts to learn the IP Multicast group membership. IGMP snooping allows the Layer-2 device to forward only that multicast traffic that is addressed to ports in its own multicast group. Without IGMP snooping, multicast traffic is forwarded to all ports. This reduces multicast traffic through the Layer-2 device. IGMP snooping drops all but one of the host join messages per multicast group and only forwards this one join message to the multicast router.

Layer2 Features Configuration

This section shows a configuration example for Multiple Spanning Tree Protocol (MSTP) with VLAN.

MSTP and VLAN Configurations

Configuring MST

The following example shows the general steps needed to configure Bridge, MSTP and VLAN

Step-by-Step Configuration

Step	Command	Purpose
1	Router# configure terminal	Enters the terminal configuration mode.
2	Router/configure# bridge 1 protocol mstp	Create the bridge 1 with MSTP. Only one bridge can be created in a system with bridge ID 1. After executing this command, the default VLAN (ID=1) is also created automatically.
3	Router/configure# vlan database	Enters VLAN database mode.
4	Router/configure/vlan/database# vlan [vlan number] bridge 1	Create new VLAN in a bridge. Repeats as many as required. vlan_number: ranges 2 to 4000 4001-4094 are reserved as the internal purpose.
5	Router/configure/vlan/database# exit	Exits VLAN database mode.
6	Router/configure# span mst conf	Enters MST configuration mode.
7	Router/configure/spanning-tree/mst# bridge 1 instance [instance number] vlan [vlan number]	Associates an instance with VLAN. Repeats as many as required. instance number: ranges 1 to 15.
8	Router/configure/spanning-tree/mst# exit	Exits MST configuration mode.
9	Router/configure# interface [interface name]	Enters interface configuration mode.

(Continued)

Step	Command	Purpose
10	Router/configure/interface/[<i>interface name</i>] # switchport	Sets the interface as a switch port.
11	Router/configure/interface/[<i>interface name</i>] # bridge-group 1	Includes this interface in a bridge group.
12	Router/configure/interface/[<i>interface name</i>] # bridge-group 1 instance [<i>instance number</i>]	(Optional) Attach this interface to an instance. In case a VLAN is associated with the instance and the interface is a member of the VLAN, this command must be executed for correct VLAN switching.
13	Router/configure/interface/[<i>interface name</i>] # bridge-group 1 instance [<i>instance number</i>] priority [<i>priority number</i>]	(Optional) Assigns priority. priority number: ranges 0 to 240.
14	Router/configure/interface/[<i>interface name</i>] # end	Return to the 'Router#' prompt.
15	Router# show span mst [detail]	Shows spanning-tree information.

Configuring VLANs

The following figure shows VLAN configurations between two systems. VLAN 1 and 2 are created to separate two logical groups. The packets can be forwarded through the trunk port configured between two systems.

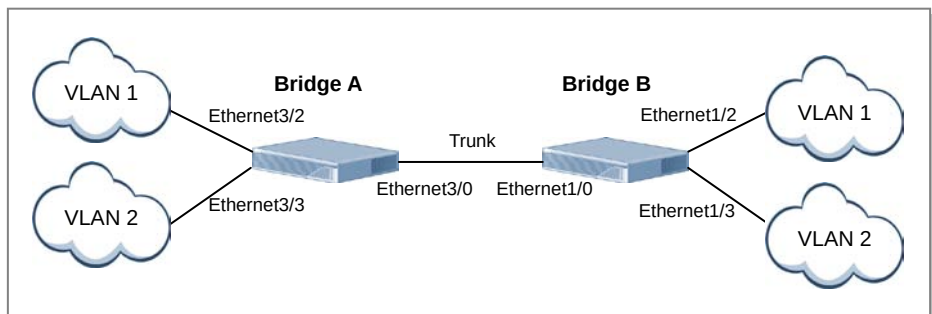


Figure 1.1 VLANs Example

The following shows the command sequences for each bridge or router in the figure1.1.

Bridge A configuration

```
BRIDGE_A# configure terminal
BRIDGE_A/configure# bridge 1 protocol mstp
BRIDGE_A/configure# vlan database
BRIDGE_A/configure/vlan/database# vlan 2 bridge 1
BRIDGE_A/configure/vlan/database# exit
BRIDGE_A/configure# interface ethernet 3/0
BRIDGE_A/configure/interface/ethernet (3/0)# switchport
BRIDGE_A/configure/interface/ethernet (3/0)# bridge-group 1
BRIDGE_A/configure/interface/ethernet (3/0)# switchport mode
trunk
BRIDGE_A/configure/interface/ethernet (3/0)# switchport
trunk allowed vlan all
BRIDGE_A/configure/interface/ethernet (3/0)# exit
BRIDGE_A/configure# interface ethernet 3/2
BRIDGE_A/configure/interface/ethernet (3/2)# switchport
BRIDGE_A/configure/interface/ethernet (3/2)# bridge-group 1
BRIDGE_A/configure/interface/ethernet (3/2)# exit
BRIDGE_A/configure# interface ethernet 3/3
BRIDGE_A/configure/interface/ethernet (3/3)# switchport
BRIDGE_A/configure/interface/ethernet (3/3)# bridge-group 1
BRIDGE_A/configure/interface/ethernet (3/3)# switchport
access vlan 2
BRIDGE_A/configure/interface/ethernet (3/3)# exit
```

Bridge B configuration

```
BRIDGE_B# configure terminal
BRIDGE_B/configure# bridge 1 protocol mstp
BRIDGE_B/configure# vlan database
BRIDGE_B/configure/vlan/database# vlan 2 bridge 1
BRIDGE_A/configure/vlan/database# exit
BRIDGE_B/configure# interface ethernet 1/0
BRIDGE_B/configure/interface/ethernet (1/0)# switchport
BRIDGE_B/configure/interface/ethernet (1/0)# bridge-group 1
BRIDGE_B/configure/interface/ethernet (1/0)# switchport mode
trunk
BRIDGE_B/configure/interface/ethernet (1/0)# switchport
trunk allowed vlan all
BRIDGE_B/configure/interface/ethernet (1/0)# exit
BRIDGE_B/configure# interface ethernet 1/2
BRIDGE_B/configure/interface/ethernet (1/2)# switchport
BRIDGE_B/configure/interface/ethernet (1/2)# bridge-group 1
BRIDGE_B/configure/interface/ethernet (1/2)# exit
BRIDGE_B/configure# interface ethernet 1/3
```

```

BRIDGE_B/configure/interface/ethernet (1/3)# switchport
BRIDGE_B/configure/interface/ethernet (1/3)# bridge-group 1
BRIDGE_B/configure/interface/ethernet (1/3)# switchport
access vlan 2
BRIDGE_B/configure/interface/ethernet (1/3)# exit

```

Verifying and Troubleshooting Commands

```

show vlan brief
show spanning-tree mst
show interface switchport bridge 1

```

Show example

The following example shows the configuration given above, displayed using the show commands.

Bridge A configuration show

```

BRIDGE_A/configure# show vlan brief
%VLAN Information
  Bridge-group 1
  Number of existing VLANs : 1 (254 available)
  **Valid number of VLANs   255
  **Valid VLAN ID Range   2-4000

VLAN ID  Name      State  Member ports([u]-Untagged, [t]-Tagged)
-----
  1      default   active [u]ethernet3/0 [u]ethernet3/2
  2      VLAN0002   active [t]ethernet3/0 [u]ethernet3/3

BRIDGE_A/configure# show spanning-tree mst
% 1: Bridge up - Spanning Tree Enabled
% 1: CIST Root Path Cost 0 - CIST Root Port 0 - CIST Bridge
Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Max-hops
20
% 1: CIST Root Id 80000001632801641
% 1: CIST Reg Root Id 80000001632801641
% 1: CST Bridge Id 80000001632801641
-----

```

index	Interface	Port_Role	Port_State	Path_Cost	Priority
9	ethernet3/3	Designated	Forwarding	20000	128
8	ethernet3/2	Designated	Forwarding	20000	128
6	ethernet3/0	Designated	Forwarding	200000	128

%

% Instance active_VLANS (no active VLANs)

% 0: 1-2

```
BRIDGE_A/configure# show interface switchport bridge 1
Interface name      : ethernet3/0
Switchport mode     : trunk
Acceptable frame types : vlan-tagged only
Default Vlan        : 1
Allowed Vlans        : 1-4000
Activated Vlans      : 1-2

Interface name      : ethernet3/2
Switchport mode     : access
Acceptable frame types : all
Default Vlan        : 1
Allowed Vlans        : 1
Activated Vlans      : 1

Interface name      : ethernet3/3
Switchport mode     : access
Acceptable frame types : all
Default Vlan        : 2
Allowed Vlans        : 2
Activated Vlans      : 2
BRIDGE_A/configure# bridge 1 protocol mstp
BRIDGE_A/configure# vlan database
BRIDGE_A/configure/vlan/database# vlan 2 bridge 1
BRIDGE_A/configure/vlan/database# exit
BRIDGE_A/configure# interface ethernet 3/0
BRIDGE_A/configure/interface/ethernet (3/0)# switchport
BRIDGE_A/configure/interface/ethernet (3/0)# bridge-group 1
BRIDGE_A/configure/interface/ethernet (3/0)# switchport mode
trunk
BRIDGE_A/configure/interface/ethernet (3/0)# switchport trunk
allowed vlan all
BRIDGE_A/configure/interface/ethernet (3/0)# exit
BRIDGE_A/configure# interface ethernet 3/2
BRIDGE_A/configure/interface/ethernet (3/2)# switchport
BRIDGE_A/configure/interface/ethernet (3/2)# bridge-group 1
```



```

BRIDGE_A/configure/interface/ethernet (3/2)# exit
BRIDGE_A/configure# interface ethernet 3/3
BRIDGE_A/configure/interface/ethernet (3/3)# switchport
BRIDGE_A/configure/interface/ethernet (3/3)# bridge-group 1
BRIDGE_A/configure/interface/ethernet (3/3)# switchport
access vlan 2
BRIDGE_A/configure/interface/ethernet (3/3)# exit

```

Configuring VLANs with multiple instances of MSTP

The following figure shows a scenario where two systems are interconnected using two links. Multiple instances are used for the traffic load balancing. VLAN 2 is associated with instance 1 which is newly configured in MSTP configuration. The member ports must be associated with the instance to be bound with the VLAN. Ethernet 3/0 and Ethernet 1/0 are used as the main path for VLAN 1. Ethernet 3/1 and Ethernet 1/1 are used as the main path for VLAN 2. The path cost of instance 1 should be changed in Ethernet 1/0 which can be configured as the main path for VLAN 2.

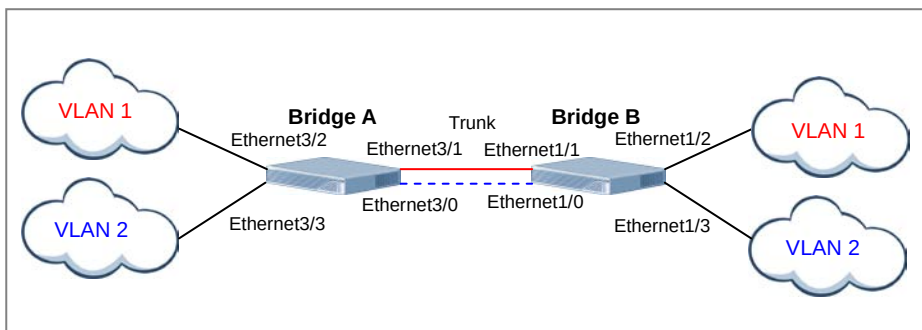


Figure 1.2 VLANs Example with multiple instances of MSTP

The following shows the command sequences for each bridge or router in the figure1.2.

Bridge A configuration

```
BRIDGE_A# configure terminal
BRIDGE_A/configure# bridge 1 protocol mstp
BRIDGE_A/configure# vlan database
BRIDGE_A/configure/vlan/database# vlan 2 bridge 1
BRIDGE_A/configure/vlan/database# exit
BRIDGE_A/configure# spanning-tree mst config
BRIDGE_A/configure/spanning-tree/mst# bridge 1 instance 1
vlan 2
BRIDGE_A/configure/spanning-tree/mst# exit
BRIDGE_A/configure# interface ethernet 3/0
BRIDGE_A/configure/interface/ethernet (3/0)# switchport
BRIDGE_A/configure/interface/ethernet (3/0)# bridge-group 1
BRIDGE_A/configure/interface/ethernet (3/0)# switchport mode
trunk
BRIDGE_A/configure/interface/ethernet (3/0)# switchport
trunk allowed vlan all
BRIDGE_A/configure/interface/ethernet (3/0)# bridge-group 1
instance 1
BRIDGE_A/configure/interface/ethernet (3/0)# exit
BRIDGE_A/configure# interface ethernet 3/1
BRIDGE_A/configure/interface/ethernet (3/1)# switchport
BRIDGE_A/configure/interface/ethernet (3/1)# bridge-group 1
BRIDGE_A/configure/interface/ethernet (3/1)# switchport mode
trunk
BRIDGE_A/configure/interface/ethernet (3/1)# switchport
trunk allowed vlan all
BRIDGE_A/configure/interface/ethernet (3/1)# bridge-group 1
instance 1
BRIDGE_A/configure/interface/ethernet (3/1)# exit
BRIDGE_A/configure# interface ethernet 3/2
BRIDGE_A/configure/interface/ethernet (3/2)# switchport
BRIDGE_A/configure/interface/ethernet (3/2)# bridge-group 1
BRIDGE_A/configure/interface/ethernet (3/2)# exit
BRIDGE_A/configure# interface ethernet 3/3
BRIDGE_A/configure/interface/ethernet (3/3)# switchport
BRIDGE_A/configure/interface/ethernet (3/3)# bridge-group 1
BRIDGE_A/configure/interface/ethernet (3/3)# switchport
access vlan 2
BRIDGE_A/configure/interface/ethernet (3/3)# bridge-group 1
instance 1
BRIDGE_A/configure/interface/ethernet (3/3)# exit
```

Bridge B configuration

```
BRIDGE_B# configure terminal
BRIDGE_B# configure terminal
BRIDGE_B/configure# bridge 1 protocol mstp
BRIDGE_B/configure# vlan database
BRIDGE_B/configure/vlan/database# vlan 2 bridge 1
BRIDGE_B/configure/vlan/database# exit
BRIDGE_B/configure# spanning-tree mst config
BRIDGE_B/configure/spanning-tree/mst# bridge 1 instance 1
vlan 2
BRIDGE_B/configure/spanning-tree/mst# exit
BRIDGE_B/configure# interface ethernet 1/0
BRIDGE_B/configure/interface/ethernet (1/0)# switchport
BRIDGE_B/configure/interface/ethernet (1/0)# bridge-group 1
BRIDGE_B/configure/interface/ethernet (1/0)# switchport mode
trunk
BRIDGE_B/configure/interface/ethernet (1/0)# switchport
trunk allowed vlan all
BRIDGE_B/configure/interface/ethernet (1/0)# bridge-group 1
instance 1
BRIDGE_B/configure/interface/ethernet (1/0)# exit
BRIDGE_B/configure# interface ethernet 1/1
BRIDGE_B/configure/interface/ethernet (1/1)# switchport
BRIDGE_B/configure/interface/ethernet (1/1)# bridge-group 1
BRIDGE_B/configure/interface/ethernet (1/1)# switchport mode
trunk
BRIDGE_B/configure/interface/ethernet (1/1)# switchport
trunk allowed vlan all
BRIDGE_B/configure/interface/ethernet (1/1)# bridge-group 1
instance 1
BRIDGE_B/configure/interface/ethernet (1/1)# bridge-group 1
instance 1 path-cost 2000
BRIDGE_B/configure/interface/ethernet (1/1)# exit
BRIDGE_B/configure# interface ethernet 1/2
BRIDGE_B/configure/interface/ethernet (1/2)# switchport
BRIDGE_B/configure/interface/ethernet (1/2)# bridge-group 1
BRIDGE_B/configure/interface/ethernet (1/2)# exit
BRIDGE_B/configure# interface ethernet 1/3
BRIDGE_B/configure/interface/ethernet (1/3)# switchport
BRIDGE_B/configure/interface/ethernet (1/3)# bridge-group 1
BRIDGE_B/configure/interface/ethernet (1/3)# switchport
access vlan 2
BRIDGE_B/configure/interface/ethernet (1/3)# bridge-group 1
instance 1
BRIDGE_B/configure/interface/ethernet (1/3)# exit
```

Verifying and Troubleshooting Commands

```
show vlan brief
show spanning-tree mst
show interface switchport bridge 1
```

Show example

The following example shows the configuration given above, displayed using the show commands.

Bridge A configuration show

```
BRIDGE_A/configure# show vlan brief
%VLAN Information
  Bridge-group 1
  Number of existing VLANs : 1 (254 available)
  **Valid number of VLANs   255
  **Valid VLAN ID Range   2-4000

VLAN ID  Name      State   Member ports([u]-Untagged, [t]-Tagged)
-----
  1      default    active  [u]ethernet3/0 [u]ethernet3/1
[u]ethernet3/2
  2      VLAN0002    active  [t]ethernet3/0 [t]ethernet3/1
[u]ethernet3/3
BRIDGE_A/configure# show spanning-tree mst
% 1: Bridge up - Spanning Tree Enabled
% 1: CIST Root Path Cost 0 - CIST Root Port 0 - CIST Bridge
Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Max-hops
20
% 1: CIST Root Id 80000001632801641
% 1: CIST Reg Root Id 80000001632801641
% 1: CST Bridge Id 80000001632801641

-----
index Interface  Port_Role  Port_State  Path_Cost  Priority
-----
  9    ethernet3/3  Designated Forwarding 20000      128
  8    ethernet3/2  Designated Forwarding 20000      128
  7    ethernet3/1  Designated Forwarding 200000     128
  6    ethernet3/0  Designated Forwarding 200000     128
%
```

```

% Instance      active_VLANS (no active VLANs)
% 0: 1
% 1: 2
-----
% 1: Root=8001001632801641 : Bridge=8001001632801641 : RPC=0
-----
-----
instance index Interface  Port_Role  Port_State Path_Cost
Priority
-----
1:  9  ethernet3/3  Designated Forwarding 20000  128
    7  ethernet3/1  Designated Forwarding 200000 128
    6  ethernet3/0  Designated Forwarding 200000 128
BRIDGE_A/configure# show interface switchport bridge 1
Interface name      : ethernet3/0
Switchport mode     : trunk
Acceptable frame types : vlan-tagged only
Default Vlan        : 1
Allowed Vlans        : 1-4000
Activated Vlans      : 1-2

Interface name      : ethernet3/1
Switchport mode     : trunk
Acceptable frame types : vlan-tagged only
Default Vlan        : 1
Allowed Vlans        : 1-4000
Activated Vlans      : 1-2

Interface name      : ethernet3/2
Switchport mode     : access
Acceptable frame types : all
Default Vlan        : 1
Allowed Vlans        : 1
Activated Vlans      : 1

Interface name      : ethernet3/3
Switchport mode     : access
Acceptable frame types : all
Default Vlan        : 2
Allowed Vlans        : 2
Activated Vlans      : 2

```

Bridge B configuration show

```

BRIDGE_B/configure# show vlan brief
%VLAN Information
  Bridge-group 1
  Number of existing VLANs : 1 (254 available)
  **Valid number of VLANs   255
  **Valid VLAN ID Range   2-4000

  VLAN ID   Name           State   Member ports ([u]-Untagged,
  [t]-Tagged)
  -----
  1          default       active  [u]ethernet1/0 [u]ethernet1/2
  [u]ethernet1/1
  2          VLAN0002       active  [t]ethernet1/0 [u]ethernet1/3
  [t]ethernet1/1
BRIDGE_B/configure# show spanning-tree mst
% 1: Bridge up - Spanning Tree Enabled
% 1: CIST Root Path Cost 0 - CIST Root Port 6 - CIST Bridge
Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Max-hops
20
% 1: CIST Root Id 80000001632801641
% 1: CIST Reg Root Id 80000001632801641
% 1: CST Bridge Id 800000016328022e1
-----
  index Interface   Port_Role  Port_State  Path_Cost  Priority
  -----
  7     ethernet1/1  Alternate  Discarding  2000000    128
  9     ethernet1/3  Designated Forwarding  2000000    128
  8     ethernet1/2  Designated Forwarding  2000000    128
  6     ethernet1/0  Rootport   Forwarding  2000000    128
%
% Instance      active_VLANS (no active VLANs)
% 0: 1
% 1: 2
-----
% 1: Root=8001001632801641 : Bridge=80010016328022e1 :
RPC=2000
-----

```

```

instance index Interface  Port_Role  Port_State  Path_Cost
Priority
-----

```

```

1 : 9  ethernet1/3  Designated Forwarding 200000 128
    6  ethernet1/0  Alternate   Discarding 200000 128
    7  ethernet1/1  Rootport   Forwarding 2000    128

```

```

BRIDGE_B/configure# show interface switchport bridge 1

```

```

Interface name      : ethernet1/0
Switchport mode     : trunk
Acceptable frame types : vlan-tagged only
Default Vlan        : 1
Allowed Vlans        : 1-4000
Activated Vlans      : 1-2

```

```

Interface name      : ethernet1/2
Switchport mode     : access
Acceptable frame types : all
Default Vlan        : 1
Allowed Vlans        : 1
Activated Vlans      : 1

```

```

Interface name      : ethernet1/3
Switchport mode     : access
Acceptable frame types : all
Default Vlan        : 2
Allowed Vlans        : 2
Activated Vlans      : 2

```

```

Interface name      : ethernet1/1
Switchport mode     : trunk
Acceptable frame types : vlan-tagged only
Default Vlan        : 1
Allowed Vlans        : 1-4000
Activated Vlans      : 1-2

```

Configuring 802.1x

IEEE 802.1x restricts unauthenticated devices from connecting to the router, typically in a VLAN/Bridge environment. Only authenticated traffic is allowed through the Ubigate iBG router.

In the configuration example shown in fig 1.3, the RADIUS Server keeps the Client information, validating the identity of the client and updating the router with the client authentication status. iBG2016 resides in the physical path between the client, server and the RADIUS server.

To configure 802.1x authentication, enable authentication on ports Ethernet 1/1 and Ethernet 2/1, and specify the RADIUS Server IP address and port number.

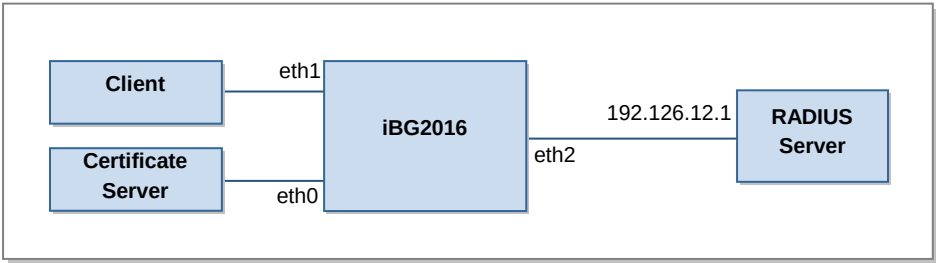


Figure 1.3 Configuring 802.1x Security

802.1x command

Command	Explanation
dot1x initialize	Initialize Port to attempt reauthentication
dot1x max-req	Maximum failed EAP request sent to supplicant
dot1x port-control	port control commands
dot1x quiet-period	Quiet period in the held state (Default is 60 seconds)
dot1x reauthentication	Enable reauthentication on a port
dot1x timeout	set a timeout parameter

Step-by-Step Configuration

Step	Command	Purpose
1	Router# configure terminal	Enters the terminal configuration mode.
2	Router/configure# bridge 1 protocol mstp	Creates the bridge 1 with MSTP. Only one bridge can be created in a system with bridge ID 1. After executing this command, the default VLAN (ID=1) is also created automatically.
3	Router/configure# vlan database	Enters VLAN database mode.
4	Router/configure/vlan/database# vlan [vlan number] bridge 1	Creates new VLAN in a bridge. Repeats as many as required. vlan_number: ranges 2 to 4000 4001-4094 are reserved as the internal purpose.
5	Router/configure/vlan/database# exit	Exits VLAN database mode.
6	dot1x system-auth-ctrl	Sets the 802.1x control
7	Router/configure/interface/[interface name]# switchport	Sets the interface as a switch port.
8	Router/configure/interface/[interface name]# bridge-group 1	Includes this interface in a bridge group.
9	dot1x port-control	Sets the port control.
10	Router/configure# interface [interface name]	Enters interface configuration mode.
11	aaa radius primary-server	Sets the radius primary server.
12	aaa radius auth_port	Sets the radius port.
13	aaa radius src_address	Sets the radius source address.
14	show dot1x all	Shows 802.x1 status.

Verifying and Troubleshooting Commands

To troubleshoot the 802.1x configuration and operation, use the following commands:

802.1x debug option

Command	Explanation
all	Turn on all debugging
event	Show 802.1x events
nsm	802.1x Nsm Information
packet	802.1x packet
timer	802.1x timer

```
Router# debug dot1x all
Router# *Jun 14,2007,08:59:31 #802.1X-warning: RECV[RADIUS]:
pal_sock_recvfrom error (S_errno_ECONNREFUSED)
```

802.1x show option

```
Router# show dot1x all
802.1X Port-Based Authentication Enabled
  RADIUS server address: 100.1.1.3:1812
  RADIUS client address: 100.1.1.2:0
  Next radius message id: 247
802.1X info for interface ethernet3/6
  Supplicant name: myid@mynet.net
  Supplicant address: 0001.0288.11bc
  portEnabled: true - portControl: Auto
  portStatus: Unauthorized - currentId: 215
  reAuthenticate: disabled
  reAuthPeriod: 3600
  abort:F fail:F start:T timeout:F success:F
  PAE: state: Authenticating - portMode: Auto
  PAE: reAuthCount: 1 - rxRespId: 1
  PAE: quietPeriod: 60 - reauthMax: 2 - txPeriod: 30
  BE: state: Request - reqCount: 1 - idFromServer: 215
  BE: suppTimeout: 30 - serverTimeout: 30 - maxReq: 2
  CD: adminControlledDirections: in -
  operControlledDirections: in
  CD: bridgeDetected: false
  KR: rxKey: false
  KT: keyAvailable: false - keyTxEnabled: false
```

Configuration Example

```
Router# configure terminal
Router/configure# bridge 1 protocol mstp
Router/configure# vlan database
Router/configure/vlan/database# vlan 2 bridge 1
Router/configure/vlan/database# exit
Router/configure# dot1x system-auth-ctrl
Router/configure# interface ethernet 1/0
Router/configure/interface/ethernet(1/0)# switchport
Router/configure/interface/ethernet(1/0)# bridge-group 1
Router/configure/interface/ethernet(1/0)# switchport
access vlan 2
Router/configure/interface/ethernet(1/0)# dot1x port-control
auto
Router/configure/interface/ethernet(1/0)# exit
Router/configure# interface ethernet 1/1
Router/configure/interface/ethernet(1/1)# switchport
Router/configure/interface/ethernet(1/1)# bridge-group 1
Router/configure/interface/ethernet(1/1)# switchport
access vlan 2
Router/configure/interface/ethernet(1/1)# dot1x port-control
auto
Router/configure/interface/ethernet(1/1)# exit
Router/configure# interface vlan vlan1.2
Router/configure/interface/ vlan vlan1.2# ip address
100.0.0.1 24
Router/configure/interface/ vlan vlan1.2# exit
Router/configure# interface ethernet 1/2
Router/configure/interface/ethernet(1/2)# ip address
192.126.12.2 24
Router/configure/interface/ethernet(1/2)# exit
Router/configure# aaa radius primary-server 192.126.12.1
Router/configure# aaa radius auth_port 1812
Router/configure# aaa radius src_address 192.126.12.2
```

LACP Configuration



This is applied to SNOS version 2.1.0 or higher.

LACP is based on the 802.3ad IEEE specification. It allows bundling of several physical interfaces to form a single logical channel providing enhanced performance and redundancy between switches, routers and servers. The aggregated interface is viewed as a single link to each system. Spanning tree also views it as one interface.

When there is a failure in one physical interface, the other aggregated interfaces provide automatic recovery for the loss of a link by redistributing the load across the remaining links.

Up to 8 physical Ethernet links can be aggregated into a single logical channel and up to 16 aggregated interfaces can be created in the Ubigate.

In this example, three links are configured between the two routers S1 and S2. These three links are assigned the same administrative key (10) so that they aggregate to form a single channel 10. They are viewed by the MSTP as one interface. Prior to be aggregated for a channel-group, the Ethernet interface should be configured as the switchport.

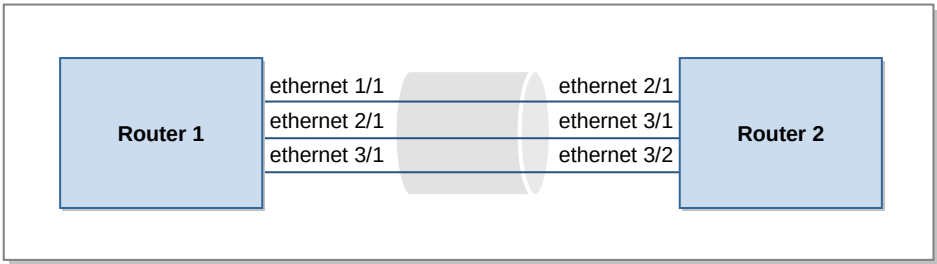


Figure 1.4 Link Aggregation Example

Configuring Router 1

```
Router#configure terminal
Router/configure# interface ethernet 1/1
Router/configure/interface/ethernet(1/1)# channel-group 10
mode active
Router/configure/interface/ethernet(1/1)# exit
Router/configure# interface ethernet 2/1
Router/configure/interface/ethernet(2/1)# channel-group 10
mode active
Router/configure/interface/ethernet(2/1)# exit
Router/configure# interface ethernet 3/1
Router/configure/interface/ethernet(3/1)# channel-group 10
mode active
Router/configure/interface/ethernet(3/1)# exit
```

Configuring Router 2

```
Router# configure terminal
Router/configure# lacp system-priority 20000
Router/configure# interface ethernet 2/1
Router/configure/interface/ethernet(2/1)# channel-group 10
mode active
Router/configure/interface/ethernet(2/1)# exit
Router/configure# interface ethernet 3/1
Router/configure/interface/ethernet(3/1)# channel-group 10
mode active
Router/configure/interface/ethernet(3/1)# exit
Router/configure# interface ethernet 3/2
Router/configure/interface/ethernet(3/2)# channel-group 10
mode active
Router/configure/interface/ethernet(3/2)# exit
```

Verifying and Troubleshooting Commands

```
show etherchannel
show etherchannel detail
show port etherchannel [interface name]
```

Show example

The following example shows the configuration given above, displayed using the show commands.

Router1 configuration show

```
Router# show etherchannel
% Total Configured Aggregator: 1

% Dynamic(Lacp) Aggregator:
=====
% [1] po10
% Mac address: 00:16:32:80:07:8c
% Member:
  ethernet1/1
    - Status : UP - SYNC ON - LINK_UP
    - Mode : active
  ethernet2/1
    - Status : UP - SYNC ON - LINK_UP
    - Mode : active
  ethernet3/1
    - Status : UP - SYNC ON - LINK_UP
    - Mode : active

Router# show etherchannel detail
% Aggregator po10 1000000
% refCnt: 3 - linkCnt: 3
% Mac address: 00:16:32:80:07:8c
% Admin Key: 0010 - Oper Key 0010
% Receive link count: 1 - Transmit link count: 0
% Individual: 0 - Ready: 1
% Partner LAG- 0x8000,00-16-32-80-16-41
% Link: ethernet1/1 (11) sync: ON
% Link: ethernet2/1 (12) sync: ON
% Link: ethernet3/1 (13) sync: ON
```

Router2 configuration show

```
Router# show etherchannel
% Total Configured Aggregator: 1

% Dynamic(Lacp) Aggregator:
=====
% [1] po10
% Mac address: 00:16:32:80:16:77
% Member:
  ethernet1/1
    - Status : UP - SYNC ON - LINK_UP
    - Mode : active
  ethernet2/1
    - Status : UP - SYNC ON - LINK_UP
    - Mode : active
  ethernet3/1
    - Status : UP - SYNC ON - LINK_UP
    - Mode : active

Router# show etherchannel detail
% Aggregator po10 1000000
% refCnt: 3 - linkCnt: 3
% Mac address: 00:16:32:80:07:81
% Admin Key: 0010 - Oper Key 0010
% Receive link count: 1 - Transmit link count: 0
% Individual: 0 - Ready: 1
% Partner LAG- 0x8000,00-16-32-80-16-41
% Link: ethernet1/1 (11) sync: ON
% Link: ethernet2/1 (12) sync: ON
% Link: ethernet3/1 (13) sync: ON
```

Configuring IGMP Snooping

This section provides steps to configure Internet Group Management Protocol (IGMP) Snooping. Without IGMP, Layer 2 routers handle IP multicast traffic in the same manner as broadcast traffic and forward frames received on one interface to all other interfaces. This creates excessive traffic on the network and affects network performance. IGMP Snooping allows routers to monitor network traffic and determine hosts that want to receive multicast traffic. Only one membership report is relayed from a group instead of a report from each host in the group. To achieve this, IGMP proxy is enabled on the routers. This example describes the configuration on Router S1. The interface Ethernet 1/1 is configured as an mrouter port. Since IGMP Snooping is used in bridged LAN environment only, router R1 does not require running IGMP Snooping and can run any multicast protocol (such as PIM-SM). The configuration on R1 is thus not included in this example. To enable IGMP Snooping on an interface:

1. Add a bridge to the spanning-tree table.
2. Specify the interface to be configured.
3. Associate the interface with bridge-group.
4. Enable IGMP Snooping globally.
5. Enable IGMP Snooping on the bridge-group.
6. Configure ports that are connected to routers as multicast router ports.
7. Enable IGMP Proxy on the router.

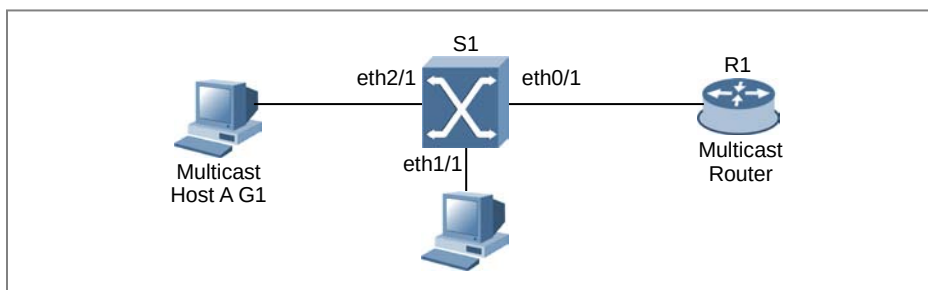


Figure 1.5 IGMP Snooping Example

As a result of this configuration, the queries received on the router by Ethernet 1/1 will not be forwarded to Ethernet 0/1 and Ethernet 2/1. The router itself will reply back with Membership report message. However, if you do not enable Proxy on the router, when it receives a IGMP Query message on Ethernet 1/1, it forwards it to both Host A and Host B. As a result, both the hosts reply with a Membership report (as Layer-2 IGMP is running on the hosts).

Since Host A and Host B are members of the same Multicast group, the router is not notified when Host A leaves the group, as the group still has another member Host B remaining. When Host B also leaves the group, the router will send a Leave message to the Router with the destination address as 224.0.0.2 (All Router Destination Address).

lgmp snooping command

Command	Explanation
explicit-tracking	Explicit Tracking Processing
fast-leave	Fast-Leave option of IGMP snooping
last-member-query-interval	Last Member Query Interval
max-response-time	Max response time for report
mrouter	Multicast Router
proxy	Enable IGMP Proxy for the box
querier	IGMP Snooping Querier
querier-timeout	Other querier timeout interval
query-interval	Query interval
ssm-safe-reporting	Source Specific Multicast Safe Reporting
version	IGMP Version for interface
vlan	Identify the VLAN to use

IGMP Snooping Configuration

```
Router#configure terminal
Router/configure# ip igmp snooping vlan 2 bridge 1
Router/configure# ip igmp snooping bridge 1
Router/configure# ip igmp snooping fast-leave vlan 2 bridge 1
Router/configure# ip igmp snooping group-membership-interval
30 vlan 2 bridge 1
Router/configure# ip igmp snooping last-member-query-
interval 40 vlan 2 bridge 1
Router/configure# ip igmp snooping max-response-time 60 vlan
2 bridge 1
Router/configure# ip igmp snooping mrouter interface
ethernet1/1
Router/configure# ip igmp snooping other-querier-interval
100 vlan 2 bridge 1
Router/configure# ip igmp snooping proxy
Router/configure# ip igmp snooping querier vlan 2 bridge 1
Router/configure# ip igmp snooping ssm-safe-reporting vlan 2
bridge 1
Router/configure# ip igmp snooping version 2 vlan 2 bridge 1
ethernet1/1
```

Verify and Troubleshooting

Use the following ‘show’ commands to verify your IGMP and IGMP snooping configuration.

- show ip igmp groups displays the multicast groups with hosts directly connected to the router and learned through IGMP.
- show ip igmp groups detail displays information about the specified group.
- show ip igmp interface displays multicast-related information about an interface.
- show ip igmp interface ethernet 1/1 shows the IGMP configuration for all interfaces (or a specified interface).
- show ip igmp snooping shows the status of IGMP snooping.
- show ip igmp snooping explicit-tracking shows the hosts being tracked explicitly (a Version 3 feature).
- show ip igmp snooping fast-leave shows fast-leave processing information.
- show ip igmp snooping group-membership-interval shows the value of the group-membership interval.

- show ip igmp snooping last-member-query-interval shows the last-member-query-interval processing for IGMP hosts.
- show ip igmp snooping max-response-time shows the maximum response time setting.
- show ip igmp snooping mrouter shows the multicast router interfaces.
- show ip igmp snooping other-querier-interval shows the querier interval setting.
- show ip igmp snooping querier shows the querier interval setting.
- show ip igmp snooping ssm-safe-reporting shows the status of IGMP snooping SSM-safe-reporting.
- show ip igmp snooping interface version shows the version of IGMP being used.
- show ip igmp snooping vlan shows the IGMP snooping state for the default VLAN.
- show ip igmpv2 snooping statistics shows Version 2 statistics.
- show ip igmpv3 snooping statistics shows Version 3 statistics.

igmp show command

```
Router# show ip igmp groups
IGMP Connected Group Membership
Group Address  Interface    Uptime    Expires    Last Reporter
224.1.1.100    ethernet3/0  00:00:05  00:04:14  20.20.20.1
224.1.1.100    ethernet3/1  00:00:00  00:04:19  30.30.30.1
Router# show ip igmp interface

Interface ethernet0/4 (Index 5)
IGMP Enabled, Active, Querier, Default version 2
Internet address is 10.10.10.2
IGMP query interval is 125 seconds
IGMP querier timeout is 255 seconds
IGMP max query response time is 10 seconds
Last member query response interval is 1000 milliseconds
Group Membership interval is 260 seconds
Number of groups IGMP joined on this interface: 0
Number of received IGMP V1-reports: 0
Number of received IGMP V2-reports: 0
Number of received IGMP V2-leaves: 0
Multicast routing is enabled on interface
```

```
Interface ethernet3/0 (Index 6)
  IGMP Enabled, Active, Querier, Default version 2
  Internet address is 20.20.20.2
  IGMP query interval is 125 seconds
  IGMP querier timeout is 255 seconds
  IGMP max query response time is 10 seconds
  Last member query response interval is 1000 milliseconds
  Group Membership interval is 260 seconds
  Number of groups IGMP joined on this interface: 1
  Number of received IGMP V1-reports: 0
  Number of received IGMP V2-reports: 4
  Number of received IGMP V2-leaves: 1
  Multicast routing is enabled on interface
```

```
Router# show ip igmp groups detail
```

```
Interface: ethernet3/0
Group: 224.1.1.100
Uptime: 00:03:02
Group mode: Exclude (Expires: 00:03:54)
Last reporter: 20.20.20.1
Source list is empty
Interface: ethernet3/1
Group: 224.1.1.100
Uptime: 00:02:57
Group mode: Exclude (Expires: 00:03:59)
Last reporter: 30.30.30.1
Source list is empty
```



CHAPTER 2. DHCP Relay

Ubigate iBG router's DHCP relay feature eliminates the need for a DHCP server on every LAN, because DHCP requests can be relayed to a single remote DHCP server. The relay agent forwards traffic between clients and servers when they are located on different subnets. When the relay agent receives a DHCP message, it generates a new DHCP and sends it out on another interface. This differs from normal IP forwarding on routers wherein traffic is switched between networks.

Ubigate iBG router's implementation of DHCP relay is based on RFC 1542. Additional RFCs supported are:

- RFC 951, Bootstrap Protocol (BOOTP)
- RFC 2131, Dynamic Host Configuration Protocol
- RFC 2132, DHCP Options and BOOTP Vendor Extensions

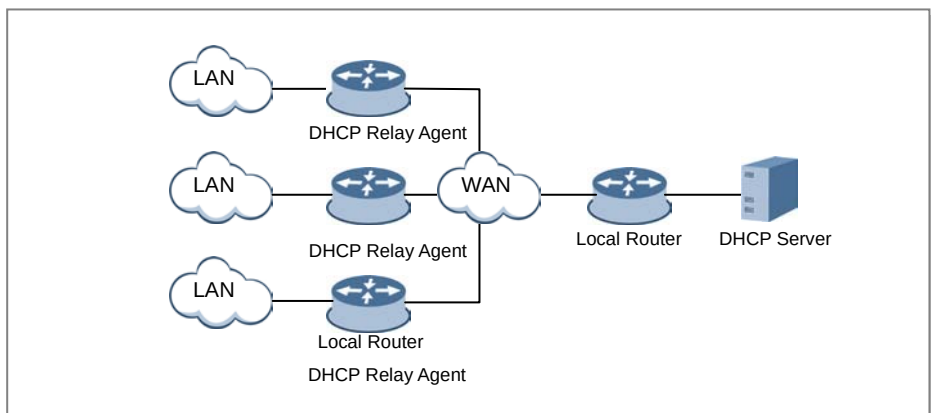


Figure 2.1 DHCP relay overview

Functionality

The DHCP relay feature uses BOOTP requests and replies to negotiate packet delivery between the DHCP client and server.

BOOTP Requests and Replies

BOOTP Requests

BOOTP requests are messages from client to server. Request messages include DHCP DISCOVER, DHCP REQUEST, DHCP RELEASE, etc. The relay agent modifies the packet header by adding relay information to the DHCP gateway address (giaddr) field. The server replies to the gateway address specified in the packet's giaddr field.

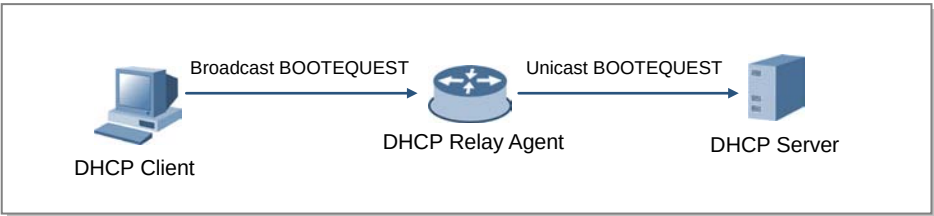


Figure 2.2 BOOTP Requests

BOOTP Replies

BOOTP replies are messages from the server to the client. Reply messages include DHCP OFFER, DHCP ACK, DHCP NAK, etc. The relay agent looks up the MAC address and either sends the packet to the client or broadcasts it on the LAN.

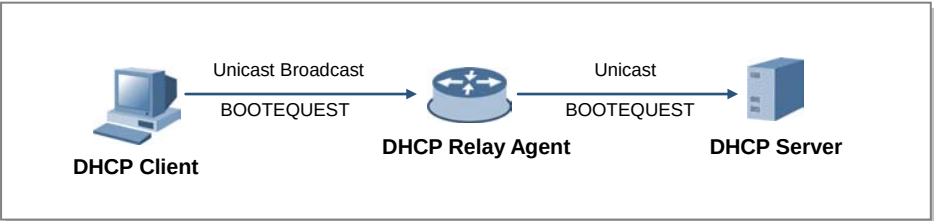


Figure 2.3 BOOTP Replies

Using DHCP Relay with NAT

When NAT is enabled, the DHCP server may discard packets because the giaddr does not match the source of the packet. Additionally, it may not know how to route the packet back to the client. See Figure 2.4. The solution is that the gateway address (giaddr) field needs to have IP address 192.168.20.1 (in this example). The DHCP server configuration should be able to give 10.1.1.x addresses for packets from 192.168.20.1. However, there may be a limitation that the DHCP server does not allow configuration using IP addresses from a different subnet, although this is mentioned in the RFC.

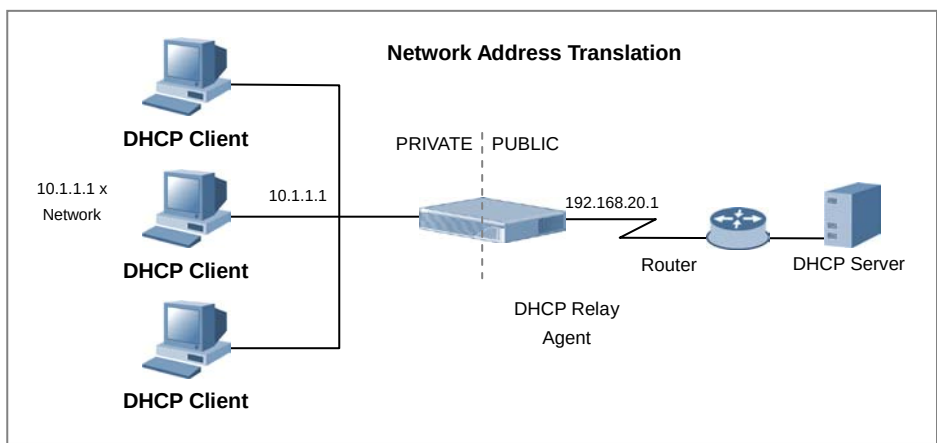


Figure 2.4 Typical Scenario for DHCP Relay with NAT

Command Line Interface

The following are examples of command strings relevant to DHCP relay

```
Router# configure terminal
Router/configure# interface ethernet 0/0
Router/configure/interface/ethernet(0/0)# dhcp_relay
server_address 20.1.1.1

Disabling DHCP Relay
Router/configure/interface/ethernet(0/0)# no dhcp_relay
server_address 20.1.1.1

Configuring the Gateway Address field when NAT is enabled
Router/configure/interface/ethernet(0/0)# dhcp_relay
gateway_address 192.168.20.1
```

Verifying and Troubleshooting Commands

```
debug# dhcp_relay enable_debug
show dhcp_relay statistics
show dhcp_relay config
```

```
Router/debug# dhcp_relay enable_debug

Received BOOTREQUEST on 33.3.3.1 -> unicasting to 10.1.1.2
Got BOOTREPLY - unicast to 33.3.3.2 (port: 68)
Received BOOTREQUEST on 33.3.3.1 -> unicasting to 10.1.1.2
Got BOOTREPLY - unicast to 33.3.3.2 (port: 68)

Router# show dhcp_relay statistics

DHCP RELAY CONFIGURATION
-----
ethernet3/0 : DHCP server 10.1.1.2
      DHCP REQ Forwarded: 2      DHCP REQ Dropped: 0
      DHCP REP Forwarded: 2      DHCP REP Dropped: 0

Router# show dhcp_relay config

DHCP RELAY CONFIGURATION
-----

ethernet3/0 : DHCP server 10.1.1.2
```




CHAPTER 3. Static Routing

Static routing is a user-defined way of configuring packet routes. Since routers can forward packets only to known routes, if routers can not learn routes dynamically, the static entry can be used for routers to route incoming packets.

Compared to Static Routing, Dynamic Routing, on the other hand, is typically used when static routing entries should be unwieldy in a large network, where the administrator would have to operate complex manual tasks.

This chapter describes how to configure static routing in the Ubigate iBG router.

Configuring Static Routes

Static routes are specified by adding and deleting route entries to and from the route table. This section shows how to add a route entry.

The following steps show the way to add a route entry.

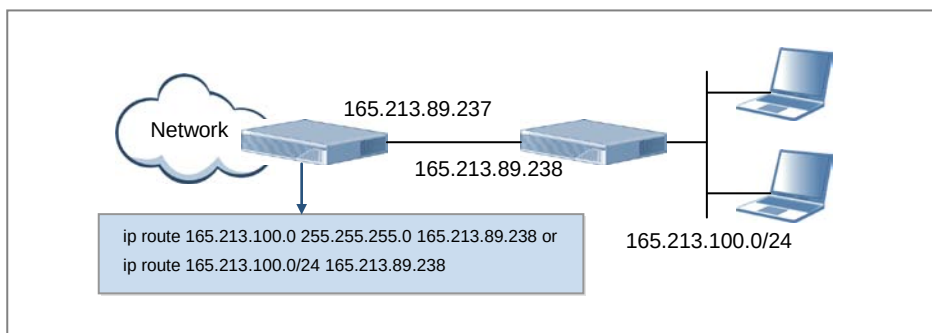
Step-by-Step Configuration

Step	Command	Purpose
1	Router# configure terminal	Enters the terminal configuration mode.
2	Router/configure# ip route [network] [mask] {address interface} Or Router/configure# ip route [network]/[number of bit mask] {address interface}	Adds a routing entry

To delete a route entry, just add the key word 'no' in front of the command that have added it.

Example

The following figure illustrates a simple network configuration.



The following example shows the way to add a routing entry in the figure.

```
Router# configure terminal
Router/configure# ip route 165.213.100.0 255.255.255.0
165.213.89.238

or

Router# configure terminal
Router/configure# ip route 165.213.100.0/24 165.213.89.238
```

To delete the entry, simply add 'no' just as follows.

```
Router# configure terminal
Router/configure# no ip route 165.213.100.0 255.255.255.0
165.213.89.238

or

Router# configure terminal
Router/configure# no ip route 165.213.100.0/24
165.213.89.238
```



CHAPTER 4. RIP

Routing Information Protocol (RIP) is a classical distance-vector routing protocol. It is simple to implement and performs good for small networks. Distance Vector Routing requires that each node maintain the distance from itself to each possible destination. The distances are computed using the information in neighbor's distance vectors.

RIP version 1 (defined in RFC 1058) has been later augmented by RIP version 2 (RFC 2453) to increase its usefulness. RIP 2 enabled RIP messages to carry more information, which permitted the use of a simple authentication mechanism to secure table updates. More importantly, RIP 2 supported subnet masks, a critical feature that was not available in RIP.

RIP Protocol Features

RIP sends routing-update messages at regular intervals and when the network topology changes. When a router receives a routing update that includes changes to an entry, it updates its routing table to reflect the new route. The metric value for the path is increased by 1, and the sender is indicated as the next hop. RIP routers maintain only the best route (the route with the lowest metric value) to a destination. After updating its routing table, the router immediately begins transmitting routing updates to inform other network routers of the change. These updates are sent independently of the regularly scheduled updates that RIP routers send.

RIP uses a single routing metric (hop count) to measure the distance between the source and a destination network. Each hop in a path from source to destination is assigned a hop count value, which is typically 1.

When a router receives a routing update that contains a new or changed destination network entry, the router adds 1 to the metric value indicated in the update and enters the network in the routing table. The IP address of the sender is used as the next hop.

RIP prevents routing loops from continuing indefinitely by implementing a limit on the number of hops allowed in a path from the source to a destination. The maximum number of hops in a path is 15. If a router receives a routing update that contains a new or changed entry, and if increasing the metric value by 1 causes the metric to be infinity (that is, 16), the network destination is considered unreachable. The downside of this stability feature is that it limits the maximum diameter of a RIP network to less than 16 hops.

RIP includes a number of other stability features that are common to many routing protocols. These features are designed to provide stability despite potentially rapid changes in a network's topology. For example, RIP implements the split horizon and hold down mechanisms to prevent incorrect routing information from being propagated.

Split horizon helps reduce convergence time by not allowing routers to advertise networks in the direction from which those networks were learned. The only information sent in RIP announcements are for those networks that are beyond the neighboring router in the opposite direction. Networks learned from the neighboring router are not included. Split horizon eliminates count-to-infinity and routing loops during convergence in single-path internetworks and reduces the chances of count-to-infinity in multi-path internetworks.

Split horizon with poison reverse differs from simple split horizon because it announces all networks. However, those networks learned in a given direction are announced with a hop count of 16, indicating that the network is unreachable. In a single-path internetwork, split horizon with poison reverse has no benefit beyond split horizon. However, in a multipath internetwork, split horizon with poison reverse greatly reduces count-to-infinity and routing loops. Split horizon with poison reverse does have the disadvantage of additional RIP message overhead because all networks are advertised.

RIP uses numerous timers to regulate its performance. These include a routing-update timer, a route-timeout timer, and a route-flush timer. The routing-update timer clocks the interval between periodic routing updates. Generally, it is set to 30 seconds, with a small random amount of time added whenever the timer is reset.

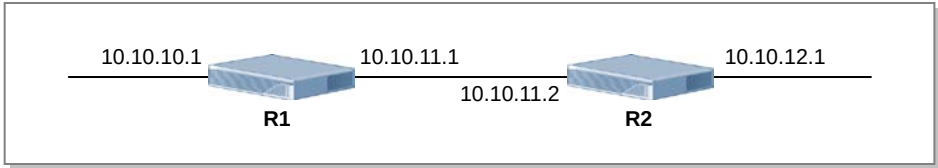
This is done to help prevent congestion, which could result from all routers simultaneously attempting to update their neighbors. Each routing table entry has a route-timeout timer associated with it. When the route-timeout timer expires, the route is marked invalid but is retained in the table until the route-flush timer expires.

Triggered updates allow a RIP router to announce changes in metric values almost immediately rather than waiting for the next periodic announcement. The trigger is a change to a metric in an entry in the routing table. For example, networks that become unavailable can be announced with a hop count of 16 through a triggered update. Note that the update is sent almost immediately, where a time interval to wait is typically specified on the router. If triggered updates were sent by all routers immediately, each triggered update could cause a cascade of broadcast traffic across the IP internetwork.

Triggered updates improve the convergence time of RIP internetworks but at the expense of additional broadcast traffic as the triggered updates are propagated.

Configuring RIP

This section describes the steps to configure RIP and show a simple example. R1 and R2 are two Ubigate iBG routers connecting to a common network 10.10.11.0/24. They are also connected to network 10.10.10.0/24 and 10.10.12.0/24, respectively.



The following table shows the steps to enable RIP on a Ubigate iBG router.

Step-by-Step Configuration

Step	Command	Purpose
1	Router# configure terminal	Enters the terminal configuration mode.
2	Router/configure# router rip	Enters the RIP setup mode.
3	Router/configure/router rip# network [IP address]/[number of bit masks] or Router/configure/router rip# network [interface]	Associates a network to RIP.
4	Router/configure/router rip# end	Returns to the 'Router#' prompt.
5	Router # show ip protocols rip	Display RIP configuration.

Configuration Example

To configure and enable RIP, after changing modes for RIP configuration, associate networks to run RIP on by specifying networks with a subnet number or an interface name.

The following example shows the commands used to configure RIP for R1.

```
R1# configure terminal
R1/configure# router rip
R1/configure/router rip# network 10.10.10.0/24
R1/configure/router rip# network 10.10.11.0/24
R1/configure/router rip# end
R1# show ip protocols rip
```

The following example shows the commands used to configure RIP for R2.

```
R1# configure terminal
R1/configure# router rip
R2/configure/router rip# network 10.10.11.0/24
R2/configure/router rip# network 10.10.12.0/24
R2/configure/router rip# end
R2# show ip protocols rip
```

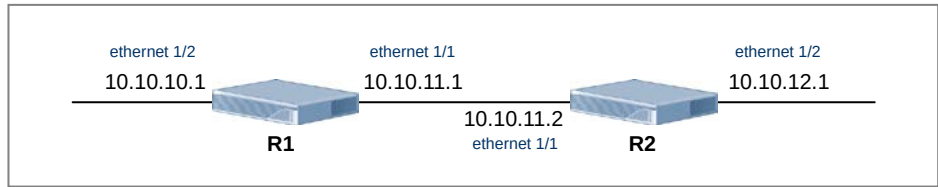
Specifying the RIP version

Configure a router to receive and send specific versions of packets on an interface. In this example, router R1 and R2 are configured to receive and send RIP version 1 and version 2 information on both Ethernet 1/1 and Ethernet 1/2 interfaces.

Step-by-Step Configuration

Step	Command	Purpose
1	Router# configure terminal	Enters the terminal configuration mode.
2	Router/configure# router rip	Enters the RIP setup mode.
3	Router/configure/router rip# network [interface]/[number of bit masks]	Associates a network to RIP.
4	Router/configure/router rip# redistribute connected	Enables redistributing from connected routes.
5	Router/configure/router rip# exit	Returns to the upper level prompt.
6	Router/configure# interface [interface]	Specify the interface for authentication
7	Router/configure/interface/[interface]# ip rip send version {1 2 1 2}	Selects send version.
8	Router/configure/interface/[interface]# ip rip receive version {1 2 1 2}	Selects receive version.
9	Router # show ip protocols rip	Displays RIP configuration.

Configuration Example



The following example shows the commands used to configure RIP send and receive version for R1.

```

R1# configure terminal
R1/configure# router rip
R1/configure/router rip# network 10.10.11.0/24
R1/configure/router rip# redistribute connected
R1/configure/router rip# exit
R1/configure# interface ethernet 1/1
R1/configure/interface/ethernet(1/1)# ip rip send version 1 2
R1/configure/interface/ethernet(1/1)# ip rip receive version
1 2

```

The following example shows the commands used to configure RIP send and receive version for R2.

```

R2# configure terminal
R2/configure# router rip
R2/configure/router rip# network 10.10.11.0/24
R2/configure/router rip# redistribute connected
R2/configure/router rip# exit
R2/configure# interface ethernet 1/1
R2/configure/interface/ethernet(1/1)# ip rip send version 1 2
R2/configure/interface/ethernet(1/1)# ip rip receive version
1 2

```

Configuring RIPv2 authentication

The Ubigate iBG router provides RIPv2 authentication and the choice of a single key or multiple keys for the authentication. This section describes a simple example to configure RIPv2 authentication with a single key.

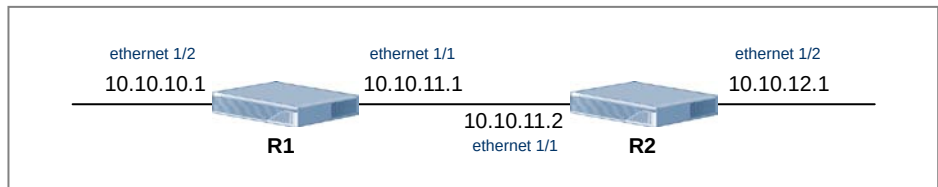
- In this case, not only the network numbers but also the network interfaces should be specified for authentication.

The following table shows the steps to enable RIPv2 authentication on a Ubigate iBG router.

Step-by-Step Configuration

Step	Command	Purpose
1	Router# configure terminal	Enters the terminal configuration mode.
2	Router/configure# router rip	Enters the RIP setup mode.
3	Router/configure/router rip# network [interface]/[number of bit masks]	Associates a network to RIP.
4	Router/configure/router rip# redistribute connected	Enables redistributing from connected routes.
5	Router/configure/router rip# exit	Returns to the upper level prompt.
6	Router/configure# interface [interface]	Specify the interface for authentication
7	Router/configure/interface/[interface]# ip rip authentication mode {md5 text}	Selects authentication mode.
8	Router/configure/interface/[interface]# ip rip authentication string [string]	Specify the authentication string.
9	Router # show ip protocols rip	Displays RIP configuration.

Configuration Example



The following example shows the commands used to configure RIPv2 authentication for R1.

```

R1# configure terminal
R1/configure# router rip
R1/configure/router rip# network 10.10.11.0/24
R1/configure/router rip# redistribute connected
R1/configure/router rip# exit
R1/configure# interface ethernet 1/1
R1/configure/interface/ethernet(1/1)# ip rip authentication
mode md5
R1/configure/interface/ethernet(1/1)# ip rip authentication
string UBI
  
```

The following example shows the commands used to configure RIPv2 authentication for R2.

```

R2# configure terminal
R2/configure# router rip
R2/configure/router rip# network 10.10.11.0/24
R2/configure/router rip# redistribute connected
R2/configure/router rip# exit
R2/configure# interface ethernet 1/1
R2/configure/interface/ethernet(1/1)# ip rip authentication
mode md5
R2/configure/interface/ethernet(1/1)# ip rip authentication
string UBI
  
```

The following example shows the commands used to configure RIPv2 text authentication for R1.

```
R1# configure terminal
R1/configuration# router rip
R1/configuration/router rip# network 10.10.11.0/24
R1/configuration/router rip# redistribute connected
R1/configuration/router rip# exit
R1/configuration# interface ethernet 1/1
R1/configuration/interface/ethernet(1/1)# ip rip authentication
mode text
R1/configuration/interface/ethernet(1/1)# ip rip authentication
string UBI
```

The following example shows the commands used to configure RIPv2 text authentication for R2.

```
R2# configure terminal
R2/configuration# router rip
R2/configuration/router rip# network 10.10.11.0/24
R2/configuration/router rip# redistribute connected
R2/configuration/router rip# exit
R2/configuration# interface ethernet 1/1
R2/configuration/interface/ethernet(1/1)# ip rip authentication
mode text
R2/configuration/interface/ethernet(1/1)# ip rip authentication
string UBI
```

As in the examples, RIP should be run on the network to be authenticated at first. The redistribute command is enabled to see to it that the authentication be performed correctly. Then, the interface to be authenticated, the authentication mode and string are specified.

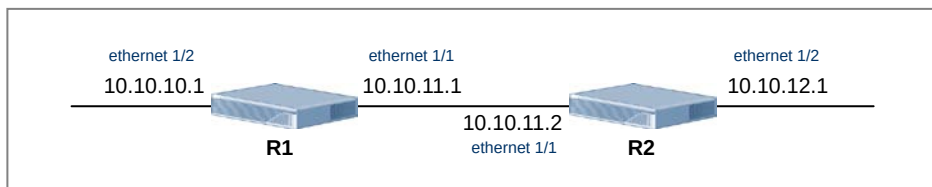
Configuring RIP Split Horizon

The Ubigate iBG router provides RIP split horizon. Using the split horizon command omits routes learned from one neighbor, in updates sent to that neighbor. Using the poisoned parameter with this command includes such routes in updates, but sets their metrics to infinity. Thus, advertising that these routes are not reachable.

Step-by-Step Configuration

Step	Command	Purpose
1	Router# configure terminal	Enters the terminal configuration mode.
2	Router/configure# router rip	Enters the RIP setup mode.
3	Router/configure/router rip# network [interface]/[number of bit masks]	Associates a network to RIP.
4	Router/configure/router rip# redistribute connected	Enables redistributing from connected routes.
5	Router/configure/router rip# exit	Returns to the upper level prompt.
6	Router/configure# interface [interface]	Specify the interface for authentication
7	Router/configure/interface/[interface]# ip rip split-horizon (poisoned)	Perform Split Horizon (with Poisoned Reverse).
8	Router # show ip protocols rip	Displays RIP configuration.

Configuration Example



The following example shows the commands used to configure RIP split horizon for R1.

```

R1# configure terminal
R1/configure# router rip
R1/configure/router rip# network 10.10.11.0/24
R1/configure/router rip# redistribute connected
R1/configure/router rip# exit
R1/configure# interface ethernet 1/1
R1/configure/interface/ethernet(1/1)# ip rip split-horizon
  
```

The following example shows the commands used to configure RIP split horizon with poisoned reverse for R2.

```

R2# configure terminal
R2/configure# router rip
R2/configure/router rip# network 10.10.11.0/24
R2/configure/router rip# redistribute connected
R2/configure/router rip# exit
R2/configure# interface ethernet 1/1
R2/configure/interface/ethernet(1/1)# ip rip split-horizon
poisoned
  
```

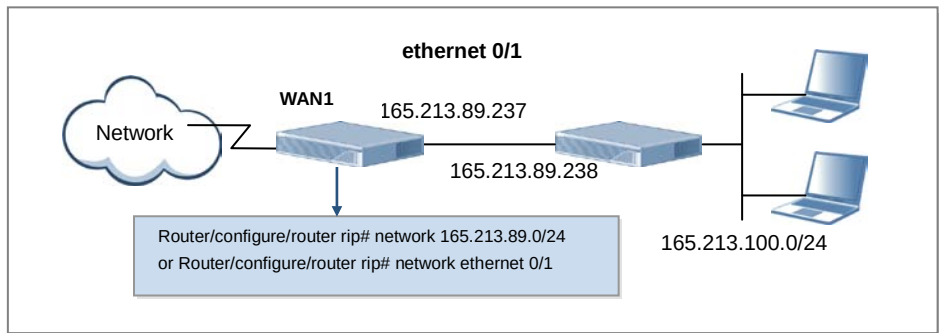
Configuring RIP on a bundle interface

Step-by-Step Configuration

Step	Command	Purpose
1	Router# configure terminal	Enters the terminal configuration mode.
2	Router/configure# router rip	Enters the RIP setup mode.
3	Router/configure/router rip# network [IP address]/[number of bit masks] or Router/configure/router rip# network [interface]	Designates a bundle interface to run RIP on.
4	Router/configure/router rip# end	Returns to the 'Router#' prompt.
5	Router # show ip protocols rip	Display RIP configuration.

Configuration Example

The following figure illustrates a simple network configuration.



The following example shows the commands used to configure RIP using a bundle interface.

```
Router# configure terminal
Router/configure# router rip
Router/configure/router rip# network 165.213.89.0/24
Router/configure/router rip# network wan1
Router/configure/router rip# end
Router# show ip protocols rip
```

Verifying and Troubleshooting Commands

```

debug# rip events
debug# rip packet
debug# rip packet detail
debug# rip packet rcv
debug# rip packet rcv detail
debug# rip packet send
debug# rip packet send detail
show ip rip
show ip rip interface
show ip protocols rip

```

```
Router# show ip rip
```

```
-----
External RIP entry count: 3
-----
```

```
Codes: R - RIP, Rc - RIP connected, Rs - RIP static,
       K - Kernel, C - Connected, S - Static, O - OSPF, B - BGP
```

Network	Next Hop	Metric	From	If	Time
Rc 33.1.1.0/24		1		ethernet3/3	
R 70.1.1.0/24	33.1.1.10	1	33.1.1.10	ethernet3/3	02:57
R 70.1.2.0/24	33.1.1.10	1	33.1.1.10	ethernet3/3	02:57
R 70.1.3.0/24	33.1.1.10	1	33.1.1.10	ethernet3/3	02:57
Rc 192.100.1.0/24		1		ethernet0/2	

```
Router#
```

```

Router# show ip rip interface
ethernet0/2 is up, line protocol is up
  Routing Protocol: RIP
    Receive RIP packets
    Send RIP packets
    Passive interface: Disabled
    Split horizon: Enabled with Poisoned Reversed
    Authentication disabled
    IP interface address:
      192.100.1.1/24
ethernet3/2 is down, line protocol is down

```



```

RIP is enabled, but not running on this interface
ethernet3/3 is up, line protocol is up
Routing Protocol: RIP
  Receive RIP packets
  Send RIP packets
  Passive interface: Disabled
  Split horizon: Enabled with Poisoned Reversed
  Authentication disabled
  IP interface address:
    33.1.1.1/24
Router#

```

```

Router# show ip protocols rip
Routing Protocol is "rip"
  Sending updates every 30 seconds, next due in 18 seconds
  Timeout after 180 seconds, garbage collect after 120
  seconds
  Outgoing update filter list for all interface is not set
  Incoming update filter list for all interface is not set
  Default redistribution metric is 1
  Redistributing:
  Default version control: send version 2, receive version 2
    Interface      Send      Recv      Key-chain
    ethernet0/2    2         2
    ethernet3/3    2         2
  Routing for Networks:
    33.1.1.0/24
    ethernet3/2
    ethernet3/3
    ethernet3/8
    ethernet0/2
  Routing Information Sources:
    Gateway        Distance  Last Update  Bad Packets  Bad
Routes
    33.1.1.10      120      00:00:07      0            0
  Distance: 120 (default is 120)
Router#

```



This page is intentionally left blank.



CHAPTER 5. RIPng

RIP Next Generation (RIPng) is a distance-vector routing protocol for IPv6 that is defined in RFC 2080. RIPng is an adaptation of the RIPv2 protocol to advertise IPv6 network prefixes. RIPng for IPv6 has a simple packet structure and uses UDP port 521 to periodically advertise its routes, respond to requests for routes, and asynchronously advertise route changes.

RIPng for IPv6 has a maximum distance of 15, where 15 is the routing metric (hop count). Locations that are a distance of 16 or further are considered unreachable. RIPng is a simple routing protocol with a periodic route-advertising mechanism designed for use in small to medium-sized IPv6 networks. RIPng does not scale well to a large IPv6 network.



NOTE

The contents of this chapter is applied to SNOS version 2.0.0 or higher.

RIPng Protocol Features

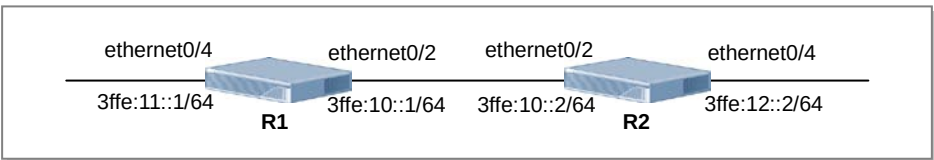
When a RIPng router is initialized, it announces the appropriate routes in its routing table on all interfaces. The RIPng router also sends a General Request message on all interfaces. All neighboring routers send the contents of their routing tables in response. Learned routes are given a 180-second lifetime (by default) before being removed from the IPv6 routing table by RIPng.

After initialization, the RIPng router periodically announces (every 30 seconds, by default) the appropriate routes in its routing table for each interface. The exact set of routes being announced depends on whether the RIPng router is implementing split horizon (where routes are not announced over the interfaces on which they were learned) or split horizon with poison reverse (where routes are announced as unreachable over the interfaces on which they were learned).

Fault tolerance for RIP networks is based on the timeout of RIPng for IPv6-learned routes. If a change occurs in the network topology, RIPng routers can send a triggered update (a routing update, sent immediately) rather than waiting for a scheduled announcement.

Configuring RIPng

This section describes the steps to configure RIP and show a simple example. R1 and R2 are two Ubigate iBG routers connecting to a common network 3ffe:10::/64. They are also connected to network 3ffe:11::/64 and 3ffe:12::/64, respectively.



The following table shows the steps to enable RIPng on a Ubigate iBG router.

Step-by-Step Configuration

Step	Command	Purpose
1	Router# configure terminal	Enters the terminal Configuration mode.
2	Router/configure# interface [interface]	Specifies the interface to be configured and enters the Interface mode.
3	Router/configure/interface/[interface]# ipv6 router rip	Enables RIPng routing on the interface.
4	Router/configure/interface/[interface]# exit	Exits the Interface mode and enters the Configuration mode.
5	Router/configure# router ipv6 rip	Defines a RIPng routing process and enters the Router mode.

Configuration Example

The following example shows the commands used to configure RIPng for R1.

```
R1# configure terminal
R1/configure# interface ethernet 0/2
R1/configure/interface/ethernet (0/2)# ipv6 router rip
R1/configure/interface/ethernet (0/2)# exit
R1/configure# interface ethernet 0/4
R1/configure/interface/ethernet (0/4)# ipv6 router rip
R1/configure/interface/ethernet (0/4)# exit
R1/configure# router ipv6 rip
R1/configure/router/ipv6/rip# end
R1#
```

The following example shows the commands used to configure RIPng for R2.

```
R2# configure terminal
R2/configure# interface ethernet 0/2
R2/configure/interface/ethernet (0/2)# ipv6 router rip
R2/configure/interface/ethernet (0/2)# exit
R2/configure# interface ethernet 0/4
R2/configure/interface/ethernet (0/4)# ipv6 router rip
R2/configure/interface/ethernet (0/4)# exit
R2/configure# router ipv6 rip
R2/configure/router/ipv6/rip# end
R2#
```

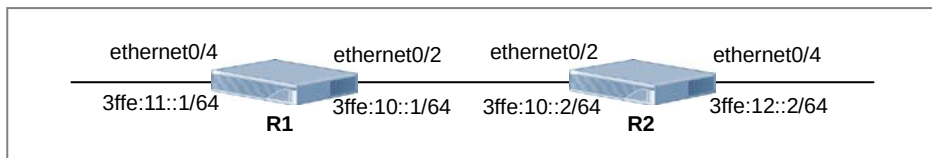
Configuring RIPng Split Horizon

The Ubigate iBG router provides RIPng split horizon. Using the split horizon command omits routes learned from one neighbor, in updates sent to that neighbor. Using the poisoned parameter with this command includes such routes in updates, but sets their metrics to infinity. Thus, advertising that these routes are not reachable.

Step-by-Step Configuration

Step	Command	Purpose
1	Router# configure terminal	Enters the terminal Configuration mode.
2	Router/configure# interface [interface]	Specifies the interface to be configured and enters the Interface mode.
3	Router/configure/interface/[interface]# ipv6 router rip	Enables RIPng routing on the interface.
4	Router/configure/interface/[interface]# exit	Exits the Interface mode and enters the Configuration mode.
5	Router/configure# router ipv6 rip	Defines a RIPng routing process and enters the Router mode.
6	Router/configure/router/ipv6/rip#exit	Exits the Router mode and enters the Configuration mode.
7	Router/configure# interface [interface]	Specifies the interface to be configured and enters the Interface mode.
8	Router/configure/interface/[interface]# ipv6 rip split-horizon (poisoned)	Perform Split Horizon (with Poisoned Reverse).

Configuration Example



The following example shows the commands used to configure RIPng split horizon for R1.

```

R1# configure terminal
R1/configure# interface ethernet 0/2
R1/configure/interface/ethernet (0/2)# ipv6 router rip
R1/configure/interface/ethernet (0/2)# exit
R1/configure# router ipv6 rip
R1/configure/router/ipv6/rip# exit
R1/configure# interface ethernet 0/2
R1/configure/interface/ethernet (0/2)# ipv6 rip split-horizon
  
```

The following example shows the commands used to configure RIPng split horizon with poisoned reverse for R2.

```

R2# configure terminal
R2/configure# interface ethernet 0/2
R2/configure/interface/ethernet (0/2)# ipv6 router rip
R2/configure/interface/ethernet (0/2)# exit
R2/configure# router ipv6 rip
R2/configure/router/ipv6/rip# exit
R2/configure# interface ethernet 0/2
R2/configure/interface/ethernet (0/2)# ipv6 rip split-horizon
  
```

Verifying and Troubleshooting Commands

```

debug# ipv6 rip events
debug# ipv6 rip packet
debug# ipv6 rip packet detail
debug# ipv6 rip packet recv
debug# ipv6 rip packet recv detail
debug# ipv6 rip packet send
debug# ipv6 rip packet send detail
show ipv6 rip
show ipv6 rip interface
show ipv6 protocols rip

```

```
R1# show ipv6 rip
```

```

Codes: R - RIP, Rc - RIP connected, Rs - RIP static,
       Ra - RIP aggregated, Rcx - RIP connect suppressed,
       Rsx - RIP static suppressed, K - Kernel,
       C - Connected, S - Static, O - OSPF, B - BGP

```

Network	Metric	Tag	Time
Next Hop	If		
Rc 1100::/48		1	0
::	ethernet0/2		
Rc 2007:5:28::/48		1	0
::	ethernet3/3		
R 2008:1:1::/64		2	0 02:43
fe80::200:fff:feb6:a2bd	ethernet3/3		
R 2008:1:1:1::/64		2	0 02:43
fe80::200:fff:feb6:a2bd	ethernet3/3		
R 2008:1:1:2::/64		2	0 02:43
fe80::200:fff:feb6:a2bd	ethernet3/3		
R 2008:1:1:3::/64		2	0 02:43
fe80::200:fff:feb6:a2bd	ethernet3/3		
R 2008:1:1:4::/64		2	0 02:43
fe80::200:fff:feb6:a2bd	ethernet3/3		

```
R1#
```



```

R1# show ipv6 rip interface
ethernet0/2 is up, line protocol is up
  Routing Protocol: RIPng
    Passive interface: Disabled
    Split horizon: Enabled with Poisoned Reversed
    IPv6 interface address:
      1100::1/48
      fe80::216:32ff:fe80:1183/10
ethernet3/2 is down, line protocol is down
  RIPng is enabled, but not running on this interface
ethernet3/3 is up, line protocol is up
  Routing Protocol: RIPng
    Passive interface: Disabled
    Split horizon: Enabled with Poisoned Reversed
    IPv6 interface address:
      2007:5:28::1/48
      fe80::216:32ff:fe80:1189/10
ethernet3/5 is down, line protocol is down
  RIPng is enabled, but not running on this interface
ethernet3/8 is down, line protocol is down
  RIPng is enabled, but not running on this interface
R1#

```

```

R1# show ipv6 protocols rip
Routing Protocol is "ripng"
  Sending updates every 30 seconds, next due in 31 seconds
  Timeout after 180 seconds, garbage collect after 120
seconds
  Outgoing update filter list for all interface is not set
  Incoming update filter list for all interface is not set
  Default redistribute metric is 1
  Redistributing: static
  Interface
    ethernet0/2
    ethernet3/3
  Routing for Networks:
  Routing Information Sources:
    Gateway                               Distance  Last Update
    fe80::200:fff:feb6:a2bd              120      00:00:10
  Distance: 120 (default is 120)
R1#

```



This page is intentionally left blank.



CHAPTER 6. OSPF

The Open Shortest Path First (OSPF) protocol is an interior gateway protocol (IGP) that routes packets within a single autonomous system (AS). OSPF uses link-state information to make routing decisions, making route calculations using the shortest path first (SPF) algorithm (also referred to as the Dijkstra algorithm). Each router running OSPF floods link-state advertisements throughout the AS that contain information about that router's attached interfaces and routing metrics. Each router takes the information in these link-state advertisements and creates a complete routing table for the network.

OSPF Protocol Features

OSPF was designed for the TCP/IP environment and as a result explicitly supports IP sub netting and the tagging of externally derived routing information. OSPF also provides for the authentication of routing updates. OSPF routes IP packets based solely on the destination IP address contained in the IP packet header. OSPF quickly detects topological changes, such as when router interfaces become unavailable, and calculates new loop-free routes quickly and with a minimum of routing overhead traffic.

Each interface running OSPF is assigned a cost, which is a unitless number based on factors such as throughput, round-trip time, and reliability, which are used to determine how easy or difficult it is to reach a destination. If two or more routes to a destination have the same cost, OSPF distributes traffic equally among the routes, a process that is called load balancing.

Each router maintains a database that describes the topology of the AS. Each OSPF router has an identical topological database so that all routers in the area have a consistent view of the network. All routers maintain summarized topologies of other areas within an AS. Each router distributes information about its local state by flooding link-state advertisements throughout the AS. When the AS topology changes, OSPF ensures that the contents of all routers' topological databases converge quickly.

Externally derived routing data (for example, routes learned from BGP) is passed transparently throughout the AS. This externally derived data is kept separate from the OSPF link-state data. Each external route can be tagged by the advertising router, enabling the passing of additional information between routers on the boundaries of the AS.

In OSPF, a single AS can be divided into smaller groups called areas. This reduces the number of link-state advertisements and other OSPF overhead traffic sent on the network, and it reduces the size of the topological database that each router must maintain. OSPF network architecture is built around hub-and-spoke topology where the backbone area (designated area id 0.0.0.0) provides the connectivity to the areas that attach to it. Small networks can be accommodated with in a single area and large networks require multi-level area architecture.

System Basic Configuration

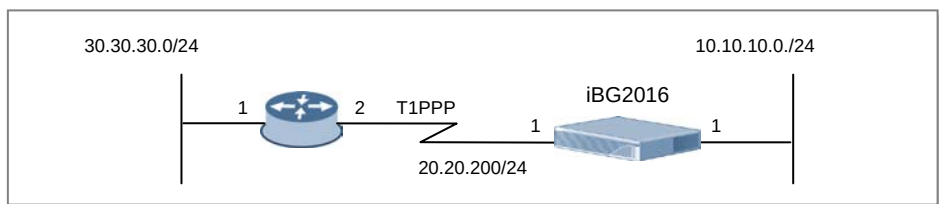
Configuring Host Name

Step-by-Step Configuration

Step	Command	Purpose
1	Router# configure terminal	Enters the terminal configuration mode.
2	Router/configure# hostname [Host Name]	Sets the host name.

Configuration Example

The following figure illustrates a simple network configuration.



The following example shows the commands used to configure the host name in the figure.

```
Router# configure terminal
Router/configure# hostname router
router/configure#
```

Configuring Local Network Interface

Step-by-Step Configuration

Step	Command	Purpose
1	router/configure# interface ethernet [slot/port]	Enters the ethernet interface configuration mode.
2	router/configure/interface/ethernet# ip address [IP address] { [bit mask] [number of bits for mask] }	Sets the local ip address.
3	router/configure/interface/ethernet# exit	Returns to the upper configuration level

Configuration Example

The following example shows the commands used to configure the local network ip address.

```
router/configure# interface ethernet 0/1
router/configure/interface/ethernet(0/1)# ip address
10.10.10.1 24
router/configure/interface/ethernet(0/1)# exit
router/configure#
```

Configuring Bundle Interface: T1 PPP

Step-by-Step Configuration

Step	Command	Purpose
1	router/configure# interface bundle [Bundle Name]	Enters the bundle interface configuration mode.
2	router/configure/interface/bundle [Bundle name]# link t1 { [slot/port] [slot/subslot/port] }	Links T1 interface to the [Bundle Name] bundle interface
3	router/configure/interface/bundle [Bundle name]# encapsulation ppp	Selects PPP as an encapsulation method.
4	router/configure/interface/bundle [Bundle name]# ip address [IP address] { [bit mask] [number of bits for mask] }	Sets the bundle interface ip address.
5	router/configure/interface/bundle [Bundle name]# exit	Returns to the upper configuration level

Configuration Example

The following example shows the commands used to configure the bundle interface.

```
router/configure# interface bundle WAN
router/configure/interface/bundle WAN# link t1 1/1
router/configure/interface/bundle WAN# encapsulation ppp
router/configure/interface/bundle WAN# ip address 20.20.20.1
24
router/configure/interface/bundle WAN# exit
router/configure#
```

Configuring Loopback Interface

Step-by-Step Configuration

Step	Command	Purpose
1	router/configure# interface loopback lo	Enters the loopback interface configuration mode.
2	router/configure/interface/loopback lo# ip address [<i>IP address</i>] { [<i>bit mask</i>] [<i>number of bits for mask</i>] }	Sets the loopback interface ip address.
3	router/configure/interface/loopback lo# [<i>Bundle name</i>]# exit	Returns to the upper configuration level

Configuration Example

The following example shows the commands used to configure the bundle interface.

```
router/configure# interface loopback lo1
router/configure/interface/loopback lo1# ip address 1.1.1.1
32
router/configure/interface/loopback lo#exit
router/configure#
```


Configuring OSPF Router

Configuring OSPF Network Area

Step-by-Step Configuration

Step	Command	Purpose
1	router/configure# router-id [<i>loopback interface ip address</i>]	Sets the router ID. router utilizes its loopback address for the router ID.
2	router/configure# router ospf [<i>Process ID</i>]	Sets OSPF Process ID. Process ID ranges from 0 to 65535
3	router/configure/router/ospf# network [<i>IP address</i>]/[<i>number of bit masks</i>] area [<i>Area ID</i>]	Sets OSPF network. Area ID is an ip address or an integer value from 0 to 4294967295
4	router/configure/router/ospf# exit	Returns to the upper configuration level

Configuration Example

The following example shows the commands used to configure the bundle interface.

```

router/configure# router-id 1.1.1.1
router/configure# router ospf 1
router/configure/router/ospf# network 10.10.10.1/24 area 760
router/configure/router/ospf# network 20.20.20.1/24 area 0
router/configure/router/ospf# exit
router/configure#

```

Configuring OSPF Stub Area

Step-by-Step Configuration

Step	Command	Purpose
1	router/configure# router ospf [<i>Process ID</i>]	Sets OSPF Process ID. Process ID ranges from 0 to 65535
2	router/configure/router/ospf# network [<i>IP address</i>]/[<i>number of bit masks</i>] area [<i>Area ID</i>]	Sets OSPF network. Area ID. Stub area can not configure to backbone area
3	router/configure/router/ospf# area [<i>Area ID</i>] stub	Sets OSPF stub area. Stub area can not configure to vlink or nssa area
4	router/configure/router/ospf# exit	Returns to the upper configuration level

Configuration Example

The following example shows the commands used to configure the bundle interface.

```
router/configure# router ospf 1
router/configure/router/ospf# network 20.20.20.1/24 area 10
router/configure/router/ospf# area 10 stub
router/configure/router/ospf# exit
router/configure#
```

Configuring OSPF NSSA Area

Step-by-Step Configuration

Step	Command	Purpose
1	router/configure# router ospf [Process ID]	Sets OSPF Process ID. Process ID ranges from 0 to 65535
2	router/configure/router/ospf# network [IP address]/[number of bit masks] area [Area ID]	Sets OSPF network. Area ID. Nssa area can not configure to backbone area
3	router/configure/router/ospf# area [Area ID] nssa	Sets OSPF nssa area. Nssa area can not configure to vlink or stub area
4	router/configure/router/ospf# exit	Returns to the upper configuration level

Configuration Example

The following example shows the commands used to configure the bundle interface.

```
router/configure# router ospf 1
router/configure/router/ospf# network 20.20.20.1/24 area 10
router/configure/router/ospf# area 10 nssa
router/configure/router/ospf# exit
router/configure#
```

Configuring OSPF Virtual-Link Area

Step-by-Step Configuration

Step	Command	Purpose
1	router/configure# router ospf [<i>Process ID</i>]	Sets OSPF Process ID. Process ID ranges from 0 to 65535
2	router/configure/router/ospf# network [<i>IP address</i>]/[<i>number of bit masks</i>] area [<i>Area ID</i>]	Sets OSPF network. Area ID. Vlink area can not configure to backbone area
3	router/configure/router/ospf# area [<i>Area ID</i>] vlink [<i>Router-id of neighbor</i>]	Sets OSPF vlink area. Vlink area can not configure to stub or nssa area
4	router/configure/router/ospf# exit	Returns to the upper configuration level

Configuration Example

The following example shows the commands used to configure the bundle interface.

```
router/configure# router ospf 1
router/configure/router/ospf# network 20.20.20.1/24 area 10
router/configure/router/ospf# area 10 vlink 2.2.2.2
router/configure/router/ospf# exit
router/configure#
```

Configuring OSPF Interface

Configuring OSPF Cost

Step-by-Step Configuration

Step	Command	Purpose
1	router/configure# interface ethernet [slot/port]	Enters the interface configuration mode.
2	router/configure/interface/ethernet # ip ospf cost [cost]	Sets OSPF interface cost is an interger value from 1 to 65535
3	router/configure/interface/ethernet # exit	Returns to the upper configuration level

Configuration Example

The following example shows the commands used to configure the interface of ospf interface cost.

```
router/configure# interface ethernet 0/1
router/configure/interface/ethernet (0/1)# ip ospf cost 15
router/configure/interface/ethernet (0/1)# exit
router/configure#
```

Configuring OSPF Priority

Step-by-Step Configuration

Step	Command	Purpose
1	router/configure# interface ethernet [slot/port]	Enters the interface configuration mode.
2	router/configure/interface/ethernet # ip ospf priority [priority]	Sets OSPF interface priority is an integer value from 0 to 255
3	router/configure/interface/ethernet # exit	Returns to the upper configuration level

Configuration Example

The following example shows the commands used to configure the ospf interface priority

```
router/configure# interface ethernet 0/1
router/configure/interface/ethernet (0/1)# ip ospf priority 5
router/configure/interface/ethernet (0/1)# exit
router/configure#
```

Configuring OSPF Authentication (Simple)

Step-by-Step Configuration

Step	Command	Purpose
1	router/configure# interface ethernet [slot/port]	Enters the interface configuration mode.
2	router/configure/interface/ethernet # ip ospf authentication [type]	Enable authentication. (default is simple authentication)
3	router/configure/interface/ethernet # ip ospf authentication-key [word]	Set simple authentication password.
4	router/configure/interface/ethernet # exit	Returns to the upper configuration level

Configuration Example

The following example shows the commands used to configure the ospf simple authentication.

```
router/configure# interface ethernet 0/1
router/configure/interface/ethernet (0/1)# ip ospf
authentication
router/configure/interface/ethernet (0/1)# ip ospf
authentication-key samsung
router/configure/interface/ethernet (0/1)# exit
router/configure#
```

Configuring OSPF Authentication (Message-digest)

Step-by-Step Configuration

Step	Command	Purpose
1	router/configure# interface ethernet [slot/port]	Enters the interface configuration mode.
2	router/configure/interface/ethernet # ip ospf authentication [type]	Enable authentication. (default is simple authentication)
3	router/configure/interface/ethernet # ip ospf message-digest-key [key-id] md5 [word]	Set message digest authentication password.
4	router/configure/interface/ethernet # exit	Returns to the upper configuration level

Configuration Example

The following example shows the commands used to configure the ospf message-digest authentication

```
router/configure# interface ethernet 0/1
router/configure/interface/ethernet (0/1)# ip ospf
authentication message-digest
router/configure/interface/ethernet (0/1)# ip ospf message-
digest-key 1 md5 samsung
router/configure/interface/ethernet (0/1)# exit
router/configure#
```


Configuring OSPF Interface Parameter

Step-by-Step Configuration

Step	Command	Purpose
1	router/configure# interface ethernet [slot/port]	Enters the interface configuration mode.
2	router/configure/interface/ethernet # ip ospf hello-interval [interval]	Sets OSPF hello packet time interval is an integer value from 1 to 65535
3	router/configure/interface/ethernet # ip ospf dead-interval [interval]	Sets OSPF neighbor dead time interval is an integer value from 1 to 65535
4	router/configure/interface/Ethernet # ip ospf retransmit-interval [interval]	Set time between retransmitting lost link state advertisement interval is an integer value from 1 to 65535
5	router/configure/interface/ethernet # ip ospf transmit-delay [delay]	Set link state transmit delay interval is an integer value from 1 to 65535
6	router/configure/interface/ethernet # exit	Returns to the upper configuration level

Configuration Example

The following example shows the commands used to configure the ospf interface parameter.

```

router/configure# interface ethernet 0/1
router/configure/interface/ethernet (0/1)# ip ospf hello-
interval 5
router/configure/interface/ethernet (0/1)# ip ospf dead-
interval 10
router/configure/interface/ethernet (0/1)# ip ospf
retransmit-interval 20
router/configure/interface/ethernet (0/1)# ip ospf transmit-
delay 30
router/configure/interface/ethernet (0/1) # exit
router/configure#

```

Verifying and Troubleshooting Commands

```
debug# ip ospf ifsm
debug# ip ospf nfsm
debug# ip ospf packet
show ip ospf
show ip ospf interface
show ip ospf neighbor
show ip ospf virtual-links
show ip ospf database
show ip ospf route
```

To display information for OSPF status (neighbor/interface/OSPF router).

```
router# show ip ospf
Routing Process "ospf 1" with ID 1.1.1.1
Process uptime is 5 minutes
Process bound to VRF default
Conforms to RFC2328, and RFC1583Compatibility flag is
disabled
Supports only single TOS(TOS0) routes
Supports opaque LSA
This router is an ABR, ABR Type is Alternative Cisco
(RFC3509)
SPF schedule delay 5 secs, Hold time between two SPFs 10
secs
Refresh timer 10 secs
Number of incoming current DD exchange neighbors 0/5
Number of outgoing current DD exchange neighbors 0/5
Number of external LSA 0. Checksum 0x0000000
Number of opaque AS LSA 0. Checksum 0x0000000
Number of non-default external LSA 0
External LSA database is unlimited.
Number of LSA originated 6
Number of LSA received 4
Number of areas attached to this router: 2
  Area 0 (BACKBONE)
    Number of interfaces in this area is 1(1)
    Number of fully adjacent neighbors in this area is 1
    Area has no authentication
    SPF algorithm last executed 00:00:21.110 ago
    SPF algorithm executed 4 times
    Number of LSA 7. Checksum 0x03296d
```

```

Area 760
  Number of interfaces in this area is 1(1)
  Number of fully adjacent neighbors in this area is 0
  Number of fully adjacent virtual neighbors through
this area is 0
  Area has no authentication
  SPF algorithm last executed 00:00:21.110 ago
  SPF algorithm executed 1 times
  Number of LSA 2. Checksum 0x008a7b

```

```

router# show ip ospf interface
ethernet0/1 is up, line protocol is up
  Internet Address 10.10.10.1/24, Area 0.0.2.248, MTU 1500
  Process ID 1, Router ID 1.1.1.1, Network Type BROADCAST,
Cost: 15
  Transmit Delay is 130 sec, State DR, Priority 5, TE Metric
15
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 5, Dead 10, Wait 10,
Retransmit 520
    Hello due in 00:00:04
  Neighbor Count is 0, Adjacent neighbor count is 0
  Authentication disabled
  Crypt Sequence Number is 946740454
  Hello received 0 sent 5585, DD received 0 sent 0
  LS-Req received 0 sent 0, LS-Upd received 0 sent 0
  LS-Ack received 0 sent 0, Discarded 0

```

```

router# show ip ospf neighbor
OSPF process 1:

```

Neighbor ID	Pri	State	Dead Time	Address	Interface
2.2.2.2	1	Full/ -	00:00:40	20.20.20.2	WAN
2.2.2.2	1	Full/ -	00:00:37	20.20.20.2	VLINK0

```

router# show ip ospf virtual-links
Virtual Link VLINK0 to router 2.2.2.2 is up
  Transit area 0.0.0.10 via interface WAN, Cost of using 65
  Local address 20.20.20.1/32
  Remote address 20.20.20.2/32
  Transmit Delay is 1 sec, State Point-To-Point,
  Timer intervals configured, Hello 10, Dead 40, Wait 40,
  Retransmit 5
    Hello due in 00:00:04
    Adjacency state Full
    Authentication disabled

```

```

router# show ip ospf database

          OSPF Router with ID (2.2.2.2) (Process ID 1)

          Router Link States (Area 0.0.0.10)

Link ID      ADV Router    Age Seq#          CkSum Link
count
2.2.2.2      2.2.2.2              1805 0x80000000c 0x9426 1

          Area-Local Opaque-LSA (Area 0.0.0.10)

Link ID      ADV Router    Age Seq#          CkSum Opaque ID
1.0.0.1      2.2.2.2              688 0x800000007 0x0a2f 1

          Router Link States (Area 0.0.2.248)

Link ID      ADV Router    Age Seq#          CkSum Link
count
2.2.2.2      2.2.2.2              66 0x800000007 0xd53e 1

```

```

router# show ip ospf route

OSPF process 1:
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter
area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA
external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2

```

```
C 10.10.10.0/24 [10] is directly connected, lo1, Area
0.0.2.248
C 20.20.20.0/24 [65] is directly connected, WAN, Area
0.0.0.10
```



This page is intentionally left blank.



CHAPTER 7. OSPFv3

OSPFv3 Protocol Features

OSPFv3 adds support for IPv6 in the Open Shortest Path First (OSPF) routing protocol, as detailed in RFC 2740. Most configuration and operational commands function essentially the same as in OSPFv2

- Using same basic packet type
Hello, DataDescription, Ls-request, Ls-update, Ls-ack
- Using same mechanisms for neighbor discovery and adjacency formation.
- Using same interface type
P2P, Broadcast, NBMA, Virtual link
- Using same LSA flooding and ageing
- Almost same LSA types.

IPv6 supports OSPFv3, which functions similarly to OSPFv2, the current version that IPv4 supports, except for the following enhancements:

- Support for IPv6 addresses and prefixes.
- In general, you can configure several IPv6 addresses on a router interface. OSPFv3 imports all or none of the address prefixes configured on a router interface. You cannot select which addresses to import.
- OSPFv3 now runs on a per-link basis, instead of on a per-IP-subnet basis. IPv6 link-local addresses are used for OSPFv3 neighbor exchanges (except over virtual links).
- You can run one instance of OSPFv2 and one instance of OSPFv3 concurrently on a link.
- IPv6 link state advertisements (LSAs).

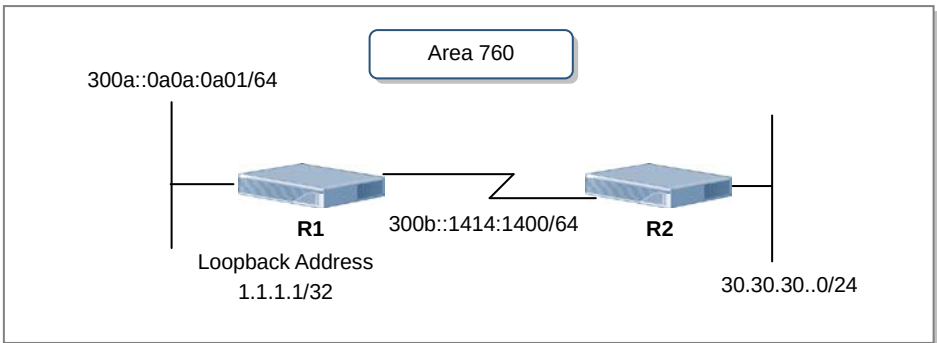
- Authentication has been removed from the OSPFv3 protocol itself and relies on the Authentication Header (AH) and Encapsulating Security Payload (ESP) portions of the IP Security protocol (IPSec) for all authentication tasks in IPv6.



The contents of this chapter is applied to SNOS version 2.0.0 or higher.

System Basic Configuration

The following example shows an iBG router connected to a router over a single T1 link. IPv6 addresses 300a::0a0a:0a01, 300b::1414:1400, and 300b::1414:1401 are assigned to area 760.



Configuring IPv6 unicast routing

Step-by-Step Configuration

Step	Command	Purpose
1	router/configure# ipv6 unicast-routing	Enable ipv6 unicast forwarding

Configuration Example

The following example shows the commands used to enable IPv6 unicast forwarding.

```
router/configure# ipv6 unicast-routing
router/configure# exit
```


Configuring Interface ethernet 0/1

Step-by-Step Configuration

Step	Command	Purpose
1	router/configure# interface ethernet [slot/port]	Enters the ethernet interface configuration mode.
2	router/configure/interface/ethernet# ipv6 address [IP address] [bit mask]	Sets the local IPv6 address.
3	router/configure/interface/ethernet# exit	Returns to the upper configuration level.

Configuration Example

The following example shows the commands used to configure the local network IPv6 address.

```
router/configure# interface ethernet 0/1
router/configure/interface/ethernet(0/1)# ipv6 address
300a::0a0a:0a01/64
router/configure/interface/ethernet(0/1)# exit
router/configure#
```

Configuring Interface bundle Suwon

Step-by-Step Configuration

Step	Command	Purpose
1	router/configure# interface bundle [Bundle Name]	Enters the bundle interface configuration mode.
2	router/configure/interface/bundle [Bundle name]# link t1 { [slot/port] [slot/subslot/port] }	Links T1 interface to the [Bundle Name] bundle interface
3	router/configure/interface/bundle [Bundle name]# encapsulation ppp	Selects PPP as an encapsulation method.
4	router/configure/interface/bundle [Bundle name]# ipv6 address [IP address] [bit mask]	Sets the bundle interface IPv6 address.
5	router/configure/interface/bundle [Bundle name]# exit	Returns to the upper configuration level

Configuration Example

The following example shows the commands used to configure the bundle interface.

```
router/configure# interface bundle Suwon
router/configure/interface/bundle Suwon# link t1 1/1
router/configure/interface/bundle Suwon# encapsulation ppp
router/configure/interface/bundle Suwon# ipv6 address
300b::1414:1401/64
router/configure/interface/bundle Suwon# exit
router/configure#
```

Configuring Loopback Interface

Step-by-Step Configuration

Step	Command	Purpose
1	router/configure# interface loopback lo	Enters the loopback interface configuration mode.
2	router/configure/interface/loopback lo# ipv6 address [IP address] [bit mask]	Sets the loopback interface IPv6 address.
3	router/configure/interface/loopback lo# [Bundle name]# exit	Returns to the upper configuration level.

Configuration Example

The following example shows the commands used to configure the loopback interface.

```
router/configure# interface loopback lo1
router/configure/interface/loopback lo1# ip address 1.1.1.1
32
router/configure/interface/loopback lo#exit
router/configure#
```

Configuring OSPFv3 router

Step-by-Step Configuration

Step	Command	Purpose
1	router/configure# router ipv6 ospf [tag tag]	Sets OSPF tag. Tag can use WORD.
2	router/configure/router/ipv6/ospf# exit	Returns to the upper configuration level.

Configuration Example

The following example shows the commands used to configure the OSPFv3 router.

```
router/configure# router ipv6 ospf 100
router/configure/router/ipv6/ospf# exit
router/configure#
```

Configuring OSPFv3 Area

Configuring Network Area

Step-by-Step Configuration

Step	Command	Purpose
1	router/configure/interface/ethernet# ipv6 router ospf area [Area ID] tag [tag]	Sets OSPF area and tag. Area ID is an IP address or an integer value from 0 to 4294967295. Tag is the ospf process ID and is optional.
2	router/configure# router ipv6 ospf tag[tag]	Enable IPv6 OSPF router. Tag is the ospf process ID and is optional
3	router/configure/router/ospf# exit	Returns to the upper configuration level

Configuration Example

The following example shows the commands used to configure the OSPFv3 router.

```
router/configure/ethernet (0/1)# ipv6 router ospf area 760
tag 100
router/configure/ethernet (0/1)# exit
router/configure#int bundle Suwon
router/configure/interface/bundle Suwon# ipv6 router ospf
area 760 tag 100
router/configure/interface/bundle Suwon# exit
router/configure#router ipv6 ospf 100
router/configure/router/ospf# exit
```

Configuring Stub Area

Step-by-Step Configuration

Step	Command	Purpose
1	router/configure# router ipv6 ospf [tag tag]	Sets OSPF tag. Tag can use WORD.
2	router/configure/router/ipv6/ospf# area [Area ID] stub	Sets OSPF stub area. Stub area can not configure to backbone or vlink area
3	router/configure/router/ipv6/ospf# exit	Returns to the upper configuration level.

Configuration Example

The following example shows the commands used to configure the OSPFv3 stub area.

```
router/configure# router ipv6 ospf 100
router/configure/router/ipv6/ospf# area 760 stub
router/configure/router/ipv6/ospf# exit
router/configure#
```

Configuring Virtual-Link Area

Step-by-Step Configuration

Step	Command	Purpose
1	router/configure# router ipv6 ospf [tag tag]	Sets OSPF tag. Tag can use WORD.
2	router/configure/router/ipv6/ospf# area [Area ID] vlink [Router-id of neighbor]	Sets OSPF vlink area. Vlink area can not configure to backbone or stub area
3	router/configure/router/ipv6/ospf# exit	Returns to the upper configuration level.

Configuration Example

The following example shows the commands used to configure the OSPFv3 router.

```
router/configure# router ipv6 ospf 100
router/configure/router/ipv6/ospf# area 760 virtual-link
2.2.2.2
router/configure/router/ipv6/ospf# exit
router/configure#
```

Configuring OSPFv3 Interface

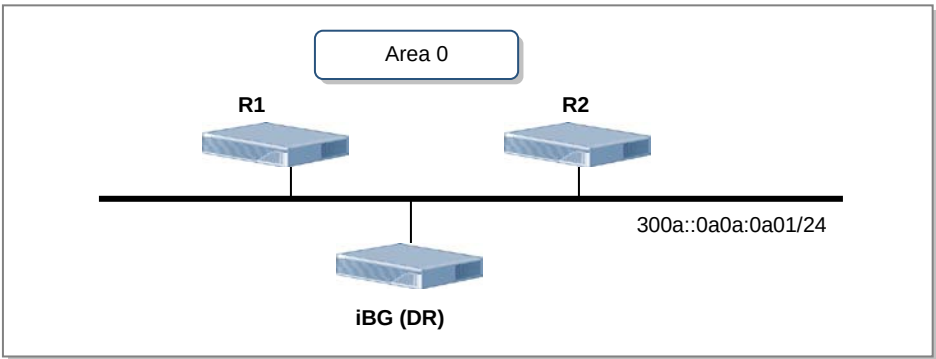
Configuring OSPFv3 Priority

Step-by-Step Configuration

Step	Command	Purpose
1	router/configure/interface/ethernet# ipv6 ospf v3 priority [priority]	Sets OSPF priority. The priority is an integer value from 0 to 255.

Configuration Example

This example shows the configuration for setting the priority for an interface. You can set a high priority for a router to make it the Designated Router (DR). Router iBG is configured to have a priority of 10, which is higher than the default priority (default priority is 1) of R1 and R2; making it the DR.



```
router/configure/ethernet (0/1)# ipv6 ospf priority 10
```

Configuring OSPFv3 Cost

Step-by-Step Configuration

Step	Command	Purpose
1	router/configure/interface/ethernet# ipv6 ospf v3 cost [cost]	Sets OSPF priority. The priority is an integer value from 1 to 65535.

Configuration Example

```
router/configure/ethernet (0/1)# ipv6 ospf cost 15
```

Configuring OSPFv3 Interface Parameter

Step-by-Step Configuration

Step	Command	Purpose
1	router/configure/interface/ethernet# ipv6 ospf v3 hello-interval [interval]	Sets time between HELLO packets. The interval is an integer value from 1 to 65535.
2	router/configure/interface/ethernet# ipv6 ospf v3 dead-interval [interval]	Sets interval after which a neighbor is declared dead. The interval is an integer value from 1 to 65535.
3	router/configure/interface/ethernet# ipv6 ospf v3 retransmit-interval [interval]	Sets time between retransmitting lost link state advertisements. The interval is an integer value from 1 to 65535.
4	router/configure/interface/ethernet# ipv6 ospf v3 transmit-delay [delay]	Sets link state transmit delay. The delay is an integer value from 1 to 65535.

Configuration Example

```
router/configure/ethernet (0/1)# ipv6 ospf hello-interval 5
router/configure/ethernet (0/1)# ipv6 ospf dead-interval 10
router/configure/ethernet (0/1)# ipv6 ospf transmit-delay 4
router/configure/ethernet (0/1)# ipv6 ospf retransmit-
interval 7
```

Verifying and Troubleshooting Commands

```

debug# ipv6 ospf ifsm
debug# ipv6 ospf nfsm
debug# ipv6 ospf packet
show ipv6 ospf
show ipv6 ospf interface
show ipv6 ospf neighbor
show ipv6 ospf virtual-links
show ipv6 ospf database
show ipv6 ospf route

```

Use the following commands to verify neighbor, interface, and OSPFv3 information. Note: For details on the commands used in the following example, refer to the Ubigate iBG Command Reference.

```

router# show ipv6 ospf
Routing Process "OSPFv3 (100)" with ID 1.1.1.1
SPF schedule delay 5 secs, Hold time between SPFs 10 secs
Minimum LSA interval 5 secs, Minimum LSA arrival 1 secs
Number of external LSA 0. Checksum Sum 0x0000
Number of AS-Scoped Unknown LSA 0
Number of LSA originated 4
Number of LSA received 3
Number of areas in this router is 1
  Area 0.0.2.248
    Number of interfaces in this area is 2
    SPF algorithm executed 4 times
    Number of LSA 3. Checksum Sum 0x18DEF
    Number of Unknown LSA 0

```

```

router# show ipv6 ospf neighbor
OSPFv3 Process (100)
Neighbor ID  Pri  State   Dead Time  Interface  Instance ID
2.2.2.2      1   Full/ -  00:00:33  SUWON      0

```



```

router# show ipv6 ospf neighbor
router# show ipv6 ospf interface
ethernet0/1 is up, line protocol is up
  Interface ID 5
  IPv6 Prefixes
    fe80::216:32ff:fe80:705/10 (Link-Local Address)
    300a::a0a:a01/64
  OSPFv3 Process (100), Area 0.0.2.248, Instance ID 0
  Router ID 1.1.1.1, Network Type BROADCAST, Cost: 15
  Transmit Delay is 4 sec, State DR, Priority 10
  Designated Router (ID) 1.1.1.1
    Interface Address fe80::216:32ff:fe80:705
  No backup designated router on this link
  Timer interval configured, Hello 5, Dead 10, Wait 10,
  Retransmit 7
    Hello due in 00:00:02
  Neighbor Count is 0, Adjacent neighbor count is 0
Suwon is up, line protocol is up
  Interface ID 71
  IPv6 Prefixes
    fe80::216:32ff:fe80:700/10 (Link-Local Address)
    300b::1414:1401/64
  OSPFv3 Process (100), Area 0.0.2.248, Instance ID 0
  Router ID 1.1.1.1, Network Type POINTOPOINT, Cost: 65
  Transmit Delay is 1 sec, State Point-To-Point, Priority 1
  No designated router on this link
  No backup designated router on this link
  Timer interval configured, Hello 10, Dead 40, Wait 40,
  Retransmit 5
    Hello due in 00:00:06
  Neighbor Count is 1, Adjacent neighbor count is 1

```

```

router# show ipv6 ospf neighbor
OSPFv3 Process (100)
Neighbor ID    Pri  State           Dead Time  Interface
Instance ID
2.2.2.2        1   Full/ -         00:00:33   Suwon      0
2.2.2.2        1   Full/ -         00:00:33   VLINK1     0

```

```

router# show ipv6 ospf virtual-links
Virtual Link VLINK1 to router 2.2.2.2 is up
  Transit area 0.0.2.248 via interface Suwon, instance ID 0
  Local address 300b::1414:1401/128
  Remote address 300b::1414:1402/128
  Transmit Delay is 1 sec, State Point-To-Point,
  Timer intervals configured, Hello 10, Dead 40, Wait 40,
  Retransmit 5
    Hello due in 00:00:06
    Adjacency state Full

```

```

router# show ipv6 ospf database

        OSPFv3 Router with ID (1.1.1.1) (Process 100)

        Link-LSA (Interface ethernet0/4)

Link State ID    ADV Router    Age Seq#      CkSum Prefix
0.0.0.5          1.1.1.1          448 0x800000001 0x7ec8    1

        Link-LSA (Interface Suwon)

Link State ID    ADV Router    Age Seq#      CkSum Prefix
0.0.0.71         1.1.1.1          1159 0x800000002 0x7c94    1
0.0.0.72         2.2.2.2          1126 0x800000002 0xff8e    1

        Router-LSA (Area 0.0.0.0)

Link State ID    ADV Router    Age Seq#      CkSum Link
0.0.0.0          1.1.1.1          621 0x800000003 0xa921    1
0.0.0.0          2.2.2.2          621 0x800000003 0x3991    1

        Inter-Area-Prefix-LSA (Area 0.0.0.0)

Link State ID    ADV Router    Age Seq#      CkSum
0.0.0.2          1.1.1.1          627 0x800000002 0x6310
0.0.0.3          1.1.1.1          622 0x800000003 0x03e7
0.0.0.5          1.1.1.1          447 0x800000001 0x0e96
0.0.0.1          2.2.2.2          454 0x800000003 0x9bc5
0.0.0.3          2.2.2.2          627 0x800000002 0x3b33
0.0.0.4          2.2.2.2          622 0x800000001 0xc424

        Router-LSA (Area 0.0.2.248)

```

Link State ID	ADV Router	Age	Seq#	CkSum	Link
0.0.0.0	1.1.1.1	438	0x8000000e	0x58d9	1
0.0.0.0	2.2.2.2	622	0x80000007	0xf147	1
Intra-Area-Prefix-LSA (Area 0.0.2.248)					
Link State ID	ADV Router	Age	Seq#	CkSum	Prefix Reference
0.0.0.1	1.1.1.1	437	0x80000011	0xfeca	3
Router-LSA					
0.0.0.1	2.2.2.2	621	0x80000007	0x64fc	2
Router-LSA					

router# show ipv6 ospf route	
OSPFv3 Process (100)	
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area	
E1 - OSPF external type 1, E2 - OSPF external type 2	
Destination	Metric
Next-hop	
C 300a::/64	15
directly connected, ethernet0/1	
C 300b::/64	65
directly connected, Suwon	
O 300b::1414:1402/128	65
via fe80::216:32ff:fe80:2460, Suwon	



This page is intentionally left blank.



CHAPTER 8. BGP

The Border Gateway Protocol (BGP) is an exterior gateway protocol (EGP) that is used to exchange routing information among routers in different Autonomous Systems (ASs). BGP routing information includes the complete route to each destination. BGP uses the routing information to maintain a database of network reachability information, which it exchanges with other BGP systems. BGP uses the network reachability information to construct a graph of AS connectivity, thus allowing BGP to remove routing loops and enforce policy decisions at the AS level.

BGP allows for policy-based routing. You can use routing policies to choose among multiple paths to a destination and to control the redistribution of routing information. BGP uses the Transmission Control Protocol (TCP) as its transport protocol, using port 179 for establishing connections. Running over a reliable transport protocol eliminates the need for BGP to implement update fragmentation, retransmission, acknowledgment, and sequencing. BGP supports classless inter-domain routing (CIDR), which eliminates the concept of network classes. Instead of assuming which bits of an address represent the network by looking at the first octet, CIDR allows you to explicitly specify the number of bits in the network address, thus providing a means to decrease the size of the routing tables. BGP also supports aggregation of routes, including the aggregation of AS paths.

BGP is essentially a Distance Vector protocol that uses TCP as its transport protocol. It runs between exactly two nodes. These two nodes establish a BGP session between them and are known as BGP peers of each other. On connection start, BGP peers exchange complete copies of their routing tables, which can be quite large. However, only changes (deltas) are subsequently exchanged, which makes long running BGP sessions more efficient than shorter ones.

BGP's basic unit of routing information is the BGP path, a route to a certain set of CIDR prefixes. Paths are tagged with various path attributes, of which the most important are AS_PATH and NEXT_HOP. One of BGP's most important functions is loop detection at the Autonomous System (AS) level, using the AS_PATH attribute. Simply put, an AS_PATH is a list of Autonomous Systems that a route goes through to reach its destination. The syntax of this attribute is made more complex by its need to support path aggregation, when multiple paths are collapsed into one to simplify further route advertisements. Loops are detected and avoided by checking for the router's own AS number in AS_PATHs received from its BGP peers. Every time a BGP path advertisement crosses an AS boundary, the NEXT_HOP attribute is changed to the IP address of the boundary router. However, when a BGP path advertisement is passed among BGP speakers in the same AS, the NEXT_HOP attribute is left untouched. Consequently, BGP's NEXT_HOP is always the IP address of the first BGP router in the next autonomous system, even though this may actually be several hops away. The AS's interior routing protocol is responsible for computing an interior route to reach the BGP NEXT_HOP. This leads to the distinction between Internal BGP (IBGP) sessions (between routers in the same AS) and External BGP (EBGP) sessions (between routers in different ASs). NEXT_HOPs are only changed across EBGP sessions, but left intact across IBGP sessions. Also, BGP does not relay routing traffic from one IBGP session to another, only from an EBGP session to an IBGP session or another EBGP session. The most important consequences of such a design are the need for interior routing protocols to reach one hop beyond the AS boundary and the need for BGP sessions within an AS to be fully meshed. Since the NEXT_HOP contains the IP address of a router interface in the next autonomous system, and this IP address is used to perform routing, the interior routing protocol must be able to route to this address. This means that interior routing tables must include entries one hop beyond the AS boundary. When a BGP routing update is received from a neighboring AS, it must be relayed directly to all other BGP speakers in the AS.

It is the responsibility of the BGP implementation to select among competing paths. RFC 1771 states only that 'The computation be based on pre-configured policy information. The exact nature of this policy information and the computation involved is a local matter.' Since the AS_PATH attribute includes a list of Autonomous Systems used to reach the destination, it is possible to implement primitive policy decisions such as 'avoid all routes through AS x'.

Protocol Features

The following BGP features such as aggregation, route reflection, AS confederation, and etc will be supported on the Ubigate iBG router.

Aggregation is the process of combining the characteristics of several different routes in such a way that a single route can be advertised. Aggregation reduces the amount of information a BGP speaker stores and exchanges with other speakers. It can be part of the decision process to reduce the amount of routing information that will be placed in the Adj-RIBs-Out. The general rule of route aggregation is that routes can be aggregated if and only if the corresponding attributes of the routes are identical.

Route reflection is used to solve the problem of full mesh IBGP in an AS with a large number of routing nodes. Multiple BGP routers can peer with a central server, the route reflector, and then route reflectors can peer with one another. The BGP routers peered with the reflector exchange routing information with it and it, in turn, passes (or reflects) the information between clients and to other IBGP and EBGp peers.

AS confederations is a second approach to solve the scaling problem with full-mesh IBGP sessions. This approach divides a given AS into many sub-ASs. For other ASs, this AS doesn't look any different from the outside. There is a full-mesh of IBGP sessions within a sub-AS. BGP sessions between routers in different sub-ASs (of the same confederation) are like EBGp sessions, but with some differences. They are sometimes referred to as EIBGP sessions.

A route in the routing table may disappear and reappear intermittently. This is known as flapping. It occurs when BGP sends a routing table and then withdraws it. A route that appears and disappears intermittently and repeatedly, propagates BGP UPDATE and WITHDRAW messages on to the Internet. This excessive flow of traffic can use up bandwidth and drive up CPU utilization of routers. Route flap dampening is used to prevent this kind of excessive traffic due to route flapping.

Routes are categorized as either well-behaved or ill-behaved. A well-behaved route shows a high degree of stability during an extended period of time (as determined by configurable limits). Ill-behaved routes are no longer advertised but suppressed until there is some indication that the route has become stable.

The BGP community attribute simplifies the configuration of complex policies. It enables an identifier to be associated with a route. Routes that are supposed to receive the same treatment with respect to policy can be assigned the same identifier. The community attribute dynamically influences the routing decisions of autonomous systems. For e.g., in a topology of two autonomous systems AS1 and AS2, AS1 can advertise a route to AS2 and simultaneously provide dynamic instructions that AS2 is not to advertise the route externally. It does so by setting the COMMUNITY attribute (assigned to the advertised route) to no-export.

Normally, whenever changes are made to the attributes or policies of a route, the BGP TCP session with its neighbor has to be reset in order for the modified routing behavior to take effect. When a session is reset, the routing cache is invalidated, routes disappear and route instability increases and is propagated throughout the Internet. To prevent this, a mechanism called soft reconfiguration is used. It allows attribute reconfigurations to be made without terminating an already established TCP session. This is a means of requesting that a peer re-advertise all the prefixes learned from other peers (its Adj-RIB-Out).

The purpose of Capability Negotiation is to facilitate the introduction of new features in BGP by providing graceful capability negotiation without requiring the BGP peers to be terminated. It is achieved with the addition of a new optional parameter called 'Capabilities' in the Optional Parameters field of the OPEN message.

Route maps are used with BGP to control and modify routing information and to define the conditions by which routes are redistributed between routers and routing processes.

Access lists based on AS path enables control of routing updates based on BGP AS path information. To control updates for all routes to or from an autonomous system, filtering based on AS path is more efficient than listing each route individually.

BGP community list is a user defined BGP community's attribute list. BGP community list can be used for matching or manipulating BGP communities attribute in updates. Valid list numbers are 1-199.

Prefix lists are yet another way of implementing BGP policy. A Prefix List enables filtering of route advertisements based on IP prefixes.

This is a group of BGP neighbors that share update policies. Instead of defining the same policies for several individual peers, a peer group is defined and policies are assigned to the group. That way, the operator is saved from repetitive configuration. It also reduces the load on system resources by allowing the routing table to be checked only once, and updates to be replicated to all peer group members instead of formulating updates individually for each peer in the peer group.

Multi-protocol BGP (MBGP) can be used to carry routing information for the IPv6 address family. All BGP commands and routing policy capabilities can be used with IPv6 addresses. Other address families (like IPv4 multicast, IPv6 multicast) will not be supported as part of MBGP.

Minimum BGP Configuration

This Section shows the minimum configuration for BGP running.

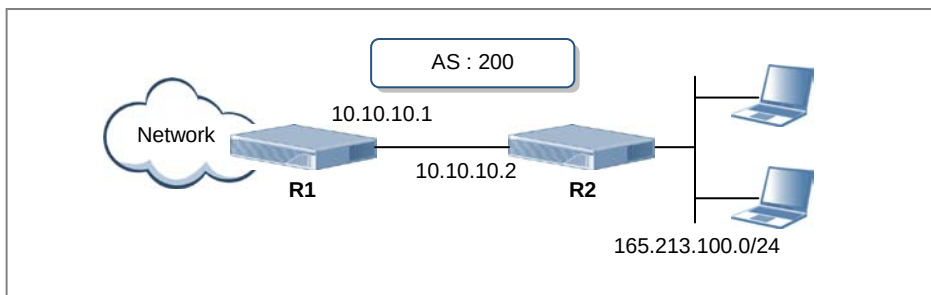
Configuring BGP in the same AS

Step-by-Step Configuration

Step	Command	Purpose
1	Router# configure terminal	Enters the terminal configuration mode.
2	Router/configure# router bgp [Autonomous Number]	Enters a BGP configuration mode.
3	Router/configure/router/bgp [AS No.]# neighbor [IP address] remote-as [Autonomous Number]	Defines a BGP neighbor with its ip address and autonomous number.

Configuration Example

In the figure, R1 and R2 are two Ubigate iBG routers belonging to the same AS (autonomous system) with the ID of 200.



The following example shows the commands used to configure the BGP for R1 in the figure.

```
R1# configure terminal
R1/configure# router bgp 200
R1/configure/bgp 200# neighbor 10.10.10.2 remote-as 200
```

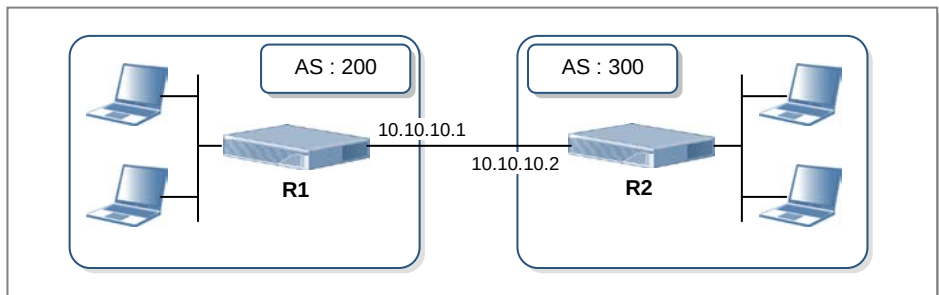
The following example shows the commands used to configure the BGP for R2 in the figure.

```
R2# configure terminal
R2/configure# router bgp 200
R2/configure/bgp 200# neighbor 10.10.10.1 remote-as 200
```

Configuring BGP in the different AS

Configuration Example

The following figure shows two Ubigate iBG routers in the different AS.



The following example shows the commands used to configure the BGP for R1 in the figure.

```
R1# configure terminal
R1/configure# router bgp 200
R1/configure/bgp 200# neighbor 10.10.10.2 remote-as 300
```

The following example shows the commands used to configure the BGP for R2 in the figure.

```
R2# configure terminal
R2/configure# router bgp 300
R2/configure/bgp 200# neighbor 10.10.10.1 remote-as 200
```

BGP Application using Route-Map

This section describes how to associate a route-map with BGP.

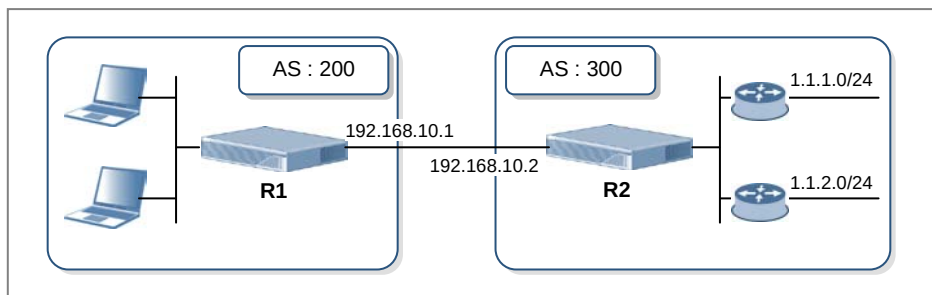
Configuring Route-Map and BGP in R1

Step-by-Step Configuration

Step	Command	Purpose
1	R1# configure terminal	Enters the terminal configuration mode.
2	R1/configure# ip prefix-list [<i>prefix name</i>] { options }	Makes a prefix-list
3	R1/configure# route-map [<i>prefix name</i>] permit 1	Enters the route-map mode to set the match operation.
4	R1/configure/route-map# match ip address prefix-list [<i>prefix name</i>]	Set the match criteria.
5	R1/configure/route-map# exit	Returns to the upper configuration level
6	R1/configure# router bgp [id]	Enters a BGP configuration mode.
7	R1/configure/router/bgp [id]# neighbor 192.168.10.2 remote-as 300	Defines a BGP neighbor with its ip address and autonomous number.
8	R1/configure/router/bgp [id]# neighbor [<i>IP address</i>] route-map [<i>prefix name</i>] in	Applies a route-map to routes for incoming advertisements.

Configuration Example

In the figure, R1 and R2 are the Ubigate iBG routers in the different autonomous systems.



The following example shows the commands used to configure the BGP using Route-Map for R1.

```
R1# configure terminal
R1/configure# ip prefix-list inpf seq 5 deny 1.1.1.0/24 ge
26 le 28
R1/configure# ip prefix-list inpf seq 10 permit any
R1/configure# route-map inpf permit 1
R1/configure/route-map# match ip address prefix-list inpf
R1/configure/route-map# exit
R1/configure# router bgp 200
R1/configure/bgp 200# neighbor 192.168.10.2 remote-as 300
R1/configure/bgp 200# neighbor 192.168.10.2 route-map inpf
in
```

The following example shows the commands used to configure the BGP for R2.

```
R1# configure terminal
R1/configure# router bgp 300
R1/configure/bgp 300# neighbor 192.168.10.1 remote-as 200
R1/configure/bgp 300# network 1.1.1.0/27
R1/configure/bgp 300# network 1.1.2.0/24
```

Verifying BGP

Use the following commands to verify your BGP configuration:

- show running-config bgp
- show ip bgp summary
- show ip bgp neighbors

```
SI3# show running-config bgp
router bgp 30000
synchronization
network synchronization
neighbor 100.100.100.2 remote-as 20000
neighbor 3ffe::32 remote-as 20000
!
```

```

address-family ipv6
neighbor 3ffe::32 activate
exit address-family
SI3#
SI3# show ip bgp summary
BGP router identifier 100.100.100.3, local AS number 30000
BGP table version is 4
1 BGP AS-PATH entries
0 BGP community entries

Neighbor      V  AS      MsgRcvd MsgSent  TblVer  InQ  OutQ
Up/Down  State/PfxRcd
100.100.100.2  4 20000      58      60        4     0     0
00:49:45      3
3ffe::32      4 20000       8       7        1     0     0
00:00:52      0

Total number of neighbors 2
SI3#
SI3# show ip bgp neighbors
BGP neighbor is 100.100.100.2, remote AS 20000, local AS
30000, external link
  BGP version 4, remote router ID 192.102.1.1
  BGP state = Established, up for 00:49:50
  Last read 00:49:50, hold time is 180, keepalive interval
is 60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 58 messages, 0 notifications, 0 in queue
  Sent 60 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 1
  Minimum time between advertisement runs is 30 seconds

For address family: IPv4 Unicast
  BGP table version 4, neighbor version 4
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  3 accepted prefixes
  0 announced prefixes

Connections established 1; dropped 0
Local host: 100.100.100.3, Local port: 1487
Foreign host: 100.100.100.2, Foreign port: 179
Nexthop: 100.100.100.3
Nexthop global: ::

```

```

Nexthop local: ::
BGP connection: non shared network

BGP neighbor is 3ffe::32, remote AS 20000, local AS 30000,
external link
  BGP version 4, remote router ID 192.102.1.1
  BGP state = Established, up for 00:00:57
  Last read 00:00:57, hold time is 180, keepalive interval
is 60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
    Address family IPv6 Unicast: advertised and received
  Received 7 messages, 1 notifications, 0 in queue
  Sent 8 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds

For address family: IPv4 Unicast
  BGP table version 4, neighbor version 4
  Index 2, Offset 0, Mask 0x4
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  3 announced prefixes

For address family: IPv6 Unicast
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

Connections established 2; dropped 1
Local host: 3ffe::33, Local port: 1536
Foreign host: 3ffe::32, Foreign port: 179
Nexthop: 100.100.100.3
Nexthop global: 3ffe::33
Nexthop local: fe80::216:32ff:fe80:2e49
BGP connection: shared network
Last Reset: 00:01:02, due to BGP Notification received
Notification Error Message: (CeaseUnspecified Error Subcode)

SI3#

```



This page is intentionally left blank.



CHAPTER 9. BGP4+

The Border Gateway Protocol (BGP) is an exterior gateway protocol (EGP) that is used to exchange routing information among routers in different autonomous systems (ASs). BGP routing information includes the complete route to each destination. BGP uses the routing information to maintain a database of network reachability information, which it exchanges with other BGP systems. BGP uses the network reachability information to construct a graph of AS connectivity, thus allowing BGP to remove routing loops and enforce policy decisions at the AS level.

BGP4+ enable BGP to support Internet Protocol version 6 (IPv6). BGP4+ defines the attributes `MP_REACH_NLRI` and `MP_UNREACH_NLRI`, which are used to carry IPv6 reachability information. The first one (`MP_REACH_NLRI`) is used to carry the set of reachable destinations together with the next hop information to be used for forwarding to these destinations. The second one (`MP_UNREACH_NLRI`) is used to carry the set of unreachable destinations. Both of these attributes are optional and non-transitive. This way a BGP speaker that doesn't support the multiprotocol capabilities will just ignore the information carried in these attributes, and will not pass it to other BGP speakers.

Network layer reachability information (NLRI) update messages carry IPv6 address prefixes of feasible routes.

BGP allows for policy-based routing. You can use routing policies to choose among multiple paths to a destination and to control the redistribution of routing information. BGP uses the Transmission Control Protocol (TCP) as its transport protocol, using port 179 for establishing connections. Running over a reliable transport protocol eliminates the need for BGP to implement update fragmentation, retransmission, acknowledgment, and sequencing.

BGP supports classless interdomain routing (CIDR), which eliminates the concept of network classes. Instead of assuming which bits of an address represent the network by looking at the first octet, CIDR allows you to explicitly specify the number of bits in the network address, thus providing a means to decrease the size of the routing tables. BGP also supports aggregation of routes, including the aggregation of AS paths.



NOTE

The contents of this chapter is applied to SNOS version 2.0.0 or higher.

Minimum BGP Configuration

This Section shows the minimum configurations required for running BGP.

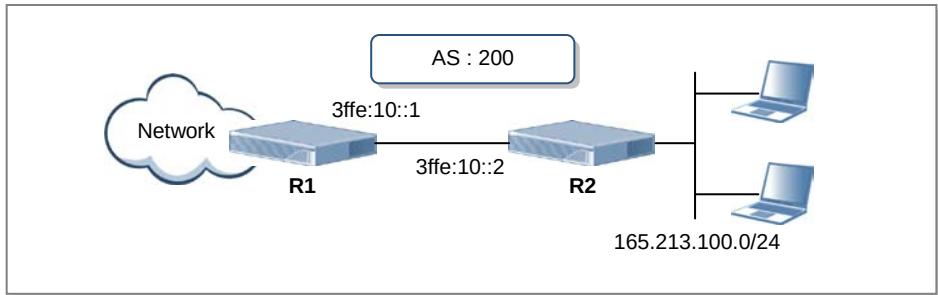
Configuring BGP in the same AS

Step-by-Step Configuration

Step	Command	Purpose
1	Router# configure terminal	Enters the terminal configuration mode.
2	Router/configure# router bgp [Autonomous Number]	Enters a BGP configuration mode.
3	Router/configure/router/bgp [AS No.]# neighbor [IP address] remote-as [Autonomous Number]	Defines a BGP neighbor with its IP address and autonomous number.
4	Router/configure/router/bgp [AS No.]# address-family ipv6	Enters Address family mode.
5	Router/configure/router/bgp [AS No.]/ address-family ipv6# neighbor [IP address] activate	Enables the Address Family for Neighbor.

Configuration Example

In the figure, R1 and R2 are two Ubigate iBG routers belonging to the same AS (autonomous system) with the ID of 200.



The following example shows the commands used to configure the BGP for R1 in the figure.

```

R1# configure terminal
R1/configuration# router bgp 200
R1/configuration/bgp 200# neighbor 3ffe:10::2 remote-as 200
R1/configuration/bgp 200# address-family ipv6
R1/configuration/bgp 200/address-family ipv6# neighbor
3ffe:10::2 activate

```

The following example shows the commands used to configure the BGP for R2 in the figure.

```

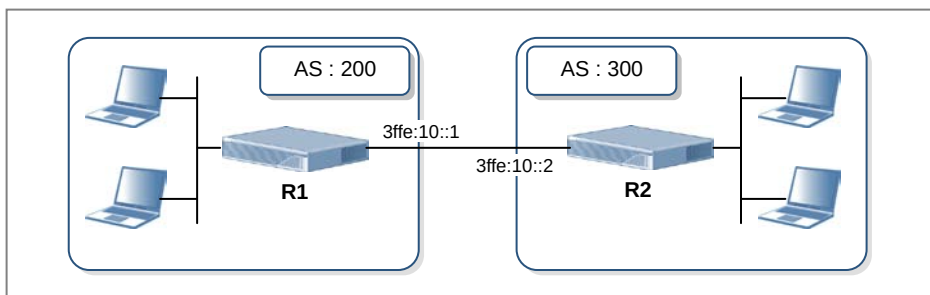
R2# configure terminal
R2/configuration# router bgp 200
R2/configuration/bgp 200# neighbor 3ffe:10::1 remote-as 200
R2/configuration/bgp 200# address-family ipv6
R2/configuration/bgp 200/address-family ipv6# neighbor
3ffe:10::1 activate

```

Configuring BGP in the different AS

Configuration Example

The following figure shows two Ubigate iBG routers in the different AS.



The following example shows the commands used to configure the BGP for R1 in the figure.

```
R1# configure terminal
R1/configuration# router bgp 200
R1/configuration/bgp 200# neighbor 3ffe:10::2 remote-as 300
R1/configuration/bgp 200# address-family ipv6
R1/configuration/bgp 200/address-family ipv6# neighbor
3ffe:10::2 activate
```

The following example shows the commands used to configure the BGP for R2 in the figure.

```
R2# configure terminal
R2/configuration# router bgp 300
R2/configuration/bgp 300# neighbor 3ffe:10::1 remote-as 200
R2/configuration/bgp 300# address-family ipv6
R2/configuration/bgp 300/address-family ipv6# neighbor
3ffe:10::1 activate
```

BGP Application using Route-Map

This section describes how to associate a route-map with BGP.

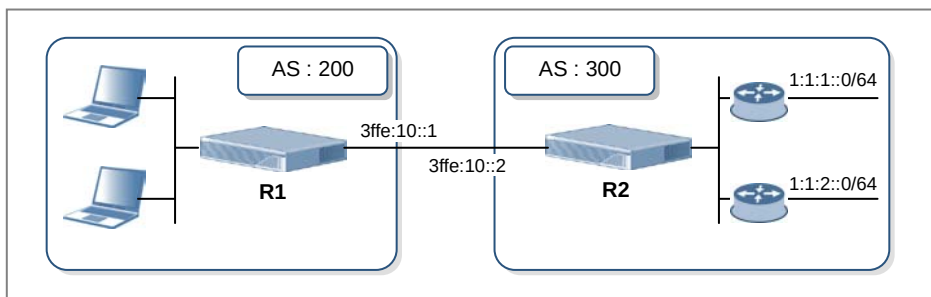
Configuring Route-Map and BGP in R1

Step-by-Step Configuration

Step	Command	Purpose
1	R1# configure terminal	Enters the terminal configuration mode.
2	R1/configure# ipv6 prefix-list [<i>prefix name</i>] { options }	Makes a prefix-list.
3	R1/configure# route-map [<i>prefix name</i>] permit 1	Enters the route-map mode to set the match operation.
4	R1/configure/route-map# match ipv6 address prefix-list [<i>prefix name</i>]	Sets the match criteria.
5	R1/configure/route-map# exit	Returns to the upper configuration level.
6	R1/configure# router bgp [<i>id</i>]	Enters a BGP configuration mode.
7	R1/configure/router/bgp [<i>id</i>]# neighbor [<i>IP address</i>] remote-as [<i>Autonomous Number</i>]	Defines a BGP neighbor with its IP address and autonomous number.
8	R1/configure/router/bgp [<i>id</i>]# neighbor [<i>IP address</i>] route-map [<i>prefix name</i>] in	Applies a route-map to routes for incoming advertisements.
9	Router/configure/router/bgp [AS No.]# address-family ipv6	Enters Address family mode.
10	Router/configure/router/bgp [AS No.]/address-family ipv6# neighbor [IP address] activate	Enables the Address Family for Neighbor.

Configuration Example

In the figure, R1 and R2 are the Ubigate iBG routers in the different autonomous systems.



R2 is connected to two different routers and their subnets are different

The following example shows the commands used to configure the BGP using Route-Map for R1.

```
R1# configure terminal
R1/configure# ipv6 prefix-list inpf seq 5 deny 1:1:1::0/64
ge 66 le 68
R1/configure# ipv6 prefix-list inpf seq 10 permit any
R1/configure# route-map inpf permit 1
R1/configure/route-map# match ipv6 address prefix-list inpf
R1/configure/route-map# exit
R1/configure# router bgp 200
R1/configure/bgp 200# neighbor 3ffe:10::2 remote-as 300
R1/configure/bgp 200# neighbor 3ffe:10::2 route-map inpf in
R1/configure/bgp 200# address-family ipv6
R1/configure/bgp 200/address-family ipv6# neighbor
3ffe:10::2 activate
```

The following example shows the commands used to configure the BGP for R2.

```
R2# configure terminal
R2/configure# router bgp 300
R2/configure/bgp 300# neighbor 3ffe:10::1 remote-as 200
R2/configure/bgp 300# address-family ipv6
R2/configure/bgp 300/address-family ipv6# neighbor 3ffe:10::1
activate
R2/configure/bgp 300/address-family ipv6# network 1:1:1::0/64
R2/configure/bgp 300/address-family ipv6# network 1:1:2::0/64
```

Verifying BGP4+

Use the following commands to verify your BGP configuration:

- show running-config bgp
- show ip bgp summary
- show ip bgp neighbors

```
SI3# show running-config bgp
router bgp 30000
synchronization
network synchronization
neighbor 100.100.100.2 remote-as 20000
neighbor 3ffe::32 remote-as 20000
!
address-family ipv6
neighbor 3ffe::32 activate
exit address-family
SI3#
SI3# show ip bgp summary
BGP router identifier 100.100.100.3, local AS number 30000
BGP table version is 4
1 BGP AS-PATH entries
0 BGP community entries
```

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ
Up/Down	State/PfxRcd						
100.100.100.2	4	20000	58	60	4	0	0 00:49:45
3ffe::32	4	20000	8	7	1	0	0 00:00:52

```
Total number of neighbors 2
SI3#
SI3# show ip bgp neighbors
BGP neighbor is 100.100.100.2, remote AS 20000, local AS
30000, external link
  BGP version 4, remote router ID 192.102.1.1
  BGP state = Established, up for 00:49:50
  Last read 00:49:50, hold time is 180, keepalive interval
is 60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 58 messages, 0 notifications, 0 in queue
  Sent 60 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 1
  Minimum time between advertisement runs is 30 seconds

For address family: IPv4 Unicast
  BGP table version 4, neighbor version 4
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  3 accepted prefixes
  0 announced prefixes
```

```

Connections established 1; dropped 0
Local host: 100.100.100.3, Local port: 1487
Foreign host: 100.100.100.2, Foreign port: 179
Nexthop: 100.100.100.3
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network

BGP neighbor is 3ffe::32, remote AS 20000, local AS 30000,
external link
  BGP version 4, remote router ID 192.102.1.1
  BGP state = Established, up for 00:00:57
  Last read 00:00:57, hold time is 180, keepalive interval
  is 60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
    Address family IPv6 Unicast: advertised and received
  Received 7 messages, 1 notifications, 0 in queue
  Sent 8 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds

For address family: IPv4 Unicast
  BGP table version 4, neighbor version 4
  Index 2, Offset 0, Mask 0x4
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  3 announced prefixes

For address family: IPv6 Unicast
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

Connections established 2; dropped 1
Local host: 3ffe::33, Local port: 1536
Foreign host: 3ffe::32, Foreign port: 179
Nexthop: 100.100.100.3
Nexthop global: 3ffe::33
Nexthop local: fe80::216:32ff:fe80:2e49
BGP connection: shared network
Last Reset: 00:01:02, due to BGP Notification received
Notification Error Message: (CeaseUnspecified Error Subcode)

SI3#

```



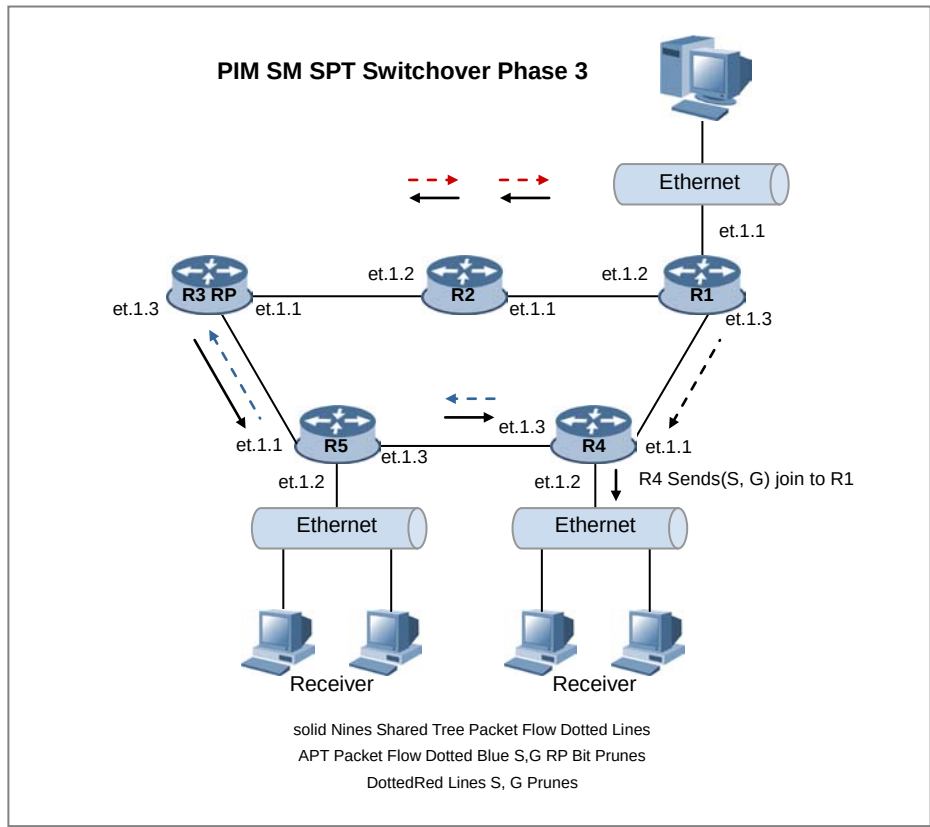

CHAPTER 10. Multicast Protocols

This chapter describes the multicast routing protocols and how to configure the multicast routing protocols. Refer to the RFCs and the standards documents for more detailed protocol specifications.

Protocol Independent Multicast (PIM)

Protocol Independent Multicast (PIM) protocols route multicast packets to multicast groups. PIM is protocol independent because it can leverage whichever unicast routing protocol is used to populate unicast routing table. There are two modes of PIM protocol - Dense mode (DM) and Sparse mode (SM). Ubigate iBG router supports SM but not DM. PIM-DM floods multicast traffic throughout the network initially and then generates prune messages as required. PIM-SM attempts to send multicast data only to networks which have active receivers. This is achieved by having a common Rendezvous Point (RP) known to the senders and receivers and by forming shared trees from the RP to the receivers. The Protocol Independent Multicasting-Sparse Mode (PIM-SM) is a multicast routing protocol designed to operate efficiently across Wide Area Networks (WANs) with sparsely distributed groups. It helps network nodes that are geographically dispersed to conserve bandwidth, and reduces traffic by simultaneously delivering a single stream of information to multiple locations. PIM-SM uses the IP multicast model of receiver-initiated membership, supporting both shared and shortest-path trees, and uses soft-state mechanisms to adapt to changing network conditions. It relies on a topology-gathering protocol to populate a multicast routing table with routes.

For SNOS version 2.0.0 or higher, Ubigate supports Source Specific Mode (SSM), wherein the receivers can apply source filtering using IGMPv3 messages, to receive multicast data only/except from a particular source(s). RP is not required for SSM operations and the non-shared multicast trees will be rooted directly from sources.



Terminology

Following is a brief description of terms and concepts used to describe the PIM-SM protocol:

Rendezvous Point (RP)

A Rendezvous Point (RP) router is configured as the root of the non-source-specific distribution tree for a multicast group. Join messages from receivers for a group are sent towards the RP. Data from senders is sent to the RP so that receivers can discover who the senders are, and receive traffic destined for the group.

Multicast Routing Information Base (MRIB)

The MRIB is a multicast topology table derived from the unicast routing table. In PIM-SM, the MRIB is used to decide where to send Join/Prune messages. It also provides routing metrics for destination addresses. These metrics are used when sending and processing Assert messages.

Reverse Path Forwarding

Reverse Path Forwarding (RPF) is a concept of an optimized form of flooding, where the router accepts a packet from SourceA through Interface IF1 only if IF1 is the interface the router would use in order to reach SourceA.

It determines whether the interface is correct by consulting its unicast routing tables. The packet that arrives through interface IF1 is forwarded because the routing table lists this interface as the shortest path to the network.

The router's unicast routing table determines the shortest path for the multicast packets. Because a router accepts a packet from only one neighbor, it floods the packet only once, meaning that (assuming point-to-point links) each packet is transmitted over each link once in each direction.

Tree Information Base (TIB)

The TIB is the collection of state at a PIM router storing the state of all multicast distribution trees at that router. It is created by receiving Join/Prune messages, Assert messages, and IGMP information from local hosts.

Upstream

Towards the root of the tree. The root of the tree might be either the Source or the RP.

Downstream

Away from the root of the tree. The root of tree might be either the Source or the RP.

Source-Based Trees

In the Source-Based Trees concept, the forwarding paths are based on the shortest unicast path to the source. If the unicast routing metric is hop counts, the branches of the multicast Source-Based Trees are minimum hop. If the metric is delay, the branches are minimum delay.

For every multicast source, there is a corresponding multicast tree that directly connects the source to all receivers. All traffic to the members of an associated group passes along the tree made for their source. Source-Based Trees have two entries with a list of outgoing interfaces--the source address and the multicast group.

Shared Trees

Shared trees or RP trees (RPT) rely on a central router called the Rendezvous Point (RP) that receives all traffic from the sources, and forwards that traffic to the receivers. All hosts might not be receivers. There is a single tree for each multicast group, regardless of the number of sources. Only the routers on the tree know about the group, and information is sent only to interested receivers. With an RP, receivers have a place to join, even if no source exists.

The shared tree is unidirectional, and information flows only from the RP to the receivers. If a host other than the RP has to send data on the tree, the data must first be tunneled to the RP, and then multicast to the members.

This means that even if a receiver is also a source, it can only use the tree to receive packets from the RP, and not to send packets to the RP (unless the source is located between the RP and the receivers).

Bootstrap Router (BSR)

When a new multicast sender starts sending data packets, or a new receiver starts sending the Join message towards the RP for that multicast group, it needs to know the next-hop router towards the RP. The BSR provides group-to-RP mapping information to all the PIM routers in a domain, allowing them to map to the correct RP address.

IP Multicast Routing Table

Note: Multicast Routing Table displays of an RP router are different from other routers.

The `show ip mroute` command displays the IP multicast routing table. In this table: RPF nbr displays the unicast next-hop to reach RP. RPF idx displays the incoming interface for this (*, G) state. RP displays the IP address for the RP router.

The leading dots Stand for VIF index

```
Router_E# show ip pim sparse-mode mroute

IP Multicast Routing Table
(*, *, RP) Entries: 0
(*, G) Entries: 1
(S, G) Entries: 0
```

```
(S,G,rpt) Entries: 0
(*, 224.0.1.3)
RP: 10.10.1.5
RPF nbr: 172.16.1.2

RPF idx: ethernet 2/1
Upstream State: JOINED

Local .....
Joined j.....
Asserted .....
Outgoing o.....
```

At Router_E, Ethernet 2/1 is the incoming interface of the (*, G) entry, and Ethernet 1/1 is on the outgoing interface list of the (*, G) entry. This means that there is a group member through Ethernet 1/1, and RP is reachable through Ethernet 2/1.

The 0 position on this 32-bit index is for Ethernet 1/1 (as illustrated in the interface display above). The j on the 0 index indicates that the Join has come from Ethernet 1/1.

Since Router_C is the RP, and the root of this multicast tree, the show ip pim sparse-mode mroute command on Router_C shows RPF nbr as 0.0.0.0 and RPF idx as none.

```
Router_C# show ip pim sparse-mode mroute

IP Multicast Routing Table

(*,*,RP) Entries: 0
(*,G) Entries: 1
(S,G) Entries: 0
(S,G,rpt) Entries: 0
(*, 224.0.1.3)
RP: 10.10.1.5
RPF nbr: 0.0.0.0
RPF idx: None
Upstream State: JOINED

Local .....
Joined j.....
Asserted .....
Outgoing o.....
```

The output for the show ip mroute command is:

```
Router# show ip mroute

IP Multicast Routing TableFlags: I - Immediate Stat,
T -TimedStat, F -Forwarder installedTimers: Uptime/Stat
ExpiryInterface State: Interface (TTL)

(10.10.1.52, 224.0.1.3), uptime 00:00:31, stat expires
00:02:59

Owner PIM-SM, Flags: TF Incoming interface: wm0 Outgoing
interface list: wm1 (1)

Router# show ip mroute 10.10.1.52 224.0.1.3

IP Multicast Routing TableFlags: I - Immediate Stat, T -
TimedStat, F -Forwarder installedTimers: Uptime/Stat
ExpiryInterface State: Interface (TTL) (10.10.1.52,
224.0.1.3), uptime 00:03:24, stat expires 00:01:28

Owner PIM-SM, Flags: TF Incoming interface: wm0 Outgoing
interface list:wm1 (1)
```

The following example shows how to display the multicast routing table for a source and destination address:

```
Router# show ip mroute 10.10.3.34 224.1.4.3
```

The following is a sample output for this command showing the IP multicast routing table in an abbreviated form:

```
Router# show ip mroute summary
IP Multicast Routing TableFlags: I - Immediate Stat,
T - Timed Stat, F - Forwarder installedTimers: Uptime/Stat
ExpiryInterface State: Interface (TTL)
(10.10.1.52, 224.0.1.3), 00:01:32/00:03:20, PIM-SM, Flags: TF
```

PIM Group-to-RP Mappings

Use the `show ip pim sparse-mode rp mapping` command to display the group-to-RP mapping details. The output displays information about RP candidates. There are two RP candidates for the group range 224.0.0.0/4. RP Candidate 10.10.1.5 has a default priority of 192, whereas, RP Candidate 172.16.1.2 has been configured to have a priority of 2. Since RP candidate 172.16.1.2 has a higher priority, it is selected as RP for the multicast group 224.0.0.0/4.

```
Router# show ip pim sparse-mode rp mapping

This system is the Bootstrap Router (v2)
Group(s): 224.0.0.0/4

RP: 10.10.1.5

Info source: 172.16.1.2, via bootstrap, priority 192 Uptime:
00:00:13, expires: 00:02:29 RP: 172.16.1.2

Info source: 172.16.1.2, via bootstrap, priority 2   Uptime:
00:34:42, expires: 00:01:49
```

RP Details

To display information about the RP router for a particular group, use the following command. This output displays that 172.16.1.2 has been chosen as the RP for the multicast group 224.0.1.3.

```
Router_D# show ip pim sparse-mode rp-hash 224.0.1.3
Group(s): 224.0.0.0/4
RP: 172.16.1.2

Info source: 172.16.1.2, via bootstrap
```

After RP information reaches all PIM routers in the domain, various state machines maintain all routing states as the result of Join/Prune from group membership.

SSM

Source Specific Mode (SSM) is a subset of PIM-SM. Using SSM, a receiver besides joining a multicast group, can opt for receiving multicast data from a particular set of source (s). The receiver can also opt for receiving multicast data from all the sources for a multicast group except from a particular set of source (s). IGMPv3 membership reports are used by the receivers to specify the list of sources that they are interested in receiving the data from, along with the multicast group. The SSM range designated by IANA is 232.0.0.0/8. However the user has an option to configure the SSM range.



SSM is applied to SNOS version 2.0.0 or higher.

PIM Configuration Examples

This section shows examples of how the PIM commands are used.

The following example enters the BSR mode and sets Ethernet 1/0 as the BSR interface.

```
Router/configure# ip multicast-routing
Router/configure# ip pim bsr-candidate ethernet1/0
```

To set the hash mask length for Rendezvous Point selection to 24 and set the priority for candidate bootstrap router to 45, enter:

```
Router/configure# ip pim bsr-candidate ethernet1/0
```

To enter the candidate Rendezvous Point interface, enter:

```
Router/configure#ip pim rp-candidate ethernet1/0
```

To set the group IP address for CRP advertisements to 224.1.1.0 using the group-list ACL, enter:

```
Router/configure#ip pim rp-candidate ethernet1/0 group-list ACL
```


To set the flag at the DR to switch to the SPT on receiving the first packet (default on), enter:

```
Router/configure#ip pim spt-threshold
```

The following example configures the Register Suppression Timeout to be 70 seconds.

```
Router/configure#ip pim register-suppression 70
```

To set the RP static IP address to 10.10.1.1, enter:

```
Router/configure#ip pim rp-address 10.10.1.1
```

To set the flag for the RP to switch to the SPT for (S, G) upon receipt of the first Register message (default: on). To turn on this feature, enter:

```
Router/configure#ip pim spt-threshold
```

To specify that the message checksum will be calculated over the entire encapsulated packet, rather than just over the Register message header, enter:

```
Router/configure#ip pim cisco-register-checksum
```

To enable SSM with the default SSM range (232/8), enter:

```
Router/configure#ip pim ssm default
```



NOTE

SSM is applied to SNOS version 2.0.0 or higher.

To enable SSM with a user configured SSM range, say 225.0.0.0/16 defined under the access list name SSM_RANGE, enter:

```
Router/configure#ip pim ssm range SSM_RANGE
```

**NOTE**

SSM is applied to SNOS version 2.0.0 or higher.

To set the hello hold time to 60 seconds, enter:

```
Router/configure/interface/ethernet (1/0)# ip pim hello-  
holdtime 60
```

To set the hello interval time to 145 seconds, enter:

```
Router/configure/interface/ethernet (1/0)# ip pim hello-  
interval 145
```

To set the jp-timer to 30 seconds, enter:

```
Router/configure#ip pim jp-timer 30
```

To display information for all interfaces, enter:

```
Router# show ip pim sparse-mode interface or  
Router# show ip pim sparse-mode interface detail or  
Router# show ip pim sparse-mode bsr-router
```

To display information on PIM neighbors, enter:

```
Router# show ip pim sparse-mode neighbor detailNeighbor  
Interface  
Uptime Expires Hello Priority
```

To examine PIM BSR statistics, enter:

```
Router# show ip pim sparse-mode bsr-router
Candidate BSR Information
Candidate BSR Status: Disabled
Candidate BSR Interface: NOT CONFIGURED
Candidate BSR Priority: 45
Candidate BSR Period: 30
Candidate BSR Hold Time: 2048
Candidate BSR Admin Scope: Disabled
No BSR's
```

Verifying PIM

Use the following commands to verify your PIM configuration:

- show ip pim sparse-mode interface
- show ip pim sparse-mode neighbor
- show ip pim sparse-mode bsr-router
- show ip pim sparse-mode rp mapping

```
SI3/configure# show ip pim sparse-mode interface
Address          Interface  VIFindex Ver/   Nbr    DR  DR
                  Mode      Count  Prior
8.1.1.2          ethernet0/4  0    v2/S  0  1  8.1.1.2
100.100.100.3    ethernet3/3  2    v2/S  1  1  100.100.100.3
SI3/configure#
SI3/configure#
SI3/configure# show ip pim sparse-mode neighbor
Neighbor          Interface      Uptime/Expires   Ver  DR
Address                               Priority/Mode
100.100.100.2    ethernet3/3    00:11:19/00:01:27 v2   1 /
SI3/configure#
SI3/configure#
SI3/configure# show ip pim sparse-mode bsr-router
PIMv2 Bootstrap information
This system is the Bootstrap Router (BSR)
BSR address: 100.100.100.3
Uptime: 00:08:33, BSR Priority: 0, Hash mask length: 30
Next bootstrap message in 00:00:37
Role: Candidate BSR
State: Elected BSR
```

```
Candidate RP: 100.100.100.3(ethernet3/3)
  Advertisement interval 60 seconds
  Next Cand_RP_advertisement in 00:00:36
SI3/configure#
SI3/configure#
SI3/configure# show ip pim sparse-mode rp mapping
PIM Group-to-RP Mappings
This system is the Bootstrap Router (v2)
Group(s): 224.0.0.0/4
  RP: 100.100.100.3
    Info source: 100.100.100.3, via bootstrap, priority 192
    Uptime: 00:08:32, expires: 00:01:58
SI3/configure#
```

Other PIM Commands Supported

Other useful PIM commands supported in this release are:

- Interface mode commands:
 - ip pim accept-register list
 - ip pim exclude-genid
 - ip pim dr-priority
 - ip pim neighbor-filter
 - ip pim sparse-mode
- Config mode commands
 - ip pim accept-register list
 - ip pim register-source
 - ip pim register-rate-limit
 - ip pim ignore-rp-set-priority
 - ip pim rp-register-kat
 - ip pim register-suppression
 - ip pim cisco-register-checksum group-list
 - ip pim ssm default (for SNOS version 2.0.0 or higher)
- clear ip mroute
- clear ip pim sparse-mode bsr rp-set all
- debug pim all
- debug pim sparse-mode events
- debug pim sparse-mode mib
- debug pim sparse-mode mfc
- debug pim sparse-mode packet

- debug pim sparse-mode timer assert
- debug pim sparse-mode timer bsr
- debug pim sparse-mode timer hello
- debug pim sparse-mode timer joinprune
- debug pim sparse-mode timer register

Distance Vector Multicast Routing Protocol (DVMRP)

Distance Vector Multicast Routing Protocol (DVMRP) is a multicast routing protocol that provides an efficient mechanism for connectionless datagram delivery to a group of hosts across an internetwork. It is a distributed protocol that dynamically generates IP multicast delivery trees using a technique called Reverse Path Multicasting.

Terminology

Following is a brief description of terms and concepts used to describe the DVMRP protocol.

DRIB

DVMRP maintains DVMRP Routing Information Base (DRIB).

The DRIB contains the table of routes for multicast sources learned through DVMRP route exchanges. Both the upstream and the downstream parts of a route-state reside physically in a combined, single DRIB node. A DRIB node is called a DVMRP Routing Table (DRT) entry.

The DRT entry contains a vector of downstream interfaces; each vector slot position represents a virtual interface (VIF). It is used to store all required information for the state to ultimately decide the set of forwarding interfaces for corresponding multicasting data packets.

DVMRP requires a per-source network Designated Forwarder (DF) on each downstream interface, i.e., DF (S, I). DF election is based on the metric toward the source network.

If DF (S,I) changes for an interface, Ubigate iBG router updates the outgoing VIF list (Olist) for all prune (S, G) states and their corresponding forwarding caches.

VIF Table

The VIF table is a tree of virtualized physical and tunnel interfaces indexed by a virtual interface number.

Neighbor Table

The Neighbor table is a list of detected DVMRP neighbors on an interface. Neighbors announce themselves using the Probe message.

Route Report Arrays of Lists

Because route reporting is done by grouping together all routes that belong to the same mask, a Route Report Array of Lists (AOL) is used to expedite general route reporting.

Configuration Example

The main requirement is to enable DVMRP on the desired interfaces. This section provides a DVMRP configuration example for a relevant scenario. In this example, the Source_1 address is 10.10.1.52, and the group address is set to 224.0.1.3. The following figure displays the network topology used in this example: 10.101.52

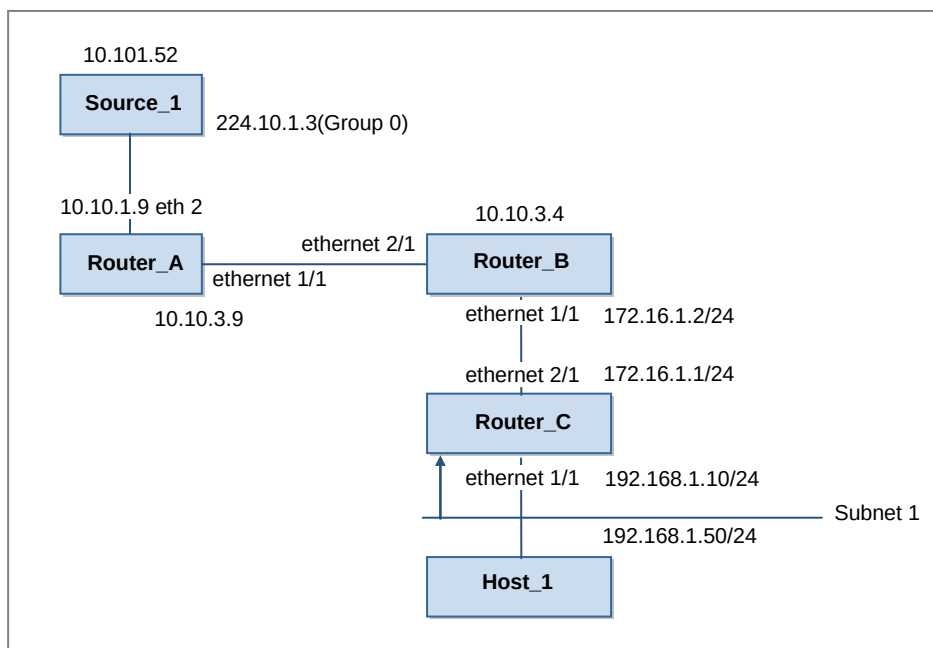


Figure 7.1 DVMRP Network

In this example, all routers are running DVMRP.

1. Host_1 sends an IGMP membership report to Subnet 1.
2. After Router_C receives this report, it associates its receiving interface, Ethernet 1/1, with the group reported in the IGMP message, for example, Group 1.
3. Source_1 then sends a data packet for Group 1.
4. Every router creates an (S,G) entry in the multicast routing table.
5. When the data packet reaches Router_C, it forwards via the interface, Ethernet 1/1, because there is a local member on this interface for this group. Router_C has a downstream receiver, hence, it does not send a prune message to its upstream neighbor router, Router_B.

Enabling DVMRP

Use the following command to enable DVMRP on an interface. Use this command for each interface: `ip dvmrp enable`

For example:

```
Router# configure terminal Router/configure# interface
ethernet 1/1
Router/configure/interface/ethernet (1/1)# ip dvmrp enable
Router/configure/interface/ethernet (1/1)# exit
Router/configure# interface ethernet 2/1
Router/configure/interface/ethernet (2/1)# ip dvmrp enable
Router/configure/interface/ethernet (2/1)# exit
```

Verifying Configuration

Use the following commands to verify interface, neighbor, route, prune, and DVMRP global state information. Note: For details on the commands used in the following example, refer to the Ubigate iBG Command Reference.

Interface Information

The `show ip dvmrp interface` command displays the interface information for Router_C. For example:

```
Router_C# show ip dvmrp interface
Address      Interface    Vif   Ver.   Nbr   Type   Remote
              Index      Cnt
192.168.1.10 ethernet1/1   1    v3.ff   0    BCAST  N/A
172.16.1.1   ethernet2/1   0    v3.ff   0    BCAST  N/A
```


Neighbor Information

The show ip dvmrp neighbor command displays the neighbor information for Router_C. For example:

```
Router_C# show ip dvmrp neighbor
Codes: d - day(s), h - hour(s), m - minute(s) w - week(s)
Cap Flg - Capability Flag
```

Neighbor Address	Interface	Uptime/Expires	Maj Ver	Min Ver	Cap Flg
192.168.1.10	ethernet1/1	00:00:04/00:00:31	3	255	2e
172.16.1.2	ethernet2/1	00:00:07/00:00:28	3	255	2e

Route Information

The show ip dvmrp route command displays the route information for Router_C. For example:

```
Router_C# show ip dvmrp route
Flags: N = New, D = DirectlyConnected, H = Holddown
```

Network	Flags	Nexthop Xface	Nexthop Neighbor	Metric	Uptime	Exptn
192.168.1.0/24	.D.	ethernet1/1	Directly Connected	1	00:04:05	
172.16.1.0/24	.D.	ethernet2/1	Directly Connected	1	00:04:11	

DVMRP Prune Information

The show ip dvmrp prune command displays DVMRP prune information for Router_C. For example:

```
Router_C# show ip dvmrp prune
Codes: P -Pruned, H - Host, D - Holddown, N - Negative MFC,
I - Init
FCR - forwarding cache entries
```

Source Prune/Graft Address	Mask Len	Group Address	State Cnt	FCR	Exptime ReXmit-Time
10.101.52.1	32	224.10.1.3	PH.N.	1	01:13:42 00:09:50

DVMRP Global State

The `show ip dvmrp` command displays the global DVMRP state for Router_C. For example:

```
Router_C# show ip dvmrp
DVMRP Daemon Start Time: THU    DVMRP Daemon Uptime: 00:16:26
DVMRP Number of Route Entries: 2
DVMRP Number of Reachable Route Entries: 2
DVMRP Number of Prune Entries: 1
DVMRP Route Report Timer: Running
DVMRP Route Report Timer Last Update: 00:00:26
DVMRP Route Report Timer Next Update: 00:00:34
DVMRP Flash Route Update Timer: Not Running
```

Internet Group Management Protocol (IGMP)

Internet Group Management Protocol (IGMP) is enabled on hosts and routers that want to receive multicast traffic. IGMP informs locally-attached routers of their multicast group memberships. Hosts inform routers of the groups of which they are members by multicasting IGMP Group Membership Reports. When multicast routers listen for these reports, they can exchange group membership information with other multicast routers. This reporting system allows distribution trees to be formed to deliver multicast datagrams. The original version of IGMP was defined in RFC 1112, Host Extensions for IP Multicasting. Extensions to IGMP, known as IGMP version 2.

IGMPv2 improves performance and supports the following message types:

1. **IGMP Query:** IGMP Query is sent by the router to know which groups have members on the attached network.
2. **IGMP Reports:** IGMP reports are sent as a response to the query by hosts to announce their group membership. Reports can be sent ‘unsolicited’ when the hosts come up.
3. **IGMP Leaves:** IGMP Leaves are sent by the host when it relinquishes membership of a group.

To enable the receivers to apply source filtering on the multicast data reception, an extension of IGMPv2 was designed which is called IGMP version 3, and is defined in the RFC .3376, Internet Group Management Protocol, Version 3.

Along with the existing IGMPv1 and v2 membership reports, IGMPv3 supports the following message types: (for SNOS version 2.0.0 or higher)

1. **IGMPv3 Query:** IGMPv3 Query is a superset of the IGMPv2 query, which includes number of source and list of source addresses fields. The same query message can be sent in 3 different forms - general query, group specific query and group-source specific query.
2. **IGMPv3 Reports:** IGMPv3 reports maintain the state of the group membership records on a router in two modes - Include and Exclude. There are six types of IGMPv3 membership reports generated by the receivers based on the current state/mode:
 - Mode_Is_Include
 - Mode_Is_Exclude
 - Change_To_Include_Mode
 - Change_To_Exclude_Mode
 - Allow_New_Sources
 - Block_Old_Sources

IGMP Commands

The IGMP commands supported in Ubigate iBG router are:

- ip igmp access-group
- ip igmp immediate-leave
- ip igmp last-member-query-count
- ip igmp last-member-query-interval
- ip igmp querier-timeout
- ip igmp query-interval
- ip igmp query-max-response-time
- ip igmp version
- debug igmp tib
- clear ip igmp groups
- clear ip igmp interface

Verifying the Configuration

To verify your IGMP configuration use the following commands:

- show ip igmp groups
- show ip igmp interface

IGMP Configuration Examples

Use the examples shown in this section to use IGMP in multicast configurations.

Example 1

The following example configures default IGMP version to 2 to run on interface Ethernet (0/1).

```
Router/configure/interface/ethernet (0/1)# ip igmp version 2
```

Example 2

The following example configures Ethernet (0/1) with the Query Interval to be 100 seconds.

```
Router/configure/interface/ethernet (0/1)# ip igmp query-  
interval 100
```

Example 3

The following example configures Ethernet (0/1) with the Query time-out to be 300 seconds.

```
Router/configure/interface/ethernet (0/1)# ip igmp querier-  
timeout 300
```

Example 4

The following example configures Ethernet (0/1) with the query-max-response-time to be 10 seconds.

```
Router/configure/interface/ethernet (0/1)# ip igmp query-  
max-response-time 10
```

Example 5

The following example configures Ethernet (0/1) with the last-memberquery-count to be 3.

```
Router/configure/interface/ethernet (0/1)# ip igmp last-  
memberquery-count 3
```

Example 6

The following example configures Ethernet (0/1) with the last-member-query-interval to be 2000 seconds.

```
Router/configure/interface/ethernet (0/1)# ip igmp last-  
member-query-interval 2000
```

Example 7

The following example configures an Access Group on the Router for multicast group 224.7.7.7 with mask 0.0.0.0 with permit option

```
Router/configure# access-list routing 1 permit 224.7.7.7  
0.0.0.0  
Router/configure# interface ethernet 0/1  
Router/configure/interface/ethernet (0/1)# ip igmp access-  
group 1
```

Example 8

The following example configures Immediate leave on Ethernet (0/1) for multicast group 224.7.7.7.

```
Router/configure# access-list routing 1 permit 224.7.7.7
0.0.0.0
Router/configure# interface ethernet 0/1
Router/configure/interface/ethernet (0/1)# ip igmp
immediate-leave group-list 1
```

Example 9 (for SNOS version 2.0.0 or higher)

The following example configures IGMP version to 3 to run on interface Ethernet (0/1).

```
Router/configure/interface/ethernet (0/1)# ip igmp version 3
```

Verifying and Troubleshooting Commands

```
debug# igmp tib
show ip igmp groups
show ip igmp groups detail
show ip igmp interface
```

```
Router# show ip igmp groups
IGMP Connected Group Membership
Group Address  Interface      Uptime    Expires    Last
Reporter
227.1.1.1      ethernet3/3    01:42:26  00:04:07  33.1.1.10
227.1.1.2      ethernet3/3    01:42:26  00:04:07  33.1.1.10
Router#
```

```
Router# show ip igmp groups detail

Interface: ethernet3/3
Group: 227.1.1.1
Uptime: 00:04:54
Group mode: Exclude (Expires: 00:03:59)
Last reporter: 33.1.1.10
```

```
Group source list: (R - Remote, M - SSM Mapping)
```

Source Address	Uptime	v3 Exp	Fwd	Flags
38.1.1.12	00:02:00	stopped	No	R

```
Interface: ethernet3/3
```

```
Group: 227.1.1.2
```

```
Uptime: 00:04:54
```

```
Group mode: Exclude (Expires: 00:03:59)
```

```
Last reporter: 33.1.1.10
```

```
Group source list: (R - Remote, M - SSM Mapping)
```

Source Address	Uptime	v3 Exp	Fwd	Flags
38.1.1.12	00:01:35	stopped	No	R

```
Router#
```

```
Router# show ip igmp interface
```

```
Interface ethernet0/2 (Index 3)
```

```
IGMP Enabled, Active, Querier, Default version 2
```

```
Internet address is 192.100.1.1
```

```
IGMP query interval is 125 seconds
```

```
IGMP querier timeout is 255 seconds
```

```
IGMP max query response time is 10 seconds
```

```
Last member query response interval is 1000 milliseconds
```

```
Group Membership interval is 260 seconds
```

```
Number of groups IGMP joined on this interface: 0
```

```
Number of received IGMP V1-reports: 0
```

```
Number of received IGMP V2-reports: 0
```

```
Number of received IGMP V2-leaves: 0
```

```
Multicast routing is enabled on interface
```

```
Interface ethernet3/3 (Index 9)
```

```
IGMP Enabled, Active, Querier, Configured for version 3
```

```
Internet address is 33.1.1.1
```

```
IGMP query interval is 125 seconds
```

```
IGMP querier timeout is 255 seconds
```

```
IGMP max query response time is 10 seconds
```

```
Last member query response interval is 1000 milliseconds
```

```
Group Membership interval is 260 seconds
```

```
Number of groups IGMP joined on this interface: 2
```

```
Number of received IGMP V1-reports: 0
```

```
Number of received IGMP V2-reports: 0
```

```
Multicast routing is enabled on interface
```

```
Interface ethernet3/5 (Index 11)
  IGMP Inactive, Default version 2
  IGMP query interval is 125 seconds
  IGMP querier timeout is 255 seconds
  IGMP max query response time is 10 seconds
  Last member query response interval is 1000 milliseconds
  Group Membership interval is 260 seconds
  Number of groups IGMP joined on this interface: 0
  Number of received IGMP V1-reports: 0
  Number of received IGMP V2-reports: 0
  Number of received IGMP V2-leaves: 0
  Multicast routing is disabled on interface
Router#
```




CHAPTER 11. VRRP

In statically routed networks, when a router fails, all the network devices connected to this router are unable to have traffic routed. Typically this means these devices cannot reach the Internet or other networks.

IPv4's Virtual Router Redundancy Protocol (VRRP) eliminates this single point of failure by dynamically assigning virtual routers that can provide network connectivity in the event the primary router fails. One virtual router is designated as the Master which is assigned the IP addresses of connected devices. The Master router can manage multiple primary and secondary IP addresses.

Alternate virtual routers (up to 254) are designated as backup virtual routers in the event the Master fails. Each backup is configured with a priority setting that determines the order in which backup routers take over in the event the Master fails. When the Master router fails, the backup router with the smallest priority number will preempt all other backup routers in assuming the duties of the Master router. If you disable the preempt feature (using the `no vrrp preempt` command), the backup virtual router that is configured as the Master virtual router will remain such until the original Master virtual router recovers. The mechanism by which virtual routers in the same network communicate status and priority is through VRRP advertisements from the Master virtual router. VRRP uses the assigned multicast address 224.0.0.18. By default, these advertisements are sent every second, but you can configure the interval.

In addition to maintaining network connectivity when a router fails, VRRP allows network administrators to share routing duties with multiple routers thereby reducing the impact of heavy traffic loads.

Configuring VRRP

A simple VRRP configuration example is shown in the following figure. The Ubigate iBG router labeled Ubigate iBG1 at 10.1.1.1 is configured as the Master virtual router and the Ubigate iBG router labeled Ubigate iBG2 at 10.1.1.2 is configured as the backup virtual router. In the event Ubigate iBG1 fails, Ubigate iBG2 automatically takes over routing traffic between the subnets labeled Host A, B, and C, and the Gateway Router providing Internet connectivity.

To configure VRRP in this environment, you need to configure Ubigate iBG1 as the Master virtual router, and Ubigate iBG2 as the backup virtual router.

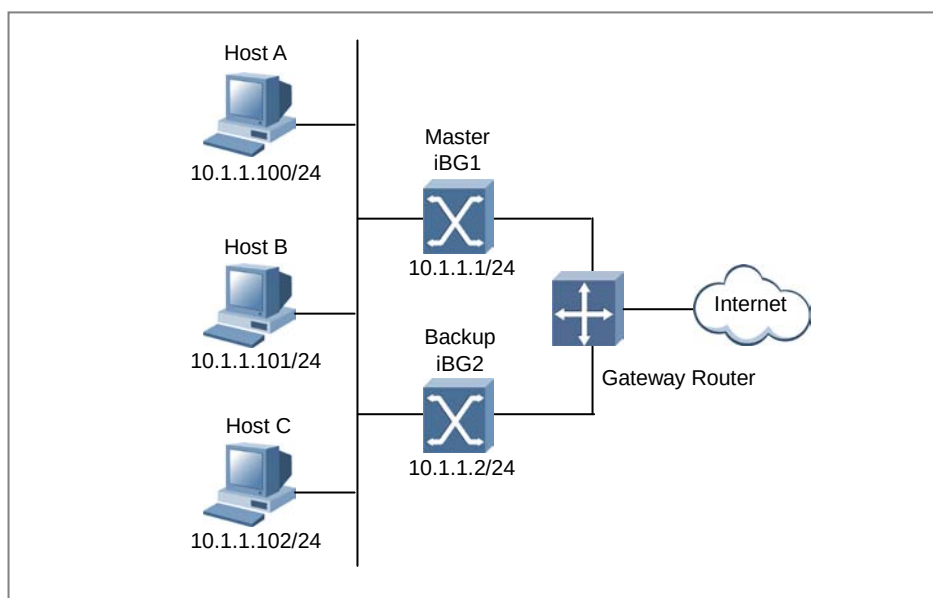


Figure 11.1 Configuring a VRRP Network

Configuring Master Router

```
Router# configure terminal
Router/configure# interface ethernet 0/1
Router/configure/interface/ethernet(0/1)# vrrp 10
Router/configure/interface/ethernet(0/1)/vrrp 10# ipaddr
10.1.1.10
Router/configure/interface/ethernet(0/1)/vrrp 10# priority 130
Router/configure/interface/ethernet(0/1)/vrrp 10# preempt
Router/configure/interface/ethernet(0/1)/vrrp 10#
advertisement_interval 2
Router/configure/interface/ethernet(0/1)/vrrp 10# enable
```

Configuring Backup Router

```
Router# configure terminal
Router/configure# interface ethernet 0/1
Router/configure/interface/ethernet(0/1)# vrrp 10
Router/configure/interface/ethernet(0/1)/vrrp 10# ipaddr
10.1.1.10
Router/configure/interface/ethernet(0/1)/vrrp 10# priority
120
Router/configure/interface/ethernet(0/1)/vrrp 10# preempt
Router/configure/interface/ethernet(0/1)/vrrp 10#
advertisement_interval 2
Router/configure/interface/ethernet(0/1)/vrrp 10# enable
```

Verifying and Troubleshooting

Ubigate iBG router provides commands to verify VRRP status and configuration.

To display detailed status of all VRRP groups on the router.

```
Router# show vrrp detailed
VRRP Group Number: 10
  Description:
    State: MASTER Priority: 130 Preempt: on Advertisement: 2
secs
  Authentication Type: No Authentication
  Virtual IP Addresses:
    IP Address 1: 10.1.1.10
  Virtual MAC Address: 00:00:5e:00:01:0a
  VRRP Router Up Time: 0 Days. : 0 Hours. : 1 mins. : 34 secs.
  Group Master IP Address: 10.1.1.1
  VRRP Configured Interface: ethernet0/1
```

```
Statistics:
  Became Master: 1  Advertisements Received: 0
  Priority zero packets - Received : 0  Sent: 0
  Checksum errors: 0  Version Errors: 0  VRID errors: 0
  Advertisement Interval errors: 0  IP TTL Errors: 0  Packet
Type Errors:
  Auth Failures: 0  Invalid Auth Types: 0  Mismatched Auth
Types: 0
  Address List mismatches: 0  Packet length Errors: 0
```

To display a brief status of all VRRP groups on the router.

```
Router# show vrrp summary
VRRP Group Number: 10
  Description:
    State: MASTER Priority: 130 Preempt: on Advertisement: 2 secs
    Authentication Type: No Authentication
    Virtual IP Addresses:
      IP Address 1: 10.1.1.10
    Virtual MAC Address: 00:00:5e:00:01:0a
    VRRP Router Up Time: 0 Days. : 0 Hours. : 2 mins. : 38 secs.
    Group Master IP Address: 10.1.1.1
    VRRP Configured Interface: ethernet0/1
```



CHAPTER 12. QoS

Quality of Service

The iBG series support software-based QoS for CPU ethernet ports and WAN interfaces by the operating system. For optional L2/L3 Ethernet modules hardware-based QoS is supported. Each type of QoS support has its own configuration capability in the CLI.

The following sections describe the software-base features of QoS followed by a description of hardware-based QoS.

QoS ensures bandwidth guarantees throughout the system by implementing Random Early Detection (RED) to address congestion and Class Based Queuing (CBQ) to address bandwidth guarantees.

iBG series' bandwidth management capability allows multiple agencies or customers to share access bandwidth on a WAN link in a controlled fashion to effectively and efficiently utilize available bandwidth. Even during times of congestion, each customer is guaranteed a share of the access bandwidth and is allowed to borrow unused bandwidth from other customers. This bandwidth management capability allows service providers to offer their customers Internet access based on the amount of guaranteed bandwidth-committed rate (CR) and the amount of bandwidth-borrowed burst rate (BR).

Similarly, an organization can share its access bandwidth among its different departments.

Features

The network administrator manages bundle bandwidth across various customers by defining traffic classes. Each traffic class is assigned the desired committed bandwidth as well as the burst bandwidth. The sum of the CRs of all classes must be less than or equal to the total bundle bandwidth. CBQ can only be used in the WAN outbound direction.

A traffic class is characterized by the following parameters:

- Class name
- Parent class
- Committed rate (CR)
- Peak rate (PR)
- Classification type based on:
 - Application ports (TCP or UDP)
 - Network level
- Source or destination IP addresses, address ranges, or subnets
 - Ethernet MAC
- VLAN identifiers

Traffic classes are arranged in a hierarchical manner. A class has a parent class and can have one or more child classes. The root class has no parent and is identified as *root-out* or *root-in*. The only limit to the number of classes that can be created is 1500 per interface.



NOTE

QoS Mechanism for LMG20, LMG44, and LMGP-44

Ubigate supports many LAN modules to support Ethernet switching capability. QoS architecture for LMG20, LMG44 and LMGP-44 is different from the other LAN modules.

In LMG20, LMG44 and LMGP-44, a group of ports shares a common resource to control QoS internally. Because of this, ports belonging to the same group have the same QoS configuration. That is, if QoS is configured for a single port, the same configuration is automatically applied to all the ports belonging to the same group.

**NOTE**

Here is the information that maps each group and their member ports sharing the same QoS configuration.

[LMG20]

- Group 1: 0
- Group 2: 1, 2, 11, 12
- Group 3: 3, 4, 13, 14
- Group 4: 5, 6, 15, 16
- Group 5: 7, 8, 17, 18
- Group 6: 9
- Group 7: 10
- Group 8: 19

[LMG40 /LMGP44]

- Group 1: 0, 1, 22, 23
- Group 2: 2, 3, 24, 25
- Group 3: 4, 5, 26, 27
- Group 4: 6, 7, 28, 29
- Group 5: 8, 9, 30, 31
- Group 6: 10, 11, 32, 33
- Group 7: 12, 13, 34, 35
- Group 8: 14, 15, 36, 37
- Group 9: 16, 17, 38, 39
- Group 10: 18, 19, 40, 41
- Group 11: 20, 21, 42, 43

Definitions

- **Committed Rate**

Each traffic class can be assigned a CR parameter in Kbps. This is the amount of bandwidth that the class or flow is guaranteed at all times, even during congestion. The sum of the CRs for all classes in a given direction cannot exceed the access bandwidth of their parent class. By maintaining a moving average of the bandwidth for each class, the class is not ‘strictly’ policed at CR Kbps, and momentary peaks in the flow are permitted. The goal is that each class with sufficient demand will be able to receive roughly its allocated bandwidth over some interval of time.

- **Peak Rate**

Every traffic class can be configured with a peak rate parameter, which is the bandwidth that can be offered to that class if unused bandwidth is available from other classes. This provides for very efficient bandwidth utilization. A class can be configured to borrow whatever bandwidth is available from its parent class up to the PR limit set for that class. To prevent a class from borrowing, set the CR equal to the PR. Also, note that a class cannot borrow more than the bundle bandwidth.

Classification Types

The example in Figure 10.1 reserves the largest CR (1536 Kbps) for two servers, 10.1.1.1 and 10.1.1.2, which are members of the SrcOne class. The remainder of the 10.1.1.0/24 subnet is assigned to the SrcTwo class and is configured with a CR of 1024 Kbps. Additionally, the SrcTwo class is further divided into application port classes. All other hosts in Figure 10.1, the default class, are configured for a CR of 512 Kbps.

The classification type must be the same across a given level of traffic class. Note in Figure 10.1, that the classification type at the first level traffic class is the source IP address; for the second level, the classification type is the application port. Because bandwidth limitations are evaluated from most specific to least specific, 10.1.1.1/32 falls within the SrcOne class.

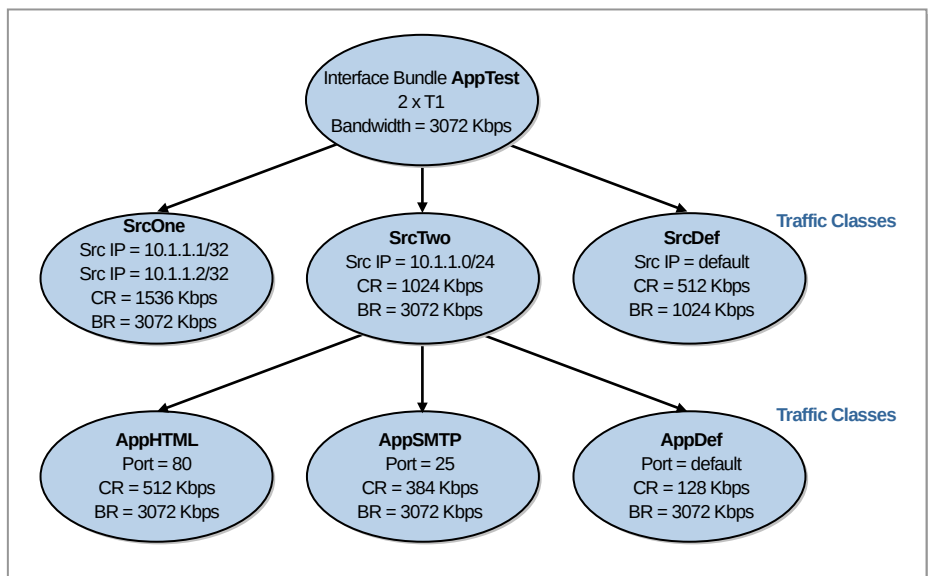


Figure 12.1 Assigning Classification Types

Configuration

Create Bundle AppTest

```
Router/configure# interface bundle AppTest
Router/configure/interface/bundle AppTest# link t3 1/19
Router/configure/interface/bundle AppTest# encaps ppp
Router/configure/interface/bundle AppTest# ip addr 199.1.1.1
255.255.255.252
```

Create Traffic Classes

```
Router/configure/interface/bundle AppTest# qos
Router/configure/interface/bundle AppTest/qos# add-policy-
class SrcOne
root-out src-ip 10.1.1.1-10.1.1.2 netmask 255.255.255.255
Router/configure/interface/bundle AppTest/qos# add-policy-
class SrcTwo
root-out src-ip 10.1.1.0 netmask 255.255.255.0
Router/configure/interface/bundle AppTest/qos# add-policy-
class SrcDef
root-out src-ip default
Router/configure/interface/bundle AppTest/qos# add-policy-
class AppDef
SrcTwo port default
Router/configure/interface/bundle AppTest/qos# add-policy-
class AppSMTP
SrcTwo port 25
Router/configure/interface/bundle AppTest/qos# add-policy-
class AppHTML
SrcTwo port 80
Router/configure/interface/bundle AppTest/qos# policy-class
SrcOne
Router/configure/interface/bundle AppTest/qos/policy-class
SrcOne# cbq cr 1536 pr 1536
Router/configure/interface/bundle AppTest/qos/policy-class
SrcOne# exit policy-class
Router/configure/interface/bundle AppTest/qos# policy-class
SrcTwo
Router/configure/interface/bundle AppTest/qos/policy-class
SrcTwo# cbq cr 1024 pr 1536
Router/configure/interface/bundle AppTest/qos/policy-class
SrcTwo# exit policy-class
```

```
Router/configure/interface/bundle AppTest/qos# policy-class
AppHTML
Router/configure/interface/bundle AppTest/qos/policy-class
AppHTML# cbq cr 512 pr 1024
Router/configure/interface/bundle AppTest/qos/policy-class
AppHTML# exit policy-class
Router/configure/interface/bundle AppTest/qos# policy-class
AppSMTP
Router/configure/interface/bundle AppTest/qos/policy-class
AppSMTP# cbq cr 384 pr 1024
Router/configure/interface/bundle AppTest/qos/policy-class
AppSMTP# exit policy-class
Router/configure/interface/bundle AppTest/qos# policy-class
AppDef
Router/configure/interface/bundle AppTest/qos/policy-class
AppDef# cbq cr 128 pr 1024
Router/configure/interface/bundle AppTest/qos/policy-class
AppDef# exit policy-class
Router/configure/interface/bundle AppTest/qos# policy-class
SrcDef
Router/configure/interface/bundle AppTest/qos/policy-class
SrcDef# cbq cr 256 pr 512
Router/configure/interface/bundle AppTest/qos/policy-class
SrcDef# exit policy-class
Router/configure/interface/bundle AppTest/qos# end
```

VLAN Identifiers

Figure 10.2 illustrates the classification based on VLAN identifiers. Note that these classes are leaf classes and do not have child classes.

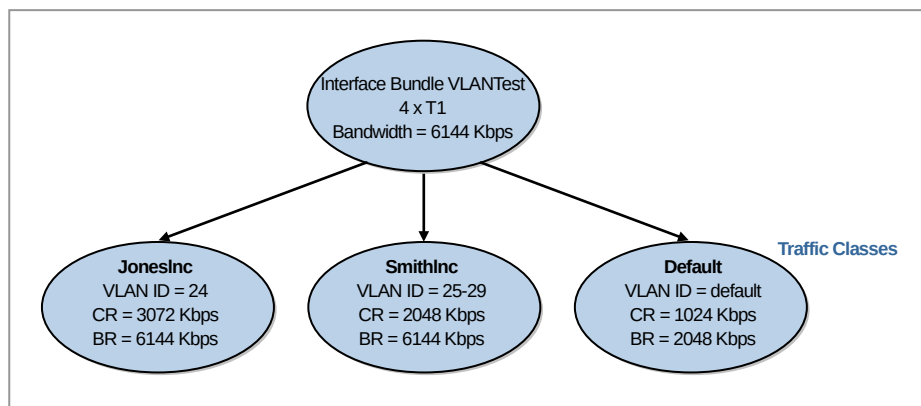


Figure 12.2 Assigning VLAN Identifiers

Configuration

The following is the configuration for the topology shown in Figure 10.2.

Create bundle VLANtest

```
Router# conf terminal
Router/configure# interface bundle VLANtest
Router/configure/interface/bundle VLANtest# link t3 1/23
Router/configure/interface/bundle VLANtest# encap ppp
Router/configure/interface/bundle VLANtest# ip addr
200.1.1.1255.255.255.252
```

Create Traffic Classes and Assign Classifications

```
Router/configure/interface/bundle VLANtest# qos
Router/configure/interface/bundle VLANtest/qos# add-policy
JonesInc root-out vlan-id 24
Router/configure/interface/bundle VLANtest/qos# add-policy
SmithInc root-out vlan-id 25 29
Router/configure/interface/bundle VLANtest/qos# add-policy
class
Default root-out vlan-id default
Router/configure/interface/bundle VLANtest/qos# policy-class
JonesInc
Router/configure/interface/bundle VLANtest/qos/class
JonesInc#
cbq cr 3072 pr 6144
Router/configure/interface/bundle VLANtest/qos/class
JonesInc#
exit
Router/configure/interface/bundle VLANtest/qos# policy-class
SmithInc
Router/configure/interface/bundle VLANtest/qos/class
SmithInc# cb
q cr 2049 pr 6144
Router/configure/interface/bundle VLANtest/qos/class
SmithInc# exit
Router/configure/interface/bundle VLANtest/qos# policy-class
Default
Router/configure/interface/bundle VLANtest/qos/class
Default# cbq 1024 pr
2048
Router/configure/interface/bundle VLANtest/qos/class
Default# exit
Router/configure/interface/bundle VLANtest/qos# enable
Router/configure/interface/bundle VLANtest/qos# end
```

Historical Statistics

The Historical statistics command enables users to collect statistics for every N hours ($N < 4$ hours) and upload the statistics for every class to an FTP server. The data is sent in an ASCII format file with three sections. The first section includes the upload time, system IP address, sample interval in minutes, and the upload interval in minutes. The second section includes class-based statistics for all bundles configured and enabled with QoS. The third section includes class-based statistics. Empty lines and header lines in the file start with the '#' character. The bundle statistics start with the character 'B', and class statistics start with the character 'C'. These designations allow easier parsing of the file.

Configuring Historical Statistics

```
Router# configure terminal
Router/configuration# qos
Router/configuration/qos# historical-stats
Router/configuration/qos/historical-stats# ftp-parameters
Primary Ftp Server: 105.52.35.77
Secondary Ftp Server: 105.52.35.78
Ftp user name: test
Ftp password: <password>
Router/configuration/qos/historical-stats# sample-interval 10
Router/configuration/qos/historical-stats# upload interval 1
file-id
Router.stats
Uploading of Historical Statistics enabled
Upload interval set to 1 hours
Upload-file ID set to Router.stats
```

```
Router/configuration/qos/historical-stats# show qos historical-
stats configuration

Historical Statistics Configuration
-----
Sample Interval      : 10minutes
Uploading            : ENABLED
```

Figure 12.3 Screen Display for show QoS bulkstats_config Command

Traffic Policing versus Traffic Shaping

Policing controls the traffic by dropping packets or marking down their priority when the configured rate is exceeded. Shaping controls the traffic by delaying packets using a queuing mechanism when they arrive faster than the configured rate. Therefore shaping can smooth out the burst in a flow, helping to minimize buffer overruns in intermediate routers. Policing does not smooth out peaks, but it can control peaks by dropping packets or marking them down.

Since shaping delays packets, thereby throttling the packet rate instead of dropping them, adaptive applications (those using TCP) perform better. Dropping packets can cause exponential back-off of TCP which can affect the throughput. This problem with policing can be minimized by configuring the peak parameter of the policer to be a sufficiently large value.

Need for Traffic Policing

Policing has the advantage of providing low latency since it does not queue packets. This makes policing a good choice for interactive and streaming voice and video applications. Policing also uses much less resources in the router than shaping. It is a better and more practical method to provide QoS for incoming traffic on an interface.

On iBG access routers, policing can be used to limit the maximum rate of a traffic flow received on a WAN interface. This is especially useful when the POP/CO router does not do any shaping or policing of traffic before transmitting it onto the WAN or it is under a different administrative domain which prevents access to the QoS configuration.

Traffic Policing Functionality

Customers can rate-limit inbound traffic on the WAN links using policing while doing CBQ for outbound traffic. It is also possible to police outbound WAN traffic. However, for shaping purpose

Traffic policing is also supported on Ethernet interfaces. Check section ‘Verifying Policing Status and Configuration’ for limitations.

Traffic policing is implemented using a token bucket algorithm. Users will be able specify two parameters when configuring traffic policing, Rate (token fill rate) and Peak (number of tokens). Rate is specified in *Kbps*. Peak can be specified in *kilobits* or as a duration (based on the configured rate) in *milliseconds*. ‘Rate’ determines the average bandwidth for the policed flow and ‘Peak’ determines the maximum peak (in bits or bytes) permitted for the flow. Packets conforming to these limits will be forwarded and those violating these limits will be dropped.

Specifying just the ‘Rate’ and ‘Peak’ makes the policing feature simple and effective. The ‘extended peak’ parameter is needed to permit a large packet, by loaning tokens, when there are not enough tokens available at a given time for the entire packet. The policing algorithm allows for such ‘loaning of tokens’ by default.

Configuring Traffic Policing

As with CBQ, the first step is traffic classification. Flows should be defined by creating traffic classes. To classify based on multiple fields, for example, source IP address and port, a hierarchy of classes should be created. Traffic policing for a class can be configured using the ‘police’ command at the class level as shown below. Policing for non-leaf classes (which define more aggregate flows) is currently not supported. Multi-level policing will be supported in a later release.

Verifying Policing Status and Configuration

The two CLI display commands below can be used to check the policing configuration and status for a class and for an interface. **show qos bundle bundle_name** shows the policing status on the interface and the bandwidth each class is getting along with its configured policing rate. **show qos bundle bundle_name class class_name** shows detailed information for the class including configured policing parameters and packet drops due to policing.

```
R87# show qos bundle wan1
Interface: Bundle wan1 (Bandwidth = 3072Kbps)
Interface Outbound Configuration & Statistics
-----
CBQ: on Policing: off MON: off
+-----+-----+-----+-----+-----+-----+-----+-----+
Traffic Class CBQ-CR CBQ-PR Police Avg Out Avg In Packets Packets
              (kbps) (kbps) (kbps) (kbps) (kbps) Fwded   Dropped
+-----+-----+-----+-----+-----+-----+-----+-----+
s1          500    3072      -  1781.2 2666.6   4451    2220
s1-def      100    3072     800   891.6 1333.1   2229    1107
s1-web      100    3072     900   889.5 1333.4   2222    1113
def-o       500    3072    1333  1290.7 1333.4   3230     109
Interface Inbound Configuration & Statistics
-----
Policing: on MON: off
+-----+-----+-----+-----+-----+-----+-----+-----+
Traffic Class CBQ-CR CBQ-PR Police Avg Out Avg In Packets Packets
              (kbps) (kbps) (kbps) (kbps) (kbps) Fwded   Dropped
+-----+-----+-----+-----+-----+-----+-----+-----+
def-in       -      -    1100   999.7  999.7    481      0
d1           -      -      -   1901.2 1999.6   1096     57
d1-def       -      -      -    998.9  998.9    576      0
d1-web       -      -    900   902.2 1000.6    520     57
R87#
```

```
R87# show qos bundle wan1 d1-web
Class: d1-web (Inbound)
Parent Class: d1 (CR = 0 kbps ; PR = 0 kbps)
Interface: Bundle wan1 (bandwidth = 3072 kbps; MON IN: off)
Configuration
-----
Policing - Rate: 900 Kbps Peak: 1000 msec
Application Ports assigned to this Class:
80 8080
Traffic Statistics
-----
```

```
Avg Rate Out: 901.8 Kbps
Avg Rate In: 1000 Kbps
Counters since last boot/clear:
Packets Forwarded: 26222      -- Packet drop details
Bytes Forwarded: 34088600    Queue overflow: 0
Packets Dropped: 2913        No buffers: 0
Bytes Dropped: 3786900       Policing: 2913
                                RED: 0
R87#
```

Limitations

The following limitations apply for this release:

- Policing is not supported for outbound traffic on Ethernet interfaces.
- Multi-level policing is not supported. Policing is done only for leaf classes. Any policing configuration on non-leaf classes is ignored.
- Policing and CBQ shaping are independent and mutually exclusive features. You must configure CBQ parameters if you to enable the CBQ shaping feature.

Multi-Field Classification

The Multi-Field (MF) classifier is an important component of QoS. Its purpose is to help define flows for which appropriate service parameters can be configured. Flow classification is the first step in the QoS process. The aggregate traffic is classified into flows or traffic classes. Each traffic class can be configured with the desired QoS parameters, which determine the forwarding treatment given to packets matching that class.

The classifier will support multi-field (MF) classification of packets based on any combination of the following header fields:

- Packet class
- Source IPv4 address (or prefix)
- Destination IPv4 address (or prefix)
- IPv4 DiffServ codepoint (DSCP)
- IPv4 precedence
- IPv4 protocol type
- Source/destination TCP/UDP ports
- VLAN ID
- 802.1p values (User Priority)
- MPLS EXP bits
- Control packet
- Source IPv6 address (or prefix)
- Destination IPv6 address (or prefix)
- Flow label
- Traffic class

Traffic classification can be configured for inbound and outbound traffic on any interface. Multiple values can be specified for each of the above attributes to define 'more aggregate' or 'coarser' flows. Values can be specified either as a range or multiple non-contiguous values. There is no restriction on the number of values, for example, any number of IP addresses can be assigned to a traffic class for creating a match rule.

A classification attribute can be wildcarded by assigning a special value of 'default' for that attribute.

Packet Marking

The following attributes can be marked for packets, which are successfully classified.

- Mark DSCP
- Mark IP Precedence
- Mark 802.1p user priority
- Mark QoS priority

Configuring MF Classification

This section will discuss how the configuration is done for MF classification and what kind of input is expected from the user.

Refer to Figure 10.4 for the following explanation.

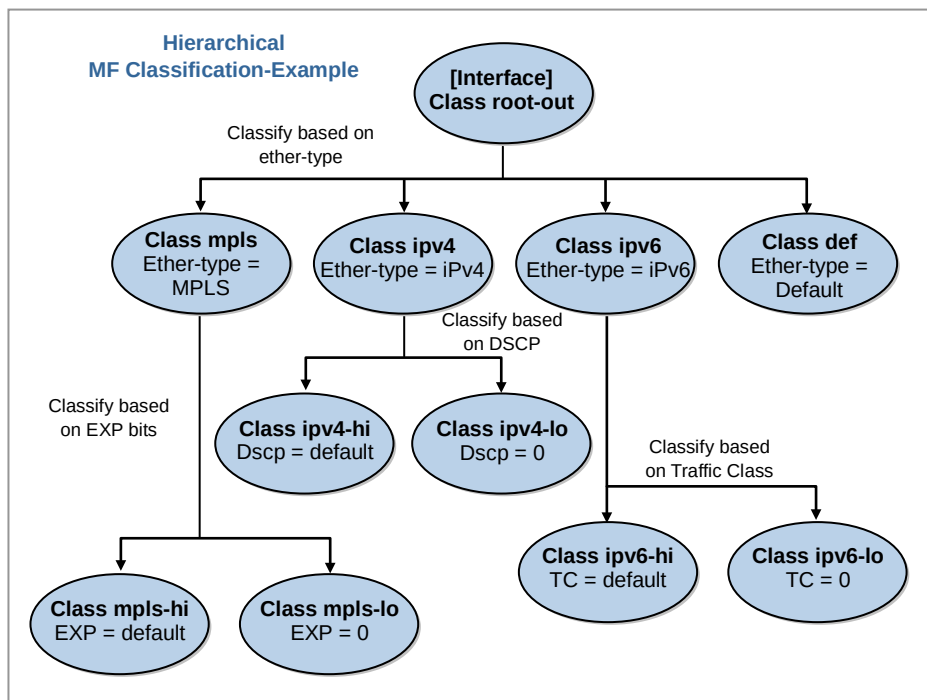


Figure 12.4 MF Classification

The user configures MF classification for a specific interface and for a specific traffic direction. He constructs the class hierarchy by specifying the parent-class for each new class he wants to create. In order to create a new class, the user must specify the class-name of the new class, the class name of the parent-class and a match rule. To add classes at the first level, the name of the root-class should be specified as the parent class. There are two root classes, 'root-out' for the outbound classification tree and 'root-in' for the inbound tree. These root classes are automatically created at interface creation time. So the general command format for creating class is

```
add-policy-class {<class-name>} {<parent-class>} [ { <match-field-type>
<match-field-values>}]
```

where

<class-name> is name of the class being added

<parent-class> can be ether 'root-out' or 'root-in'

<match-field-type> can be either 'packet-class', 'src-ip', 'dest-ip', 'port', 'vlan-id', 'dscp', 'user-priority', 'protocol-type', 'ip-precedence', 'label', or 'exp'

<match-field-values> depends on <match-field-type>

In particular if <match-field-type> is...

'packet-class'	IPv4, MPLS, ARP etc.
'src-ip' or 'dest-ip'	IP address/range/subnet
'port'	TCP/UDP port numbers
'vlan-id'	VLAN identifier
'dscp'	IPv4 DSCP value
'user-priority'	0 - 7
'protocol-type'	IPv4 protocol type
'ip-precedence'	IP header precedence value
'exp'	MPLS EXP field value
'control-packet'	Control packet

In the above command third set of argument, which specified the classification type, is optional. If not entered, it is not considered as a valid class for classification. So in such cases user can enter in to the class context via CLI command 'policy-class <class>' and then configure the required classification type. But the classification type at given level must be same as peer classes.

Here is an example of how classes 'mpls', 'mpls-lo', 'mpls-hi', 'ipv4', 'ipv4-lo', 'ipv4-hi', and 'def' (ether-type=ANY-OTHER) would be created.

```
Configure/interface/bundle wan1/qos# add-policy-class mpls
rootout
packet-class mpls
Configure/interface/bundle wan1/qos# add-policy-class mpls-
lo mpls
exp 0
Configure/interface/bundle wan1/qos# add-policy-class mpls-
hi mpls
exp default
Configure/interface/bundle wan1/qos# add-policy-class ipv4
rootout
packet-class ipv4
Configure/interface/bundle wan1/qos# add-policy-class ipv4-
lo ipv4
dscp 0
Configure/interface/bundle wan1/qos# add-policy-class ipv4-
hi ipv4
dscp default
Configure/interface/bundle wan1/qos# add-policy-class def
root-out
packet-class default
```

In the above commands, 'packet-class', 'exp', 'dscp', and 'tc' are the matching field (classification) types for various rules specified above.

Whenever the matching/classification field type specified for the first child class, which is being created, the search algorithm is decided based on the matching/classification field type in the policy rule and accordingly the search function and search structure in the parent class are initialized.

The match values are added to the search structure in the parent class and a reference to the (matching) child-class is stored in each of those entries. In this example, when class 'mpls' is added, the 'search_type' in the parent class 'root-out' is set to 'packet-class'. The search function and search structure pointers are set to do a hash table lookup based on packet-class value.

The ether-type value of 0x8847 is added to the hash table and a pointer to class 'mpls' is stored in that entry. For any classification type, it is possible for the match rule to have a range of values or multiple, non-contiguous values. Remember that once the first child-class added and the 'classification-type' or 'search-type' is set in the parent class, any subsequent child classes of that parent class must have the same classification type in its match rule. Note that this is not a limitation but an inherent property of the hierarchical classification concept.

For a given parent-class, if the search does not yield a match, the packet is matched to the child-class pointed to by the 'default_class' attribute. This class is known as a 'default class'. One of the child-classes of a given parent-class can be configured as a default class. If there is no default class, packets for which the search does not yield a match will be dropped. In our example, class 'def' is a default class of parent-class 'root-out'. It would be created as follows.

```
Configure/interface/bundle wan1/qos# add-policy-class def root-out  
packetclass default
```

Each class has a queue structure associated with it. However, when a class becomes a parent class due to the addition of child classes under it, its queue structure 'loses significance' and is no longer active. The queue structure plays major role in achieving CBQ queuing and scheduling.

Traffic Policing

Policing controls the traffic by dropping packets or marking down their priority when the configured profile is exceeded. Shaping controls the traffic by delaying packets using a queuing mechanism when they arrive faster than the configured rate. Therefore shaping can smooth out the burst in a flow, helping to minimize buffer overruns in intermediate routers. Policing does not smooth out bursts, but it can control bursts by dropping packets or marking them down.

Since shaping delays packets, thereby throttling the packet rate instead of dropping them, adaptive applications (those using TCP) perform better. Dropping packets can cause exponential back off of TCP, which can adversely affect the throughput. This problem with policing can be minimized by configuring the burst parameter of the policer to be a sufficiently large value.

Policing has the advantage of providing low latency since it does not queue packets. This makes policing a good choice for interactive and streaming voice and video applications. Policing also uses much less resources in the router than shaping. It is a better method to provide QoS for incoming traffic on an interface.

In the iBG series, policing can be enabled in both the ingress and egress directions, on the WAN interfaces, MAN interfaces, FE interfaces and the GE interfaces on the main board. For LAN GE interfaces, traffic policing will be done in hardware. The policing feature can be more appropriately described as ‘Class Based Policing’. Traffic Policing can be enabled individually for each traffic class that defines a flow. This includes any inbound or outbound ‘leaf’ class created on an interface. Policing can be enabled in either srTCM or trTCM mode.

The supported policing features in software enables to rate limit the traffic corresponding to micro flow, aggregate flow, or behavior flow. For example, VLAN ID based policing can be enabled on ingress traffic by configuring traffic class with VLAN ID is the classification key and setting appropriate policing parameters for traffic class. Similarly for application-based rate limiting, configuring traffic class with application identifier as a classification key and configuring policing parameters for traffic class can achieve rate limiting.

Some clarification on acronyms will be helpful before going into the design discussion about policing.

CIR	Committed Information Rate
CBS	Committed Burst Size
CBT	Committed Burst Time
EBS	Excess Burst Size
PIR	Peak Information Rate
PBS	Peak Burst Size
PBT	Peak Burst Time
BS	Burst Size
tc	Burst Interval.
Tc	Token bucket representing committed rates
Te	Token bucket representing excess rates
Tp	Token bucket representing peak rates

Policing Using Single Rate Three Color Marking (srTCM)

The srTCM algorithm uses single rate CIR, and two burst sizes, i.e., CBS, and EBS. The srTCM will be implemented using two token buckets, i.e., Tc of size CBS, and Te of size EBS. A packet is ‘colored’ green if it doesn’t exceed the CBS, yellow if it does exceed the CBS but not the EBS, and red otherwise. Coloring is just a means to convey the conformance level of packets. An action can be configured for each color. The supported actions include: Permit, Mark DSCP value and Drop.

The srTCM works as follows. Let the token buckets be represented by Tc(t) whose maximum capacity is CBS bytes, and Te(t) whose maximum capacity is EBS bytes. One token is the equivalent of one byte. Tc(0) is equal to CBS, and Te(0) is equal to EBS. Thereafter tokens are replenished as follows. If $Tc < CBS$ then Tc is incremented by CIR bytes-per-second up to CBS else if $Te < EBS$ then Te is incremented by CIR bytes-per-second up to EBS.

When packet of size B bytes arrives for policing, if $T_c(t) - B \geq 0$, then the packet is marked green (transmit) and T_c is decremented by B else if $T_e(t) - B \geq 0$ then packet is marked yellow and T_e is decremented by B else packet is marked red. This mode of operation is the default mode and is known as color-blind mode.

In the color aware mode, packet is assumed to be pre-colored. In this case when packet of size B bytes arrives for policing, if $T_c(t) - B \geq 0$ and packet color is green, then the packet color is unchanged (transmit) and T_c is decremented by B else if $T_e(t) - B \geq 0$ and packet's color is green then the packet is marked yellow and T_e is decremented by B else if packet color is green or yellow, then the packet is marked red.

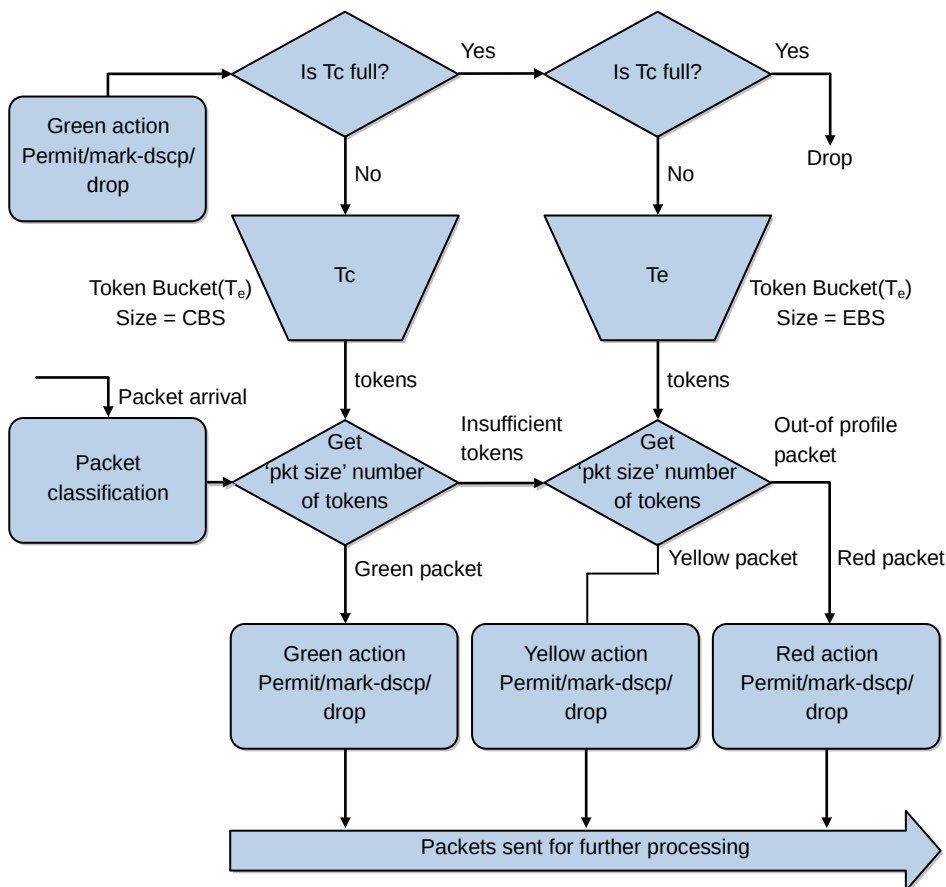


Figure 12.5 Single Rate Three Color Marking

The CIR will be specified in Kbps. CBS and EBS will be specified in Kbits. CBT is defined by the relationship ($CIR = CBS/ CBT$). The token filling process has to run at least every CBT milliseconds, without which CIR cannot be sustained. It is recommended that CBS be large enough for CBT to be at least 1 second. Therefore it is sufficient for the token filler to execute every 1 second and fill CBS number of tokens into the Tc and Te buckets.

In our implementation, we will execute the token filler every 100 ms. This process will replenish tokens in all buckets configured on all interfaces in the system. Running the token filler more frequently results in more frequent and incremental updates to the token bucket, which can result in a smoother traffic pattern. This process will execute within the context of the forwarding task so that no context switches are involved, leading to better performance.

Configuring srTCM

To enable policing using srTCM, CIR, CBS and EBS need to be configured. CIR configuration will be mandatory and CBS and EBS parameters will be optional. CBS will have a default value equal to 'CIR' Kbits, which means that the default burst time will be 1 sec. EBS will have a default value of 0 Kbits.

An action corresponding to each color assigned to the packet can also be configured. The types of actions that will be supported are 'permit', 'markdscp' and 'drop'. A DSCP value must be provided if the action type selected is 'mark-dscp'. The configuration of actions will not be mandatory. They will have the following default values: green packets - 'permit', yellow packets - 'mark-dscp 0' and red packets - 'drop'. srTCM can be configured and enabled for each 'leaf' traffic class on an interface.

The trTCM (Two Rate Three Color Marker)

The trTCM algorithm uses two rates CIR and PIR, and two burst sizes, CBS and PBS. The trTCM is typically implemented using two token buckets, Tc of size CBS, and Tp of size PBS. A packet is marked red if it exceeds PBS, yellow if it exceeds CBS but not PBS, otherwise it is green. Coloring is just a means to convey the conformance level of packets. An action can be configured for each color. Supported actions include Permit, Mark-DSCP and Drop.

Let the token buckets be represented by Tc(t) whose maximum capacity is CBS bytes, and Tp(t) whose maximum capacity is PBS bytes. One token is the equivalent of one byte. The Tc(0) is equal to CBS, and Tp(0) is equal to PBS. Thereafter, tokens are replenished as follows. If $Tc < CBS$ then Tc is incremented by CIR bytes-per-second up to CBS, and if $Tp < PBS$ then Tp is incremented by PIR bytes-per-second up to PBS.

When packet of size B bytes arrives for policing, if $Tp(t) - B < 0$, then the packet is marked red else, if $Tc(t) - B < 0$ then the packet is marked yellow and Tp is decremented by B else the packet is marked green and both Tc and Tp are decremented by B. This mode of operation is the default mode and is known as color-blind mode.

In the color aware mode, packet is assumed to be pre-colored. In this case when packet of size B bytes arrives for policing, if $Tp(t) - B < 0$ and packet color is green or yellow, then the packet marked red else if $Tc(t) - B < 0$ and packet color green then the packet marked yellow and Tp is decremented by B else packet's color is unchanged and both Tc and Tp are decremented by B.



Figure 12.6 Two Rate Three Color Marking

The CIR and PIR will be specified in Kbps. CBS and PBS will be specified in Kbits. CBT and PBT are defined by the relationships ($CIR = CBS/CBT$) and ($PIR = PBS/PBT$). The period of the token filling process should at least be equal to the lesser of CBT and PBT milliseconds. Without which CIR and PIR cannot be sustained. It is recommended that CBS and PBS be large enough so that CBT and PBT are at least 1 second.

Therefore it is sufficient for the token filler to execute every 1 second and fill CBS number of tokens into the Tc bucket and PBS number of tokens into the Tp bucket. However, in our implementation the token filler will run every 100 ms. Note that the same token-filling process will replenish tokens in all srTCM and trTCM token buckets.

Configuring trTCM

To enable policing using trTCM, CIR, CBS, PIR and PBS need to be configured. CIR and PIR configuration will be mandatory and CBS and PBS parameters will be optional. CBS will have a default value equal to 'CIR' Kbits, which means that the default committed burst time will be 1 sec. PBS will have a default value equal to 'PIR' Kbits, which means that the default peak burst time will be 1 sec. An action corresponding to each color assigned to the packet can also be configured. The types of actions that will be supported are 'permit', 'mark-dscp' and 'drop'. A DSCP value must be provided if the action type selected is 'mark-dscp'. The configuration of actions will not be mandatory. They will have the following default values: green packets - 'permit', yellow packets - 'mark-dscp 0' and red packets - 'drop'. trTCM can be configured and enabled for each 'leaf' traffic class on an interface.

Statistics

The following traffic statistics will be collected when srTCM or trTCM policing is enabled. Note that since policing can be enabled on a per-class basis, these statistics are maintained for each leaf class.

- Number of packets colored green
- Number of packets colored yellow
- Number of packets colored red
- Number of packets permitted
- Number of bytes permitted
- Number of packets dropped
- Number of bytes dropped
- Number of packets marked

Egress Queuing, Shaping and Scheduling

The CBQ along with congestion detection & avoidance and scheduling algorithm forms full fledged class-based packet queuing and scheduling method in the iBG platform. Shaping of egress traffic to a configured ‘peak rate’ is also supported as part of CBQ. The following sub-sections provide details on design, implementation and configuration & management.

The CBQ feature works closely with the hierarchical MF classifier. As a first step, traffic classes should be configured in a hierarchical fashion in the outbound direction on an interface. The leaf-classes are of greater significance since they actually represent the traffic flows for which QoS needs to be configured. When CBQ is enabled, each leaf-class will have a queue (‘class-queue’) associated with it. Hence the term Class Based Queuing. CBQ service parameters can be configured for each leaf-class.

These parameters are Committed Rate (CR), Peak Rate (PR) and Priority.

After the destination look-up, the outgoing interface is identified and the packet is taken through the hierarchical MF classification configured on that interface. After the packet is classified into a leaf traffic class, it is placed in its class-queue. The CBQ scheduler periodically services the class-queues of all leaf traffic classes on each interface. The service that each class queue receives depends on the service parameters (CR, PR, Priority) assigned to it. Eight priority levels will be supported. Priority 1 is the highest and 8 is lowest.

CBQ Scheduler Operation

This section explains the scheduler operation and algorithm.

The scheduler lists are part of CBQ structure. As you see, the scheduler list contains only leaf classes of egress classification tree in given interface. There are eight prioritized individual scheduling lists numbering from 1 through 8, where 1 being the highest, and 8 being the lowest priority. Each scheduling list is formed as circular linked list of same priority classes. In each list head points to leaf class from where scheduling starts with. The rest of the section explains about scheduling operation, excess bandwidth list formation, fairness for classes in the same priority.

For understanding of CBQ operation, let us first consider all classes to be of equal priority. The scheduler runs every 5 ms to service the queues on each interface. (Each leaf class is associated with a queue). In every scheduling interval, the scheduler makes two passes on the classes of each interface. In the first pass, it transmits bcr bytes from each class in the scheduler list, where bcr of a class is the number of bytes it can send in one scheduling interval (5 ms) proportional to its CR. If the packet to be sent is greater than bcr bytes, it is not sent and the class is given a credit of bcr bytes which it can use the next time it is serviced. (In other words, the class has a deficit of bcr bytes). Later, when the $(credit + bcr)$ for the class equals or exceeds the size of the packet (at the queue head), it is transmitted.

Packets are transmitted from a queue as long as the $(bytes\ sent + current\ packet\ size)$ does not exceed $(credit + bcr)$. When no more packets can be sent, the credit is updated to $(credit + bcr - bytes\ sent)$. During the first pass, if a class has more packets to send even after using bcr bytes, and it's $BR > CR$, the class is added to the tail of the 'xs-bw-list'. Therefore, the 'xs-bw-list' consists of classes that need to send bytes in excess of the amount permitted by their CR and are permitted to do so by their BR. Let us define Bc as the total number of bytes that can be sent on an interface in one scheduling interval

(5 ms) proportional to its bandwidth. If the total number of bytes sent or credited in the first pass is less than Bc , it means additional bytes can still be transmitted. This excess bandwidth can be given to the classes that still have packets to send and whose $BR > CR$. For this, a second pass is done, through a 'xs-bw-list'. In the second pass, the excess bytes are first offered to the first class in this list, then to the second class if some are still available and so on until the excess bytes are exhausted or all classes in the 'xs-bw-list' have been satisfied. The excess bytes available to a class cannot exceed $(bbr - bcr)$, where bbr is the maximum bytes that a class can send in a scheduling interval (5 ms) proportional to its BR. Again, packets from a queue can be sent only as long as $(excess\ bytes\ sent + current\ packet\ size)$ does not exceed $(excess\ bytes\ available + credit)$. When packets can no longer be sent, any deficit equal to $(excess\ bytes\ available + credit - excess\ bytes\ sent)$ is credited to the class. If all packets from the queue could be transmitted, the credit is set to 0. The remaining excess bytes $(Total\ excess\ bytes\ available - excess\ bytes\ offered\ to\ this\ class)$ are then offered to subsequent classes in the 'xs-bw-list'.

To sum up, the scheduler makes two passes for each interface every scheduling interval. In the first pass, enough bytes are sent from each class to guarantee its CR and a second pass is done to distribute any excess bandwidth available.

If the classes are always serviced in the same order in the first pass (and hence in the second pass as well) it will lead to unfair servicing of the equal priority classes. To solve this problem of unfairness, the 'head' of the scheduler list is advanced to point to the next class (in the circular list) for the next scheduler interval. As a result each class experiences the same average queuing delay. Since the scheduling order in the first pass also determines the order in the second pass, rotation of the list head also happens for the 'xs-bw-list'. Therefore, each class receives an equal share of the excess bandwidth on an average.

In the first pass, the scheduler services the list at the highest priority level first, followed by the list at the next lower priority level and so on. Classes in a circular list (having the same priority) are serviced in the same manner as explained above, by advancing the list-head around the circular list every scheduling interval. Classes at a higher priority will always be serviced before those at a lower priority level. The 'xs-bw-list' formed during this first pass will contain classes in the same order in which they were serviced in the first pass. Therefore, a higher priority class will always be serviced prior to a lower priority class during the both the first and second pass. Consequently its traffic will experience lower average latency and will also have access to any excess bandwidth before the traffic in the lower priority class.

When CBQ is enabled, the backpressure from packet driver is automatically handled in CBQ scheduling mechanism. As the CBQ scheduling happens at physical port level which has an associated driver queue. The logical driver queue thresholds and queue depth is maintained at port level. So before dequeuing packet from CBQ queues, the scheduling mechanism make sure that driver queue has enough capacity to accommodate it.

Following are the main points of the CBQ scheduling algorithm, which is also referred to as DRR-P (DRR with Priority).

- DRR-P can guarantee bandwidth for each class/queue.
- The algorithm offers bandwidth based on bytes and not packets. Therefore It does not allow flows with bigger packet sizes to dominate.
- The scheduler runs periodically every 5 ms. the quantum (in DRR terminology) to be sent from each class in each pass is accordingly set. This limits the queuing delay experienced by each queue/class because each class is serviced at least once every 5ms.
- The algorithm supports prioritization in terms of both latency and bandwidth borrowing.
- A class can be rate limited to a configured maximum value.

Buffer Management for Class Queues

It is not possible for a class to guarantee bandwidth if it doesn't have enough buffers for its queue, because the packets can be dropped even before they have a chance to be scheduled. Therefore it is essential to have a good buffer management scheme along with a good scheduling algorithm. This scheme should strike a good balance between buffer availability for each queue and the amount of memory consumption of these buffers.

Congestion Management on Class Queues

After a packet has been classified in to a leaf traffic class node, it needs to be queued in to packet queue of the leaf traffic class node. This queuing process is controlled by RED algorithm. By default RED is enabled on traffic classes. Either RED or DSWRED can be enabled at a time.

Peak Rate Limiting for Parent Class

As explained earlier, CBQ service parameters are configured for leaf-classes because they define the traffic flows. Parent classes are an intermediate step in the MF classification process and primarily aid in MF classification.

However, we will support the configuration of the CBQ Peak Rate (PR) for parent classes. This sets a collective rate-limit for all the child-classes in that sub-tree. This feature gives the capability to rate-limit a collection of flows. PR can be configured for any intermediate class. Its value cannot exceed the PR of the given class' parent class.

Output Queue Congestion Management

When the link bandwidth is not enough for egress traffic on an interface, queues can build up and result in increased buffer consumption. Buffer management is needed to ensure optimum and fair usage of the limited number of buffers available in the system. It is needed at two levels. It is needed at the interface level to ensure that one interface does not consume too many buffers and affect the traffic on other interfaces. Buffer management is also needed for traffic classes on an interface to ensure that the classes have an optimum share of the interface's buffers to meet their service commitments.

It is important to realize that we will not create separate buffer pools for each interface or class. Instead we will define 'logical' buffer pools for each interface and class which is nothing but a maximum limit which indicates the number of buffers that the interface or class can use. The sum of these limits, plus the limits for other uses, cannot exceed the total number of buffers available.

Following is an explanation of variables/terms used in the following subsections.

- BCR - 'Committed rate bytes'. Root-out class parameter. Number of bytes that can be sent from an interface in one scheduler interval. This depends on the bandwidth of the interface.
- CR - 'committed rate bytes'. Class parameter. Number of bytes that can be sent from the class in one scheduler interval. This is configured by the user.
- bcr - 'committed rate bytes'. Class parameter. It is the number of bytes that a class can send in one scheduler interval, corresponding to its CR.
- BR - 'Burst rate bytes'. Class parameter. Maximum number of bytes that can be sent from an interface in one scheduler interval. This is configured by the user.
- bbr - 'Burst rate bytes'. Class parameter. This is the number of bytes a class can send in one scheduler interval, corresponding to its BR.

Buffer Reservation for Interfaces

When a wan interface is created, a certain amount of queue buffers will be reserved for its transmitting queue from the global buffer pool. Buffer reservation is only done for wan interfaces and not GE interfaces because we expect congestion and hence queue build-ups only on wan interfaces. The number of buffers reserved for a wan interface's queue is such that it provides 15 ms of buffering for 100 byte packets at a rate equal to the interface bandwidth. This amount of buffering is always guaranteed for a wan interface. A wan interface can use more than its reserved amount of buffers by borrowing queue buffers from the global pool if available. However, only the portion allocated for transmit queues can be borrowed. Therefore it is not possible for traffic, flooding a WAN interface, to consume all buffers and starve other interfaces (including Ethernet) of receive buffers. The calculation below shows how the number of reserved buffers is calculated for a WAN interface.

$$\text{MAX}((\text{NxBRCR\_BUFS\_RED} * \text{Bc})/\text{AVG\_PKTSIZE\_FOR\_BUF\_CALC}, 20) + \\ (\text{Bc}/\text{MIN\_PKTSIZE\_FOR\_BUF\_CALC})$$

Where,

The value of NxBRCR_BUFS_RED is 3,

The value of _PKTSIZE_FOR_BUF_CALC is 100 bytes,

Bc is interface bandwidth proportional to scheduling interval (5 ms),

The value of MIN_PKTSIZE_FOR_BUF_CALC 64 bytes.

The first part of expression gives 15 ms worth of packet buffering, and second part of expression gives extra buffers accounting for buffers which are not freed right away after completing transmission of packet from the driver queue.

Buffer Management for Class Queues

It is not possible for a class to guarantee bandwidth if it doesn't have enough buffers for its queue. Because the packets can be dropped even before they have a chance to be scheduled. Therefore it is essential to have a good buffer management scheme along with a good scheduling algorithm. This section discusses how buffers should be reserved for class queues of an interface. It may have to be modified slightly or considerably based on memory availability and the type of interfaces on which CBQ will need to be supported.

Buffer Requirements for Traffic Class

For a class to guarantee the CR, it should have capacity to buffer at least bcr bytes, since, in the worst case, the class would have to queue bcr bytes before the scheduler can service it. (Note that, to support a rate of CR kbps, at least bcr bytes need to be sent every scheduler interval). For the class to transmit at BR kbps, bbr bytes would have to be buffered. The BR of a class can be equal to a maximum of the interface's bandwidth, which means bbr can be a maximum of BCR (interface bandwidth). A class can transmit more than its CR and up to its BR if enough unused bandwidth is available. The scheduler offers unused bandwidth to higher priority classes before the lower priority ones.

For a class to, potentially, transmit up to its BR, it needs to have at least bbr bytes in its queue to be scheduled. Hence, ideally, all classes should have a buffering capacity of at least bbr bytes. If classes are created on a bundle with BR equal to the bundle bandwidth, the total buffer requirement for the bundle would be $(n \times BCR)$ bytes, where n is the number of classes. This requirement increases in direct proportion with the number of classes created, which can result in a huge total buffer requirement for the system. To better understand this buffer/memory requirement, let's take an example in which 20 classes are created on a bundle with two T1s with each class having a CR = (3072/20) Kbps and BR = 3072 Kbps.

$$BCR = ((3072000/8) * 5)/1000 = 1920 \text{ bytes-per-scheduling interval}$$

Total buffering requirement for a class = bbr = 1920 bytes

Let's estimate the average packet size to be 100 bytes. (This would be a very conservative estimate).

The minimum # of buffers required for one class = $bbr/100 = 20$ buffers

With 20 classes on the bundle, $(20 * 20) = 400$ buffers would be required for the bundle. With 14 bundles on a t3 interface, the total buffers requirement would be $(400 * 14) = 5600$ buffers! Each buffer occupies about 2000 bytes of memory, including all the control information, which results in a total memory requirement of $(5600 * 2000) = 11.2$ Mbytes! This is the minimum buffer requirement and does not provide any burst tolerance. Moreover, this memory requirement increases in direct proportion with the number of additional classes.

One would tend to think that having a shared pool of buffers with a capacity of BCR bytes is enough to transmit line rate of traffic. That will work only if the traffic entering each queue (classes) is proportional to its CR. This is mostly not the case and which is why we do bandwidth management. It is possible for traffic entering a class to be at a much higher rate than other classes, because of which it will gain access to majority of the buffers and hence most of the bandwidth.

Buffer Requirements Analysis and Buffer Management Scheme

A more economical scheme can be developed by making a calculated compromise on the buffer guarantee (availability) for a class. In most cases, not all classes would simultaneously need to transmit at their BR. Which means only a few classes, at any given time needs a buffering capacity of bbr bytes. If all classes are over subscribed and need more than their CR at the same time, then there is not going to be any unused bandwidth and so each class can send only bcr bytes in a scheduling interval. (The previous argument is based on the assumption that the class CRs sum up to the interface bandwidth). Based on the previous observations, a buffer management scheme has been devised which is a combination of a ‘shared buffer pool’ and ‘reserved buffer pools’ for each class. This provides each class with a minimum guarantee of buffers at all times (enough to support the CR) with the option to borrow additional buffers when needed from a common pool. This results in more efficient use of buffers by allowing sharing of a portion of the buffers which the classes don’t always need.

To start off with, we allocate $(10 * \text{BCR})$ bytes of buffering for the entire interface. This provides a decent amount of burst tolerance of $(9 * T_s = 45)$ ms. the allocation in terms of buffers would be $(10 * \text{BCR}/\text{average\_packet\_size})$, where $\text{average\_packet\_size} = 100$ bytes. Since the sum (bcr) of all classes makes up the BCR of the interface, each class will have an average of $(10 * \text{bcr}/\text{average\_packet\_size})$ buffers.

A class needs at least bcr bytes of buffering to support the CR and bbr bytes to support BR. We reserve $(6 * \text{bcr})$ bytes or $(6 * \text{bcr}/\text{average\_packet\_size})$ buffers, so that the class can not only support its CR but also has quite a few extra buffers that can provide burst tolerance or, support excess bandwidth up to 6 times the CR. However, we limit the amount of reserved buffers for a class to $(2 * \text{bbr}/\text{average\_packet\_size})$, because this amount is not only enough to support the BR but also provides a 100% burst tolerance at Burst Rate. If a class is configured with a very low CR, it is possible that $(6 * \text{bcr}/\text{average\_packet\_size})$ results in a very low value, for example, 2 buffers.

To handle this, we always reserve a minimum of $\text{QOS\_MIN\_RES\_CLASS\_Q\_SIZE}$ (which is 5 in the current code version) buffers.

The expression below summarizes the above logic for calculating the number of reserved buffers for a traffic class.

```
buffers1 = (2 * bbr)/average_packet_size; /* 2*bbr */
```

```
buffers2 = (4 * bcr)/average_packet_size; /* 4*bcr */
```

```
buffers3 = (6 * bcr)/average_packet_size; /* 6*bcr */
```

```
reserved_buffers_for_class = MAX(MIN(buffers3, MAX(buffers1, buffers2)),  
QOS_MIN_RES_CLASS_Q_SIZE);
```

Where, $\text{QOS\_MIN\_RES\_CLASS\_Q\_SIZE}$ is 5.

As explained above, a maximum of $(6 * \text{BCR}/\text{average\_packet\_size})$ buffers will be used up, in total, for the reserved buffer pools of all the classes on the interface. The remaining amount of $(4 * \text{BCR}/\text{average\_packet\_size})$ is used to create the shared buffer pool. On the other hand the minimum guaranteed number of reserved buffers is not less than $(4 * \text{BCR})$ for all classes on the interface. The remaining amount of $(6 * \text{BCR}/\text{average\_packet\_size})$ is used to create the shared buffer pool.

A single class by itself should not be allowed to borrow all of the available common pool buffers. So we need to enforce a maximum limit on the buffer consumption of each class. Since we have allocated $(10 * \text{BCR} / \text{average\_packet\_size})$ buffers for the entire interface, we should, at least, allow each class to use its fair share of $(10 * \text{bcr} / \text{average\_packet\_size})$ buffers (out of which $[6 * \text{bcr} / \text{average\_packet\_size}]$ have been reserved for it). However, the buffer allocation for a class should also take into consideration the Burst Rate (BR) configured for the class. If classes are configured with a very small CR but $\text{BR} = \text{interface bandwidth}$, the above amount of buffers might not be enough for the classes. Therefore, we allow a class to use up to a maximum of $(3 * \text{bbr} / \text{average\_packet\_size})$ buffers by borrowing from the common pool. In addition to supporting the BR, this will accommodate a burst of $(2 * \text{scheduler interval})$ 10 ms at a rate of BR kbps. (For packet sizes larger than average_packet_size bytes, the burst duration

will be even longer). In this case the maximum buffers that a traffic class can loan from the common pool is as shown below.

Max loaned buffers = $(3 * \text{bbr} / \text{average\_packet\_size}) - \text{reserved\_buffers}$

For a class with $\text{BR} = \text{interface BR}$ and $\text{CR} \sim 0$,

Max loaned buffers = $(3 * \text{BCR} / \text{average\_packet\_size}) - \text{QOS\_MIN\_RES\_CLASS\_Q\_SIZE}$

Max loaned buffers $\sim (3 * \text{BCR} / \text{average\_packet\_size})$

Note that a single class can still not consume all the buffers in the common buffer pool. There will be $(\text{BCR} / \text{average\_packet\_size})$ buffers still remaining for the other classes (which is enough to support a rate of up to the interface bandwidth).

The following sums up the maximum buffer limit calculation for a class.

$\text{max1} = (3 * \text{bbr}) / \text{average\_packet\_size};$

$\text{max2} = (10 * \text{bcr}) / \text{average\_packet\_size};$

Max Buffers = $\text{MAX}(\text{max1}, \text{max2}, \text{QOS\_MAX\_CLASS\_Q\_LIMIT\_MIN});$

Where, $\text{QOS\_MAX\_CLASS\_Q\_LIMIT\_MIN}$ is 10.

It is important to note that, the buffer requirement for traffic classes is $(10 * \text{BCR} / 100)$ buffers irrespective of the number of classes.

Congestion Management on Output Queues

In the iBG router, RED (Random Early Detect) will be used to do congestion avoidance on output queues. RED is the de facto standard for congestion management in the internet today. The basic philosophy of RED is to detect the onset of congestion and start dropping packets in a random fashion before queue overflow leads to tail drops. Random drops not only improves throughput of adaptive applications using TCP but is also more suitable than tail drops for voice and streaming audio/video. Random drops result in less perceptible degradation of voice/audio/video quality than consecutive drops.

The intent of RED detects persistent congestion but allow transient or momentary bursts. In that sense, it behaves like a low pass filter. RED therefore uses the 'average queue' size and not the 'current queue size' to determine congestion. The average queue size is calculated as an EWMA (Exponential Weighted Moving Average) of the current queue size.

Simply put, the average queue size is a 'smoothened-out' version of the instantaneous queue size.

The average queue size is compared against the 'minimum threshold' or 'minth' and 'maximum threshold' or 'maxth'. When the average queue size is less than minth, all packets are queued. When it is between minth and maxth, packets are dropped based on the calculated drop probability. This drop probability increases in direct proportion with the average queue size. When the average queue size equals or exceeds maxth, all packets are dropped. The intention here is to maintain the average queue size between minth and maxth.

The average queue size is calculated using the formula:

$$Q_{\text{average}} = (1 - w) * Q_{\text{average}} + w * Q_{\text{current}}$$

Where, w is the weighting factor. It is a very small quantity and is configured as a negative power of 2 for efficiency in calculation.

The drop probability when the average queue size equals 'maxth' is known as the Mark Probability. Mark Probability = 1/MPD, where MPD is the Mark Probability Denominator. MPD is configured as a power of 2 for efficiency in Average Queue Size Calculation

Average Queue Size Calculation for Interface Queues

The average queue size computation for interface is done for every packet sent on the interface. Before deciding whether packet needs to be dropped or not, the average queue size is calculated using the following formula and by reading the current driver queue size and current average queue size.

$$Q_{\text{average}} = (1 - \text{weight}) * Q_{\text{average}} + \text{weight} * Q_{\text{current}}$$

Where $\text{weight} = 1/2^{\text{ewf}}$, and ewf is configured by the user.

It seems obviously that above expression involves more computation. To get more efficiency from the implementation perspective the same formula is regrouped and calculated as show below. The weight is restricted to be a negative power of 2 so that a shift operation can be used instead of division to make the calculation more efficient.

$$Q_{\text{average}} = Q_{\text{average}} + (Q_{\text{current}} - Q_{\text{average}}) \ll \text{ewf}$$

This Q_{average} ‘average queue size’ is used as an indication of congestion by RED and is compared against the ‘minth’ and ‘maxth’ to decide whether packet need to be allowed, randomly dropped or dropped.

Average Queue Size Calculation for Traffic Classes

The average queue size calculation for traffic classes is little bit different than for interfaces. The packet scheduler services the class queues every scheduling interval T_s ms (5 ms). In a T_s ms interval, if the queues are serviced for T ms, during the remaining time ($T_s - T$) ms, the packets are classified and queued in to the respective queues. So, the queuing process runs for sometime followed by the de-queuing process in a periodic manner.

Therefore, even if the incoming rate for a particular queue is less than its CR, the queue builds up to N packets during the queuing phase and drops to 0 during the de-queuing phase. If the queue size is greater than 0 even after the de-queuing process has happened, it indicates that the receive rate is greater than the transmit rate for the queue which is what signals congestion.

Therefore, to get an accurate indication of congestion in the queue, we read the queue size after the queue is serviced but before en-queuing process, for every T_s ms. We call this the ‘pending queue size’. It is not very useful for RED to use the ‘pending queue size’ as it is because it can be very fluctuating. RED uses an Exponential Weighted Moving Average (EWMA) of this queue which, simply put, is a smoothed out version of the instantaneous values.

This average queue size is calculated every time the pending queue size is read. The average queue size computation and applicability is same as specified in above section.

Drop Probability Calculation

Instead of using drop probability, 'drop rate' is used to do random drop of packets. $\text{DropRate} = 1/(\text{DropProbability})$. There are two advantages for using drop rate. First, it results in a more uniform distribution of drops, which is more desirable. Secondly, it results in more efficient implementation. By using drop rate, we avoid making a function call for random number generation, for every packet.

The following expression shows how drop rate is calculated,

$$\text{Drop rate} = ((\text{maxTh} - \text{minTh})/2\text{mpd})/(\text{Qaverage} - \text{minTh})$$

Also the numerator in the above expression, which is fixed for a given configuration, $((\text{maxTh} - \text{minTh})/2\text{mpd})$, is pre-calculated at the time of initialization/configuration. This saves CPU time in the forwarding path.

The above drop rate procedure is same for both interfaces, and traffic classes.

SWRED

DSWRED allows specifying the separate set of RED parameters (only minth and maxth thresholds) for each DSCP value. The weight factor (ewf), and mark probability denominator (mpd) is same for all DSCP values. But the maxth and minth thresholds can be a different for each DSCP value.

As said earlier by default RED is enabled on traffic classes. At the queuing time, if DSWRED is not enabled then minth and maxth thresholds of given class is assumed for RED calculation otherwise the minth and maxth thresholds corresponding to the packet's DSCP value is assumed.

Configuring RED parameters

This section discusses which RED parameters are configurable and how are their default values set. It also explains the effect of changing these parameter values and guidelines about how to set their values.

interface RED parameters

The EWF parameter determines the weight factor in the calculation of the average queue size. The weight factor 'w' is calculated using the formula ($w = 1/(2^{ewf})$). The EWF parameter determines how RED is sensitive to traffic fluctuations or bursts. If EWF is very low, then the RED is very sensitive to traffic fluctuations and causes un-necessary early random packet drops and there by reducing network throughput. If EWF is very high, then the RED is not sensitive to traffic fluctuations and causes frequent tail drops which reduces the effectiveness of RED. Therefore it is important to strike a good balance in the value of EWF. The default value of ewf will be 5, which means the actual EWF value = $1/32$.

The MPD value determines the drop probability when the average queue size is close to maxth. A high value will result in more aggressive drops for a given increase in average queue size and could potentially lead to queue size oscillations. A low value will result in a milder drop response for a given increase in average queue size and increases the likelihood of tail drops.

Therefore it is important to select an optimum value. MPD is entered is entered as a power of 2 and has a default value of 5. This means the actual value of MPD = 32 and the Mark Probability = $1/32$.

The minth and maxth, are the configured minimum and maximum thresholds respectively, represents packet queue depth levels at which RED algorithm changes its course of action, i.e. no-drop, probabilistic-drop, and tail-drop, depending on whether the average queue size is below minth, in between minth and maxth, and at or above maxth respectively.

Mint_h is given a default value of N packets, where N corresponds to $\frac{1}{4}$ of maximum of $(3 * T_s)$ ms of buffering (at 100 byte packets) at a rate of interface bandwidth or 20. (For larger packets, this will result in larger amount of buffering). This means that, if a interface is receiving not more than it's bandwidth, on an average at least $\frac{1}{4}xT_s$ ms of traffic will be buffered before RED starts dropping. Note that these buffering requirements are calculated for 100 byte packets which are conservative. The average internet packet size is probably between 100-200 bytes, for which the buffering would be up to twice the amount mentioned above. The minimum permissible value for mint_h is L, where L corresponds to $\frac{1}{4}xT_s$ ms of buffering (for 100 byte packets) at rate of interface bandwidth or $L = 5$, whichever is lower.

Max_h is given a default value of N packets, where N corresponds to $\frac{3}{4}$ of maximum of $(3 * T_s)$ ms of buffering (at 100 byte packets) at a rate of interface bandwidth or 20. However it is recommended to set max_h to at least 2 times the mint_h. Too small a difference between mint_h and max_h will reduce the effectiveness of RED by causing frequent tail drops. The maximum permissible value for max_h is H, where H corresponds to $(3*T_s)$ ms of buffering (for 100 byte packets) at the rate interface bandwidth or 20, whichever is higher.

Class Queue RED parameters

The EWF and MPD parameters considerations are same as described in the section Interface RED parameters.

The mint_h and max_h, are the configured minimum and maximum thresholds respectively, represents packet queue depth levels at which RED algorithm changes its course of action, i.e. no-drop, probabilistic-drop, and tail-drop, depending on whether the average queue size is below minimum threshold, in between minimum and maximum thresholds, and at or above maximum threshold respectively.

Mint_h is given a default value of N packets, where N corresponds to $2xT_s$ ms of buffering, for 200 byte packets, at a rate of CR Kbps or T_s ms of buffering at BR Kbps or $N = 5$, whichever is greater. (For larger packets, this will result in larger amount of buffering). This means that, if a class is receiving not more than it's CR, on an average at least $(2*T_s)$ ms of traffic will be buffered before RED starts dropping. Note that these buffering requirements are calculated for 200 byte packets which are conservative.

The average internet packet size is probably between 200-300 bytes, for which the buffering would be up to twice the amount mentioned above.

The minimum permissible value for minth is L, where L corresponds to Ts ms of buffering (for 200 byte packets) at CR Kbps or $L = 3$, whichever is higher.

Maxth is given a default value of 3 times the minth. However it is recommended to set maxth to at least 2 times the minth. Too small a difference between minth and maxth will reduce the effectiveness of RED by causing frequent tail drops. The maximum permissible value for maxth is a value slightly less than the maximum queue buffers by worth of Ts ms of buffering at BR Kbps. The permissible range for minth and maxth values will be displayed in the CLI. Minth can never be greater than maxth.

Statistics

The following RED statistics will be collected for interface and class queue RED.

- Packets dropped above maxth
- packets dropped between minth-maxth
- packets allowed between minth-maxth
- Total RED drops
- Current average queue size
- Maximum recorded average queue size
- Maximum recorded queue size

Differentiated Services

The iBG router is fully compliant with the DiffServ Code Point specification. For more information refer to RFC 3290, RFC 3260, and RFC 2998.

Assured Forwarding (AF), Expedited Forwarding (EF), and Class Selector Code Points (CSCP)

In CBQ scheduling and shaping there is no implicit treatment given for DiffServ code points. You have full flexibility in assigning the required scheduling priorities through policy-class CBQ priority configuration. However in queuing, the WRED functionality uses color coding information extracted from DiffServ code point and is used as drop precedence. In the case of policing with color-aware mode, the initial color is extracted from the DiffServ code point. For the expedited traffic, the color code will be set as 'Green'.

For example, the following command sequence configures the proper treatment for AF11 (DSCP = 10) traffic.



NOTE

If DS-RED is configured for a given DSCP, then those RED parameters will be instead. Otherwise, color RED parameters will be used.

```
Router/configure# interface bundle wan1
configuring new WAN bundle interface wan1
/bundle wan1# link t1 1/1
Router/configure/interface/bundle wan1# encap ppp
Router/configure/interface/bundle wan1# ip address 23.1.1.1 24
Router/configure/interface/bundle wan1# qos
Router/configure/interface/bundle wan1/qos# add-policy-class
dscp-af11 root-out
Router/configure/interface/bundle wan1/qos# policy-class
dscpaf11
Router/configure/interface/bundle wan1/qos/policy-class
dscpaf11#
match-dscp 10
Router/configure/interface/bundle wan1/qos/policy-class
dscpaf11#
```

```

cbq cr 1500 pr 1500 priority 3
Router/configure/interface/bundle wan1/qos/policy-class
dscpaf11#red minth-red 10 minth-yellow 15 minth-green 20
maxredminth-red 10 minth-yellow 15 minth-green 20 maxth-red
16 maxthyellow24 maxth-green 25
Router/configure/interface/bundle wan1/qos/policy-class
dscpaf11#
Router/configure/interface/bundle wan1/qos/policy-class
dscpaf11#red minth 20 maxth 25 dscp 10
Router/configure/interface/bundle wan1/qos/policy-class
dscpaf11#

```

QoS Statistics

The following policy-class level statistics are supported in this release.

Traffic Statistics

```

-----
Avg Rate Out: 0 Kbps   Avg Pending Q: 0 pkts
Avg Rate In: 0 Kbps   Current Q: 0 pkts, 0 bytes
                      Current WRED Q: 0 pkts
                      Max recorded Q: 0 pkts, 0 bytes

```

Counters since last boot/clear: -- Packet drop details

```

Packets Forwarded: 0   Queue overflow: 0
Bytes Forwarded: 0     No buffers: 0
Packets Dropped: 0     Policing pkts dropped: 0
Bytes Dropped: 0       RED pkts dropped: 0

```

WRED Statistics:

Color	Pkts Fwd Below Minth	Pkts Fwd Minth-Maxth	Pkts Dropd Minth-Maxth	Pkts Dropd control Above Maxth	Pkts
green	0	0	0	0	0
yellow	0	0	0	0	0
red	0	0	0	0	0

Ingress and egress FR-QoS on FR PVCs

The QoS configuration for Frame Relay is same as for regular PPP bundles, except the QoS feature configuration using ‘enable <feature> <direction>’ command. This command is allowed at FR bundle level QoS context, and is not allowed FR PVC’s QoS context.

Ingress and egress QoS for IP tunnels

The QoS configuration for IP tunnels is the same as for regular PPP bundles except CBQ queuing and shaping feature. QoS for IP tunnels provides policing, and monitoring on both directions.

Hardware QoS

This section describes the QoS features implemented in hardware. In this release, QoS hardware features are provided by the Marvel chip set. Hardware-based traffic classification uses the following two look-up tables:

- Policy PCL profile table
- Policy Profile (default)

The policy PCL profile is an ordered list of rules in policy profile. Each rule is compared from start of the profile rule list to end of the profile rule list until one of the rule matches. So it is a sequential search. After matching rule is found, the matching process terminates and corresponding action is attempted. If IP flow classification look-up fails then policy profile default table is used.

For handling congestion on egress queues, the hardware supports three levels of drop precedence (DP). When congestion occurs on an egress queue, packets with higher DP can be configured to be dropped, while packets with low DP are enqueued.

CoS Attributes Marking

CoS attributed are a set of attributes associated with any packet processed by the Marvel sub-system. These attributes are the Traffic Class (TC), Drop Precedence (DP), User Priority (UP) and DSCP. They are primarily used to at different stages of the packet processing to decide the appropriate QoS treatment to be given to a packet. CoS attributes can be assigned to a packet by any of the multiple stages of the ingress pipeline.

L2 Bridge Based CoS Marking

The first stage that assigns CoS attributes is the Bridge processing stage.
To configure the bridge port TC assignment, enter:

```
Router/configure/interface/ethernet (3/0)/qos# [no]
override-outq <queue-id(1..8)>
```

Using the **no** form will switch off TC override. When TC override is 'off', the TC gets reassigned based on the UP of the packet in the next stage.

UP-based TC assignment uses the UP attribute of the packet (if tagged) to assign the TC attribute.

To configure the associated table, enter:

```
Router/configure/qos# [no] map-up-to-outq [<UP(0..7)>
<TC(1..8)>]
```

Using the **no** form will reset a specific row to default UP-based DP assignment uses the UP attribute of the packet to assign the DP attribute.

The associated table can be configured using the following command

```
Router/configure/qos# [no] map-up-to-dp [<UP(0..7)>
<DP(0..2)>]
```

Using the **no** form will reset a specific row to default TC-based UP assignment uses the TC attribute of the packet to assign the UP attribute, if the packet is untagged.

To configure the associated table, enter:

```
Router/configure/qos# [no] map-outq-to-up [<TC(1..8)>
<UP(0..2)>]
```

Using the **no** form will reset a specific row to default.

Configuration Example

```
Router/configure/qos# map-outq-to-up 4 3
Router/configure/qos# no map-outq-to-up 4
Router/configure/qos# map-up-to-dp 4 2
Router/configure/qos# no map-up-to-dp
Router/configure/qos# no map-up-to-dp 4
Router/configure/qos# map-up-to-outq 4 5
Router/configure/qos# no map-up-to-outq 4
```

Verifying the Configuration

Use the following command to display the configuration:

- show qos global-config

InLIF Based CoS Marking

The inLIF is a logical context assigned to a user port. InLIF-based CoS marking allows you to override the marking done at the bridge stage and assign CoS based purely on the ingress interface.

To configure the inLIF-based UP attribute assignment, enter:

```
Router/configure/interface/ethernet (3/0)/qos# mark-up  
<UP(0..7)>
```

To configure the inLIF-based DSCP attribute assignment, enter:

```
Router/configure/interface/ethernet (3/0)/qos# mark-dscp  
<DSCP (0..63)>
```

Configuration Example

```
Router/configure/interface/ethernet (3/0)/qos# mark-dscp 10  
Router/configure/interface/ethernet (3/0)/qos# no mark-dscp  
Router/configure/interface/ethernet (3/0)/qos# mark-up 3  
Router/configure/interface/ethernet (3/0)/qos# no mark-up  
Router/configure/interface/ethernet (3/0)/qos# override-outq 2  
Router/configure/interface/ethernet (3/0)/qos# no override-  
outq 2
```

Verifying the Configuration

Use the following command to verify the configuration:

- show qos port-info ethernet3/0

Policy Based CoS Marking

Policy-based CoS marking assigns CoS attributes based on traffic flows identified by match rules. Policy-based CoS marking can be achieved through the configuration of policies (rules and actions) and interface-to-policy mappings.

To create a policy map, enter:

```
Router/configure/qos# policy-map <map-name>
```

To create a policy class, enter:

```
Router/configure/qos/policy-map <map-name># policy-class  
<classname>
```

To create a policy rule, enter:

```
Router/configure/qos/policy-map <map-name>/policy-class  
<classname># match ipv4 src-ip 20.20.20.20
```

To configure CoS marking actions, enter:

```
Router/configure/qos/policy-map <map-name>/policy-class  
<classname># mark-dscp <DSCP(0..63)>  
Router/configure/qos/policy-map <map-name>/policy-class  
<classname># mark-up <UP(0..7)>  
Router/configure/qos/policy-map <map-name>/policy-class  
<classname># mark-outq <queue-id(1..8)>  
Router/configure/qos/policy-map <map-name>/policy-class  
<classname># mark-dp <DP(0..2)>
```

To map the policy created above to an interface, enter:

```
Router/configure/interface/ethernet (<name>)/qos# service-  
policyinput <map-name>
```

Configuration Example

```
Router/configure/qos# policy-map map2
Router/configure/qos/policy-map map2# policy-class class2
Router/configure/qos/policy-map map2/policy-class class2#
match ipv4
Router/configure/qos/policy-map map2/policy-class class2#
mark-dp 2
Router/configure/qos/policy-map map2/policy-class class2#
markdscp 3
Router/configure/qos/policy-map map2/policy-class class2#
markoutq 5
Router/configure/qos/policy-map map2/policy-class class2#
mark-up 3
Router/configure/interface/ethernet (3/0)/qos# service-
policyinput map2
```

Verifying the Configuration

Use the following commands to verify the configuration:

- show qos policy-map
- show qos policy-class

Policing-based CoS Marking, CoS Re-marking, and L2-based CoS Re-marking

Policing-based CoS marking allows the assignment of CoS attributes based on the traffic conformance level (metered against agreed rates). CoS assignment is done using two global tables namely L3 CoS marking table and L2 CoS marking table. The L2 CoS marking table is used for non-IP traffic and the indices into this table are UP and conformance level. The L3 CoS marking table is used for IP traffic and the indices into the table are DSCP and conformance level. Policing based CoS marking can be achieved using the following configuration

To create a policy map, enter:

```
Router/configure/qos# policy-map <map-name>
```

To create a policy class enter:

```
Router/configure/qos/policy-map <map-name># policy-class  
<classname>
```

To create a policy rule, enter:

```
Router/configure/qos/policy-map <map-name>/policy-class  
<classname># match ipv4 src-ip 20.20.20.20
```

To map this policy to an interface, enter:

```
Router/configure/interface/ethernet (<name>)/qos# service-  
policyinput <map-name>
```

To configure a policer for the class configured above, enter:

```
Router/configure/qos/policy-map <map-name>/policy-class  
<classname># police  
Router/configure/qos/policy-map <map-name>/policy-class  
<classname>/ police# srtcm <rate_in_kbps> cbs  
<committed_burst_in_bytes> ebs <excess_burst_in_bytes>
```

To configure the L3-based CoS marking table, enter:

```
Router/configure/qos# police
Router/configure/qos/police# l3-cos-map <DSCP(0..63)>
<conformance (green, yellow, red)> [mark-dscp <DSCP(0..63)>
markup <UP(0..7)> mark-dp <DP(0..2)>]
```

To configure the L2-based CoS marking table, enter:

```
Router/configure/qos# police
Router/configure/qos/police# l2-cos-map < UP(0..7)>
<conformance (green, yellow, red)> [mark-dscp <DSCP(0..63)>
mark-up <UP(0..7)> mark-dp <DP(0..2)>]
```

Configuration Example

```
Router/configure/qos/police# l2-cos-map 0 green mark-dscp 10
markdp 2 mark-up 5
Router/configure/qos/police# no l2-cos-map 0 green
Router/configure/qos/police# l3-cos-map 50 green mark-dscp 20
mark-dp 1 mark-up 4
Router/configure/qos/policy-map map1/policy-class
class1/police# srtcm 100 cbs 100 ebs 200
```

Verifying the Configuration

Use the following commands to verify the configuration:

- show qos policy-class
- show qos l2-cos-map
- show qos l3-cos-map
- show qos policer policy-name map1 policy-class class1

Multi-Field Classification using PCLs

Multi field classification allows the identification of flows using multiple fields in the packet. Rules based on multiple packet fields can be configured as follows:

To create a policy map, enter:

```
Router/configure/qos# policy-map <map-name>
```

To create a policy class, enter:

```
Router/configure/qos/policy-map <map-name># policy-class
<classname>
```

To create a policy rule, enter:

```
Router/configure/qos/policy-map <map-name>/policy-class
<classname>#
[no] match <packet-class> <match-field> [<match-operation>]
value1 [<match-operation>] [<value2>] ... [<match-field>]
[ [<match-operation>] value3 [<match-operation>] [<value4>] ]
< packet-class > can be "ipv4" or "ethernet" or "ipv6"
<match-field> can be "src-ip" or "dest-ip" or "ip-proto" or
"srcport"
or "dest-port" or "dscp" or "tos" or "precedence" or
"traffic-class" or "user-priority" or "vlan-id" or "packet-
class"
or "src-mac" or "dest-mac"
< match-operation > can be "=" (exact match on value) or "-"
(range between value1 and value2) or "!=" (exclude value) or
"/" (prefix length) or ">=" (greater than or equal to value)
or "<=" (less than or equal to value)
```

Configuration Example

```
Router/configure/qos/policy-map map1/policy-class class1#  
match  
ipv4 src-ip 20.30.30.30  
Router/configure/qos/policy-map map1/policy-class class1#  
match  
ipv4 dest-ip 30.40.50.0/24  
Router/configure/qos/policy-map map1/policy-class class1#  
match  
ipv6 src-ip 2002::/64  
Router/configure/qos/policy-map map1/policy-class class1#  
match  
ipv6 ip-proto 10-12  
Router/configure/qos/policy-map map1/policy-class class1#  
match  
ipv6 ip-proto !=10  
Router/configure/qos/policy-map map1/policy-class class1#  
match  
ipv4 ip-proto 17 src-port >=100  
Router/configure/qos/policy-map map1/policy-class class1#  
match  
ipv4 ip-proto 17 src-port <=200
```

Verifying the Configuration

Use the following commands to verify the configuration:

- show qos policy-class

Traffic Policing

Traffic policing allows metering of traffic flows, classification of flows based on conformance level and assigning CoS based on the above classification. Two flavors of markers are supported namely srTCM and trTCM. Policing can be configured using the following commands:

To create a policy class, enter:

```
Router/configure/qos/policy-map <map-name># policy-class  
<classname>
```

To create a policy rule, enter:

```
Router/configure/qos/policy-map <map-name>/policy-class  
<classname>#  
match ipv4 src-ip 20.20.20.20
```

To map the policy configured above to an interface, enter:

```
Router/configure/interface/ethernet (<name>)/qos# service-  
policyinput  
<map-name>
```

To configure an srTCM policer for the class configured above, enter:

```
Router/configure/qos/policy-map <map-name>/policy-class  
<classname># police  
Router/configure/qos/policy-map <map-name>/policy-class  
<classname>/  
police# srtcm <rate_in_kbps> cbs <committed_burst_in_bytes>  
ebs <excess_burst_in_bytes>
```

To configure a trTCM policer for the class configured above, enter:

```
Router/configure/qos/policy-map <map-name>/policy-class
<classname># police
Router/configure/qos/policy-map <map-name>/policy-class
<classname>#
police# trtcm <mean_rate_in_kbps> <peak_rate_in_kbps> cbs
<committed_burst_in_bytes> pbs <peak_burst_in_bytes>
```

Configuration Example

```
Router/configure/qos/policy-map map1/policy-class
class1/police#
srtcm 100 cbs 100 ebs 200
Router/configure/qos/policy-map map1/policy-class
class1/police#
no srtcm 100
Router/configure/qos/policy-map map1/policy-class
class1/police#
trtcm 100 200 cbs 200 pbs 300
Router/configure/qos/policy-map map1/policy-class
class1/police#
no trtcm 100 200
```

Verifying the Configuration

To verify the configuration, enter:

```
Router/configure/qos/policy-map map1# show qos policer
policy-name map1 policy-class class1
```

Billing & Conformance Counters

Billing counters are used to track the amount of data that is admitted into the router. Conformance counters are used to track the amount of data classified into specific meter conformance levels.

Billing and Conformance counters can be configured using the commands given below:

To enable or disable billing at the global level, enter:

```
Router/configure/qos#[no] billing enable
```

To enable for disable billing at the class level, enter:

```
Router/configure/qos/policy-map <map-name>/policy-class  
<classname>/police#  
[no] billing enable
```

To enable or disable conformance counters at the global level, enter:

```
Router/configure/qos#[no] conformance-counter enable
```

Configuration Example

```
Router/configure/qos# billing enable  
Router/configure/qos# no billing enable  
Router/configure/qos# conformance-counter enable  
Router/configure/qos# no conformance-counter enable  
Router/configure/qos/policy-map map1/policy-class  
class1/police#  
billing enable  
Router/configure/qos/policy-map map1/policy-class  
class1/police#  
no billing enable
```

Verifying the Configuration

To verify the configuration, enter:

```
Router/configure/qos# show qos global-config
Router/configure/qos/policy-map map1# show qos policer
policy-name
map1 policy-class class1
```

Egress Queuing, Scheduling and Shaping

Two queuing disciplines are supported namely Strict Priority Queuing and Weighted Round Robin.

To configure the queuing discipline, enter:

```
Router/configure/interface/ethernet (3/0)/qos# queue-
discipline 1
Router/configure/interface/ethernet (3/0)/qos/queue-
discipline 1#
spq
Router/configure/interface/ethernet (3/0)/qos/queue-
discipline 1#
Router/configure/interface/ethernet (3/0)/qos# queue-
discipline 2
Router/configure/interface/ethernet (3/0)/qos/queue-
discipline 2#
wrr 3
```

To configure port and queue shaping, enter:

```
Router/configure/interface/ethernet (3/0)/qos# port-shaping
token-bucket-size 8KB token-refill-rate-kbps 650
Router/configure/interface/ethernet (3/0)/qos/queue-
discipline 1#
queue-shaping token-bucket-size 8KB token-refill-rate-kbps 650
```

Verifying the Configuration

To verify the configuration, enter:

```
Router/configure/interface/ethernet (3/0)# show qos port-
info
ethernet3/0
Router/configure/interface/ethernet (3/0)# show qos queue-
info ifname
ethernet3/0
```

Congestion Management on Egress Queues

To configure RED and tail drop congestion management strategies, enter:

```
Router/configure/qos# qos-congestion-set 1
Router/configure/qos/qos-congestion-set 1# red 1 0 minTh 10
maxTh
20 mpd 2
Router/configure/qos/qos-congestion-set 1# red-ewma-wt 8 10
Router/configure/interface/ethernet (3/0)/qos# qos-
congestion-map
1
```

Verifying the Configuration

To verify the configuration, enter:

```
Router/configure/interface/ethernet (3/0)# show qos port-
info
ethernet3/0
Router/configure/interface/ethernet (3/0)# show qos
congestion-set
1
```


Buffer Management

To configure buffer management and flow control, enter:

```
Router/configure/interface/ethernet (3/0)/qos# rx-buffers-  
limit  
2000  
Router/configure/interface/ethernet (3/0)/qos# tx-  
descriptorlimit  
3000  
Router/configure/interface/ethernet (3/0)/qos# xoff-  
threshold 500  
Router/configure/interface/ethernet (3/0)/qos# xon-threshold 200  
Router/configure/interface/ethernet (3/0)/qos# queue-tx-  
descrlimit  
1 2000
```

Verifying the Configuration

To verify the configuration, enter:

```
Router/configure/interface/ethernet (3/0)# show qos port-  
info ethernet3/0  
Router/configure/interface/ethernet (3/0)# show qos queue-  
info ifname ethernet3/0
```



This page is intentionally left blank.

PART IV. Security



CHAPTER 1. Authentication Authorization Accounting

CHAPTER 2. Packet Filtering

CHAPTER 3. Firewall NAT

CHAPTER 4. GRE

CHAPTER 5. IPSEC

CHAPTER 6. SSL VPN Configuration

CHAPTER 7. Management



CHAPTER 1. Authentication Authorization Accounting

The combination of accounting controls, authorization requirements, and authentication checks (AAA) is a framework for configuring security functions across the network in a consistent fashion. Each component of AAA can be implemented separately.

Authentication

Authentication is the process of determining that you are who you say you are. Typical methods of determining user identities are thorough login and password responses, encryption, and the like. AAA authentication defines the authentication methods, and then applies these methods to each interface. By default, there is a method list that is automatically applied to all interfaces. When you define a method list, it overrides this default method list.

Authorization

AAA Authorization controls remote access by defining the methods used to authorize user activities on the network. In other words, authorization is the process of determining what you are allowed to do. Authorization manages a set of attributes describing what each user is allowed to do when they access the network. This set of attributes is typically stored in a database for each user, and when a user requests access, AAA authorization looks up what this user is allowed to do and grants the appropriate access privileges.

The authorization database can be located on the router, on an access server, or remotely hosted. Remote Authentication Dial-In User Service (RADIUS) and Terminal Access Controller Access Control System+ (TACACS+) servers are typical of remotely hosted authorization database servers. iBG router only supports TACACS+. TACACS is not supported.

**NOTE**

RADIUS does not have a separate Authorization function

Accounting

Accounting defines how to collect and distribute information about the security server. The iBG router sends this information to the AAA server. This information is then used for billing users for time online, auditing who was connected, and reporting what commands were executed, and the like. Accounting lets you know what services and network resources your uses are consuming. Accounting records consist of accounting attribute-value pairs and is typically stored on the access control server.

Configuration Examples

This section describes basic AAA configurations. It shows how to enable AAA, configure RADIUS and TACACS+ clients with related parameter settings such as authentication list.

Enabling AAA

The following example shows how to enable AAA module.

```
Router# configure terminal
Router/configure# aaa
Router/configure/aaa# enable
Router/configure/aaa# show aaa status
```

The command 'show aaa status' shows whether it is enabled.

The following example shows the way to disable AAA module.

```
Router/configure/aaa# no enable
```

Configuring Authentication

The Ubigate system is configured to authenticate users on a port basis. For example, if you want to configure a port of Ethernet 2/3 with a RADIUS authentication method, you may follow the example shown below.

```
Router# configure terminal
Router/configure# aaa
Router/configure/aaa# authentication login list1
radius/local/none
Router/configure/aaa# authentication protocols list1
pap/ascii
Router/configure/aaa# exit
Router/configure# interface ethernet 2/3
Router/configure/interface/ethernet(2/3)# aaa authentication
list1 list1
Router/configure/interface/ethernet(2/3)# end
Router# show aaa interface ethernet 2/3
```

To apply a authentication method to all ports, you may use '*default*' list shown in the following example.

```
Router# configure terminal
Router/configure# aaa
Router/configure/aaa# authentication login default
radius/local/none
Router/configure/aaa# authentication protocols default
pap/ascii
Router/configure/aaa# exit
```

Configuring RADIUS

```
Router# configure terminal
Router/configure# aaa
Router/configure/aaa# radius
Router/configure/aaa/radius# primary_server 172.168.2.1
Router/configure/aaa/radius/primary_server# shared_key
45J1T4n
Router/configure/aaa/radius# secondary_server 192.168.2.1
Router/configure/aaa/radius/secondary_server# exit
```

You can also configure the accounting port (default 1813), authentication port (default 1812), the number of retries (default 3 times), and the time out (default 8 seconds) to use other than the default values. For example, to configure the accounting port to be 1580, the authentication port to be 1670, the number of retries to be 4, and the time out to be 20 seconds, enter:

```
Router/configure/aaa/radius# acct_port 1580
Router/configure/aaa/radius# auth_port 1670
Router/configure/aaa/radius# retries 4
Router/configure/aaa/radius# time_out 20
Router/configure/aaa/radius# exit
Router/configure/aaa# exit
```

Verifying RADIUS Configuration

To verify the RADIUS configuration, enter

```
Router# show aaa radius
RADIUS CLIENT CONFIGURATION
-----

Source address           : 10.10.1.41
Primary server           : 172.168.2.1
Secondary server         : 192.168.2.1
Authentication port      : 1670
Accounting port          : 1580
Shared secret            : 45J1T4n
Timeout in seconds       : 20
Maximum retries          : 4
```

Configuring TACACS

```
Router# configure terminal
Router/configure# aaa
Router/configure/aaa# enable
Router/configure/aaa# authentication login list1
tacacs/local/none
Router/configure/aaa# authentication protocols list1
ascii/pap
Router/configure/aaa# tacacs primary_server 192.168.203.213
```



```
Router/configure/aaa# tacacs secondary_server
192.170.200.211
Router/configure/aaa# tacacs shared_key key123
Router/configure/aaa# tacacs retries 5
Router/configure/aaa# tacacs time_out 5
```

Verifying TACACS Configuration

To confirm the access method, enter:

```
Router/configure/aaa# show aaa authentication login
```

List Name	Methods Order
default	NOT CONFIGURED
list1	tacacs local none

To confirm the protocols list, enter:

```
Router/configure/aaa# show aaa authentication protocols
```

Protocol List Name	Protocols Order
default	NOT CONFIGURED
list1	ascii pap

To confirm TACACS+ client configuration, enter:

```
Router/configure/aaa# show aaa tacacs
TACACS+ CLIENT CONFIGURATION
```

Primary server	: 192.168.203.213
Secondary server	: 192.170.200.211
Server port	: 49
Timeout in seconds	: 5
Maximum retries	: 5
Shared Key	: key123



This page is intentionally left blank.



CHAPTER 2. Packet Filtering

Ubigate iBG routers can be configured for MAC and IP traffic filtering capabilities. IP traffic filtering allows creation of rule sets that selectively block TCP/IP packets on a specified interface. Filters are applied independently to all interfaces: Ethernet, serial, or WAN, as well as independently to interface direction: IN (packets coming in to the Ubigate iBG router) or OUT (packets going out of the Ubigate iBG router).

IP packet filtering capability can be used to restrict access to the Ubigate iBG router from untrusted, external networks or from specific, internal networks. An example would be a filter that prohibits external users from establishing Telnet sessions to the Ubigate iBG router, and allows only specific internal users Telnet access to the system.

- At the end of every rule list is an implied ‘deny all traffic’ statement. Therefore, all packets not explicitly permitted by filtering rules, are denied. This effectively means that once you enter a ‘deny’ statement in your filter list, you are implicitly denying all packets from crossing the interface. Therefore, it is important that each filter list contain at least one ‘permit’ statement.
- The order in which you enter the filtering rules is important. As the Ubigate iBG router is evaluating each packet, the SNOS tests the packet against each rule statement sequentially. After a match is found, no more rule statements are checked. For example, if you create a rule statement that explicitly permits all traffic, all traffic is passed since no further rules are checked.
- The SNOS permits easy re-ordering of filter commands through **access-list insert** and **delete** commands.

MAC filtering is supported on inbound packets only. MAC filtering can be applied to:

- Source MAC and source mask addresses
- Destination MAC and destination mask addresses
- Ethernet type
- Class of Service (CoS)
- VLAN ID

Example: Blocking Telnet Access

Consider a Ubigate iBG router connected via a bundle 'WAN1' (wan IP address 200.1.1.1) to an ISP, with Ethernet 0/1 (IP address 222.199.19.3) connected to the internal network. The network administrator wants to completely block Telnet access to the Ubigate iBG router from all external networks as well as from all internal networks except 222.199.19.0/28. All other TCP/IP traffic, such as FTP, Ping, and HTTP, is to flow unrestricted through the Ubigate iBG router.

Step-by-Step Configuration

```
Router# configure term
Router/configure# ip access-list ip filtera
Router/configure/access-list ip filtera# add deny tcp any
200.1.1.1 dport =23
Router/configure/access-list ip filtera# add permit tcp
222.199.19.0/28 222.199.19.3 dport =23
Router/configure/access-list ip filtera # add deny tcp any
222.199.19.3 dport=23
Router/configure//access-list ip filtera # add permit ip any
any
Router/configure/access-list ip filtera # end
Router# save local
```



CHAPTER 3. Firewall NAT

Overview

Security module in Ubigate iBG router consists of various components such as stateful inspection firewall, IPSec VPN, Public Key Infrastructure and Access Control List (ACL). This chapter introduces Ubigate iBG router's firewall and its typical configuration.

The Ubigate iBG router has Smart Forwarder as a dataplane forwarding engine. So, the forwarding of packets in security module is performed in the context of Smart Forwarder task. The components of security module may have control plane such as IKE (Internet Key Exchange) for VPN, SCEP for certificate enrollment in PKI, etc. These control plane activities are performed in the context of separate tasks such as IKES, SCEP, etc.

Whenever an IP packet in transit gets to Smart Forwarder, it checks whether the interface on which the packet arrived is registered for security processing or not. If registered, it is processed for security. Otherwise, it is put through regular IP forwarding. Similarly, whenever a packet gets to the Smart Forwarder from the local TCP/IP stack, it is checked if the outbound interface is registered with security and if so, it is processed for security.

The firewall in security module is a stateful inspection firewall for IPv4. In this, packets are allowed or denied to be forwarded through the system based on pre-defined policies. When a packet is allowed by the firewall policy, in real time, an association with limited lifetime is created for the packet with the combination of various fields in the packet such as Source IP, Source port, Destination IP, Destination port, Protocol, etc. Based on the protocol type, the association maintains a state or pseudo-state.

Firewall also offers a rich set of features such as protection against DOS (Denial Of Service) attacks, Network Address Translation (NAT), etc.

Firewall policies are created by CLI/GUI and stored in the Firewall Policy Data Base and dynamically created associations are stored in the Association Data Base.

Firewall and VPN are tightly coupled together. Some of the dynamic associations created are shared by the two modules. So, it is not possible to use VPN without using firewall. However, firewall can be used without VPN enabled-VPN in pass-through mode.

Virtual Firewall

Virtual Firewalls completely break the one-device/one-policy-database constraint. Instead, many discrete firewalls can be run on a single device with the Virtual Firewall capability. A Virtual Firewall (VF) provides multiple logical firewalls for multiple networks, on one system.

This is accomplished by establishing firewall ‘maps’, with each map having its own user defined security policy. Each map has its own outbound and inbound policies and configuration objects. Maps can be added or removed to provide scalability with the growth of subscriber networks.

Virtual firewall feature can be used to provide separate firewall policies as shown in the following diagram

- 1.** Internet for the untrusted network.
- 2.** Corporation(*corp*) for the corporate network.
- 3.** Demilitarized Zone(*dmz*) for the server accessibility from the untrusted side-or other user-defined network.
- 4.** Managing access to the box.

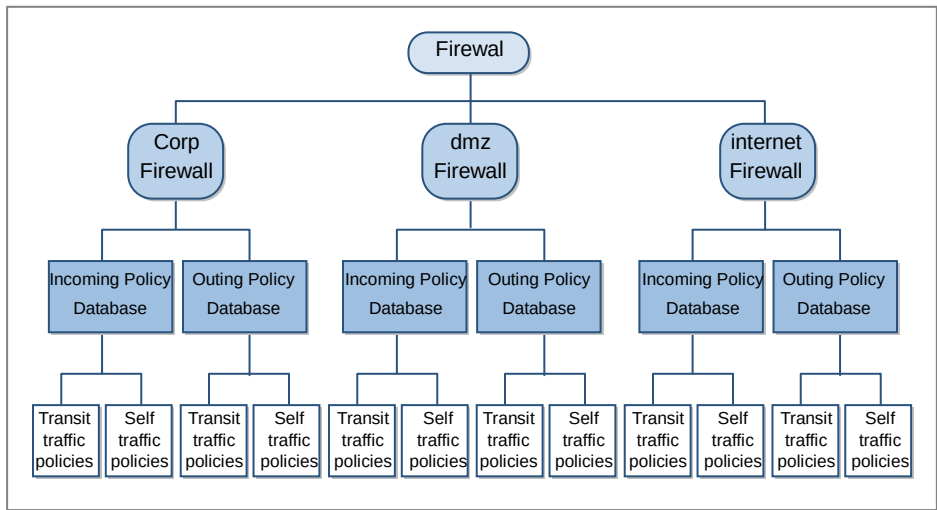


Figure 3.1 Virtual Firewall

For firewall to kick in, the IP interfaces need to be registered with security (maps/virtual firewall). It is necessary that at least one interface be registered for untrusted side (internet) and one for trusted side. Then, any interface in the router which can be a source/destination for traffic to/from the untrusted interface **MUST** be registered with security.

```

Router# configure terminal
Router/configure# firewall internet
Router/configure/firewall internet# interface ethernet0/2
Router/configure/firewall internet# exit
Router/configure# firewall corp
Router/configure/firewall corp# interface ethernet3/0
Router/configure/firewall corp# exit
Router/configure# firewall dmz
Router/configure/firewall dmz# interface ethernet0/4
Router/configure/firewall dmz# end
Router# show firewall interface all
  
```

Interface	Map Name
-----	-----
ethernet0/2	internet
ethernet0/4	dmz
ethernet3/0	corp

Typical Firewall Configuration (Three Legged Firewall Network)

A small firm has divided its corporate network into two security zones.

1. corp (private network of the firm)
2. dmz (web and mail servers exposed to internet)

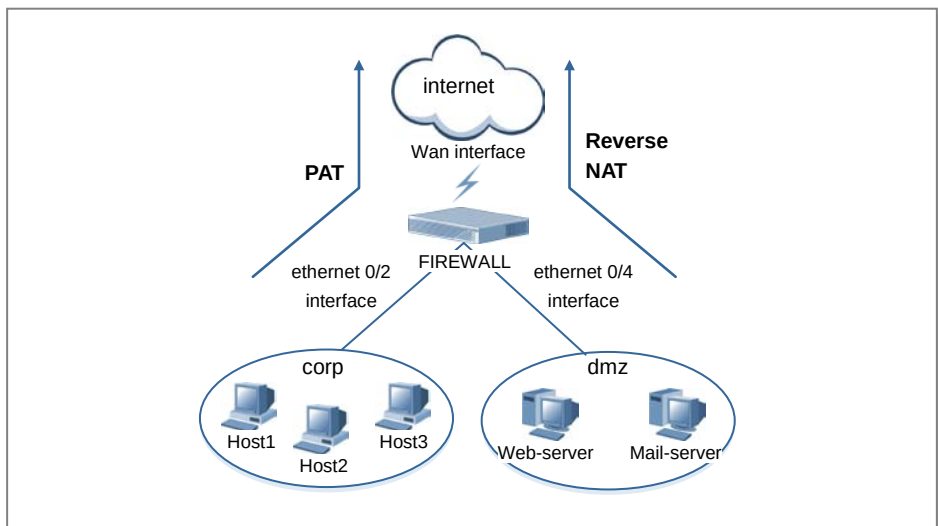


Figure 3.2 Three Legged Firewall Network

Access Policy Database

Access Policy Database is firewall's central database, commonly referred as policy database. This database makes use of all the other databases in firewall and enables in deciding whether a datagram needs to be allowed or denied and other actions associated to processing.

A policy is nothing but a rule that defines from host A to host B what action needs to be taken. Every time a new connection comes from host A to host B, this policy will be referred and the corresponding action will be taken.

This policy is available on network basis and within that direction. Currently supported policy categories are

- Outbound: Policies that govern traffic originated from one map to the external world.
- Inbound-Policies that govern traffic bound to map from the external world.

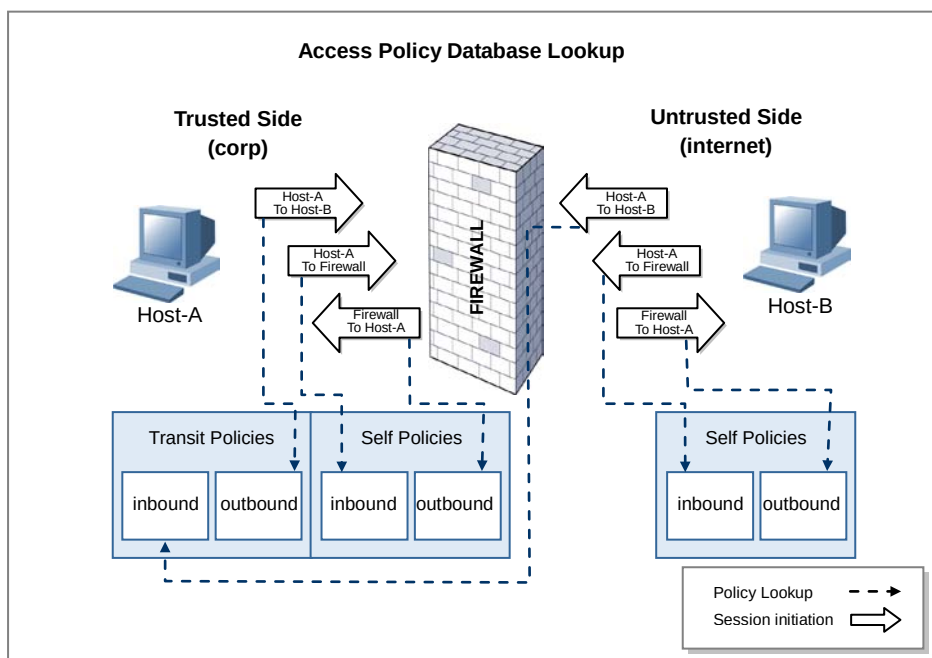


Figure 3.3 Access policy database lookup

For packets coming from untrusted to trusted side, firewall looks for a transit inbound firewall policy in the trusted map. For packets coming from trusted to untrusted side, firewall looks for a transit outbound firewall policy in the trusted map. If the packet is originated from the firewall, then the firewall looks for a self outbound firewall policy on the packet destined map. For self packets going towards internet, firewall looks for the outbound self policies on internet map. If the packet is destined to the firewall, then the firewall looks for a self inbound firewall policy on the packet originated map. For self packets going coming from internet, firewall looks for the inbound self policies on internet map.

Application Level Gateways

For packets to pass through firewall a corresponding allow policy will be required. If there is no policy, then the packet will be dropped by firewall. But some applications (for ex: FTP, games) open connections dynamically based on respective application parameter. It is a security threat to add firewall rules to pre-open such port numbers. Intelligence can be added to parse packets for such application and open appropriate dynamic connections. This is referred as Application Level Gateway (ALG), wherein the firewall, acting at routing level can parse application's data. With this, firewall can allow packets for many applications (that require some special processing) and at the same time not compromising on firewall.

All the ALGs are enabled by default and there are CLI commands to enable or disable ALGs administratively.

Network Address Translation

NAT functionality in firewall conceals network addresses avoiding this disclosure as public information. This functionality also provides solutions for IP address depletion issue, by allowing multiple hosts to share limited public IP addresses. Firewall has reverse NAT capabilities, which enables users to host various Internet services in the private IP address space, such as web servers, e-mail servers, Real Audio servers, and others.

Firewall has an inbuilt functionality for providing Network Address Translation. Firewall supports configuration of NAT records, by which NAT IP addresses can be configured before attaching them to policies. NAT database maintains a list of such NAT IP addresses and it can be eventually attached to access policies.

There are the 3 types of NAT that can be configured with the NAT database: many-to-one (PAT), one-to-one (static) and many-to-many (dynamic).

The NAT records created in the NAT databases would eventually be attached to the access policy database, based on the access policy type (whether it is out bound or in bound). The NAT record would eventually be used in one of the following category.

- Many-to-one regular NAT (NAT record attached to out bound policy)
- One-to-one regular NAT (NAT record attached to out bound policy)
- Many-to-one reverse NAT (NAT record attached to in bound policy)
- One-to-one reverse NAT (NAT record attached to in bound policy)
- Many-to-many regular NAT (NAT record attached to out bound Policy)

Multiple policies can share single NAT address, provided NAT address is of type many to one only.

Public ip addresses belonging to each map are maintained in one table. A map cannot use public ip address assigned to another map.

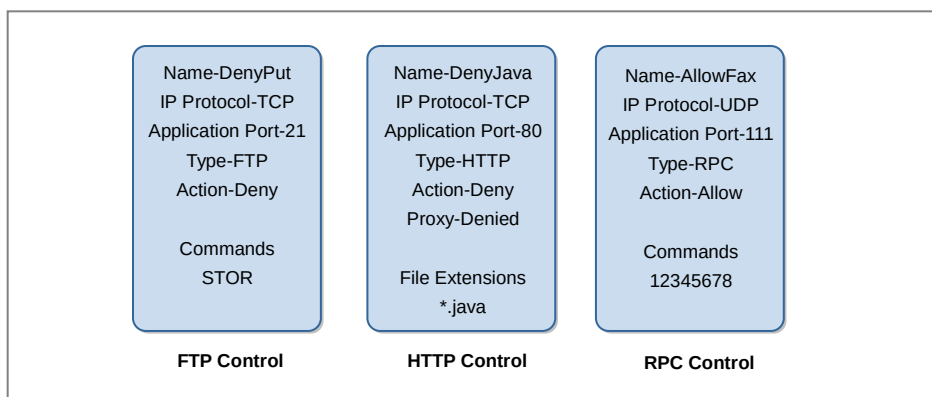
Application Content Filtering

Firewall supports command level filtering for certain well known applications. You can define application specific content filtering schemes by configuring application objects. Firewall can perform selective content filtering for SMTP, FTP, HTTP, and RPC Applications like disabling or enabling of individual commands of the application.

Firewall has the necessary intelligence to parse the contents of these applications and selectively filter out some commands. Some of these commands might reveal unwanted information. For this purpose, firewall maintains a database where such protocol commands can be configured and this database will eventually be used when the actual datagram travels in the network. This application control database maintains the above mentioned protocol commands.

Every application control in the application control database can represent for one of the above-mentioned applications. Each application control contains the application protocol information such as, the IP protocol, the transport protocol.

Along with this it maintains a set of application commands. These application commands can depend on the protocol it represents. In case of SMTP & FTP they are simple English commands, in case of RPC they are program numbers and in case of HTTP it is file extensions. Along with this command, application control also maintains the action that needs to be applied. The actions are either ALLOW or DENY. This application control can be attached to an access policy to enable application command filtering.



Configuring Firewalls

- Typical topology diagram
- Describe firewall configuration about firewall policy, dos-protect, filter, and port-trigger, etc.
 - Network Address Translation (NAT) serves two purposes:
- Allow LAN administrators to create secure, private, non-routable IP networks behind firewalls
- Stretch the number of available IP addresses by allowing LANs to use one public (real) IP address as the gateway with a very large pool of NAT addresses behind it.

In the most common NAT application (which is to provide secure networking behind a firewall), the device (Ubigate iBG router) that connects the user LAN to the Internet will have two IP addresses:

- A private IP address on the LAN side for the RFC 1918 address range
- A public address, routable over the Internet, on the WAN side

Consider a PC on the LAN sending a packet destined for *some.server.com*. The source IP address and port are in the packet together with the destination IP address and port. When the packet arrives at the Ubigate iBG router it will be de-encapsulated, modified, and re-encapsulated.

The re-encapsulated packet sent by the Ubigate iBG router destined for the Internet contains the Ubigate iBG router's public IP address, a source port allocated from its list of available ports, and the same destination IP address and port number generated by the PC.

The Ubigate iBG router also adds an entry into a table it keeps, which maps the internal address and source port number that the PC generated against the port number it allocated to this session. Therefore, when *some.server.com* sends a reply packet to the PC, the Ubigate iBG router can quickly determine how it needs to re-write the packet before transmitting it back on to the LAN.

Dynamic NAT is used when packets destined for the Internet are transported from a LAN using the public source IP address assigned to the local router. Dynamic NAT performs this task well, but it does not permit providing services to the Internet from inside a LAN which requires the use of static NAT. Static NAT also requires a public address from the upstream service provider. Individual PCs within a LAN are assigned RFC 1918 reserved IP addresses to enable access to other PCs within the LAN. The Ubigate iBG router is configured with static mapping, which maps the internal RFC 1918 IP addresses for each PC to the appropriate public IP address. When traffic is sent to the public address listed in the static mapping, the Ubigate iBG router forwards the packets to the correct PC within the LAN, according to the mapping relationship established.

NAT configuration Examples

Dynamic NAT (many to many)

In dynamic (many-to-many) NAT type, multiple sources IP addresses in the corporate network will be mapped to multiple NAT IP addresses (not necessarily of equal number). For a set of local IP address from 10.1.1.1 to 10.1.1.4 there will be a set of NAT IP address from 60.1.1.1 to 60.1.1.2. In case of many-to-many NAT, only IP address translation takes place, i.e., if a packet travels from 10.1.1.1 to yahoo.com, Firewall only substitutes the source address in the IP header with one of the NAT IP address and the source port will be the same as the original. If traffic emanates from the same client to any other server, the same NAT IP address is assigned. The advantage is that the NAT IP addresses are utilized in a better and optimum manner dynamically.

If a NAT IP address cannot be allocated dynamically at the connection creation time, the packet would be dropped.

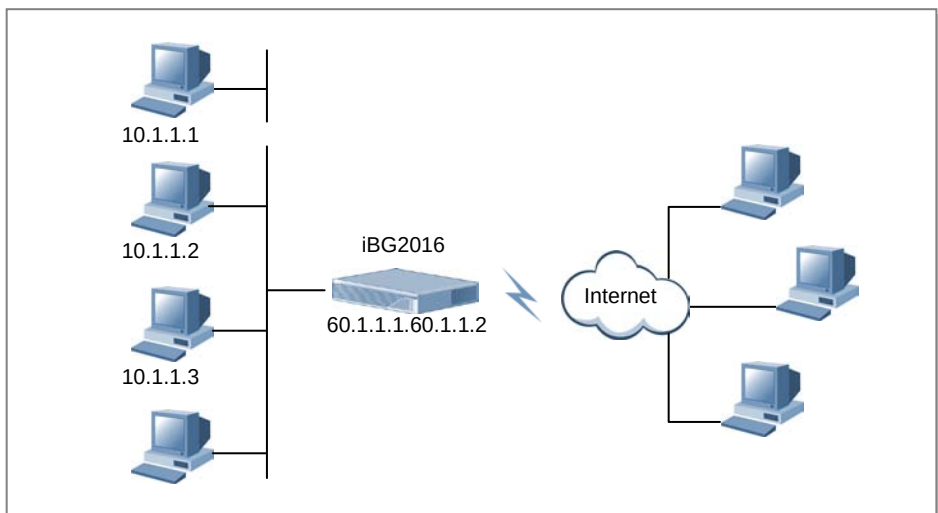


Figure 3.4 Dynamic NAT

The dynamic NAT configuration shown in Figure 3.4 includes:

- Private network addresses: 10.1.1.1-10.1.1.4
- Public (NAT) IP address range: 60.1.1.1-60.1.1.2

To create NAT pool with type **dynamic**, specify the IP address and the NAT ending IP address. Then add a policy with the source IP address range, and attach the NAT pool to the policy.

```
Router# configure terminal
Router/configure# firewall corp
Router/configure/firewall corp# object
Router/configure/firewall corp/object# nat-pool dynpool
dynamic 60.1.1.1 60.1.1.2
Router/configure/firewall corp/object# exit
Router/configure/firewall corp# policy 8 out address
10.1.1.1 10.1.1.4 any any
Router/configure/firewall corp/policy 8 out# apply-object
nat-pool dynPool1
Router/configure/firewall corp/policy 8 out# exit 2
Router/configure#
```

Port Address Translation (Many to one)

NAT allows multiple IP addresses to be mapped to one address.

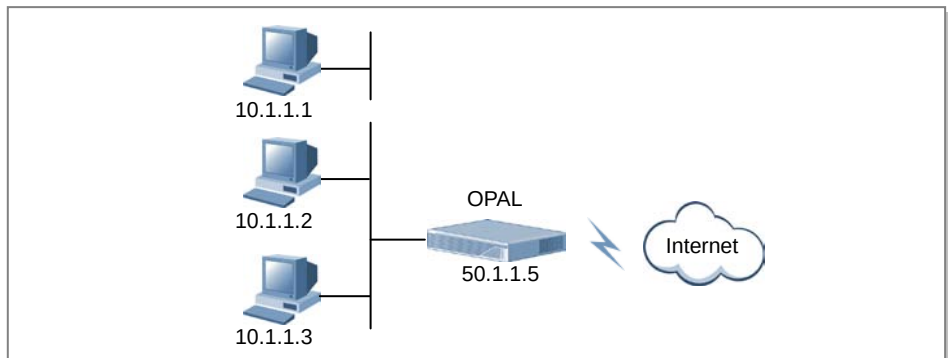


Figure 3.5 Mapping Multiple NAT Addresses to One Public IP Address

There are two methods to configure Port Address Translation (PAT) on the Ubigate iBG router. In the first method, specify the IP address to the nat-ip parameter in the policy command. In the second method, create a pool of type PAT and then attach it to the policy.

In PAT, multiple hosts can share the same IP address.

The PAT configuration shown in Figure 3.5 includes:

- Private network address: 10.1.1.1-10.1.1.3
- PAT address: 50.1.1.5

Method: 1-Specifying NAT address with the policy command

To configure this method of PAT, add the policy with the source IP address range, then specify the nat-ip address in the **policy** command.

```
Router/configure# firewall corp
Router/configure/firewall corp# policy 2 out address
10.1.1.1 10.1.1.3
any any nat-ip 50.1.1.5
Router/configure/firewall corp/policy 2 out# exit 2
Router/configure#
```

Method: 2-Attaching nat pool to the policy

To configure the second type of NAT, create a NAT pool with type pat and specify the IP address. Then add the policy with the source IP address range. Finally, attach the NAT pool to the policy.

```
Router/configure# firewall corp
Router/configure/firewall corp# object
Router/configure/firewall corp/object# nat-pool patPool pat
50.1.1.5
Router/configure/firewall corp/object# exit
Router/configure/firewall corp# policy 2 out address
10.1.1.1 10.1.1.3 any any
Router/configure/firewall corp/policy 2 out# apply-object
nat-pool patPool
Router/configure/firewall corp/policy 2 out# exit 2
Router/configure#
```

Static NAT (one to one)

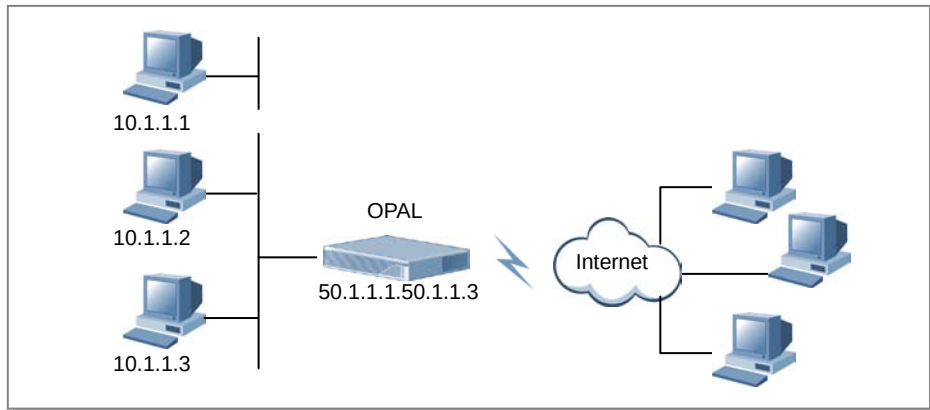


Figure 3.6 Static NAT

In static (one-to-one) NAT type, for each IP address in the corporate network, one NAT IP address will be used. For example, for the three IP addresses from 10.1.1.1 to 10.1.1.3, there is a set of three NAT IP address from 50.1.1.1 to 50.1.1.3. In case of one-to-one NAT, only IP address translation takes place, that is, if a packet travels from 10.1.1.1 to yahoo.com, the Firewall only substitutes the source address in the IP header with the NAT IP address. The source port will be the same as the original.

The static NAT configuration shown in Figure 3.6 includes:

- Private network address: 10.1.1.1-10.1.1.3
- Public (NAT) IP address range: 50.1.1.1-50.1.1.3

To create NAT pool with type **static**, specify the IP address and the ending NAT IP address. Add a policy with source IP address range and attach NAT pool to the policy.

```
Router/configure# firewall corp
Router/configure/firewall corp# object
Router/configure/firewall corp/object# nat-pool natStat
static 50.1.1.1 50.1.1.3
Router/configure/firewall corp/object# exit
Router/configure/firewall corp# policy 7 out address
10.1.1.1 10.1.1.3 any any
Router/configure/firewall corp/policy 7 out# apply-object
nat-pool natStat
Router/configure/firewall corp/policy 7 out# exit 2
Router/configure#
```

Static NAT also requires a public address from the upstream service provider. Individual PCs within a LAN are assigned RFC 1918 reserved IP addresses to enable access to other PCs within the LAN. The Ubigate iBG router is configured with static mapping, which maps the internal RFC 1918 IP addresses for each PC to the appropriate public IP address.

Then when traffic is sent to the public address listed in the static mapping, the Ubigate iBG router forwards the packets to the correct PC within the LAN, according to the mapping relationship established.

Figure 3.7 illustrates dynamic and static NAT. The static translation between 192.168.1.6 and 100.1.1.6 automatically matches the port addresses, thus a request destined for 100.1.1.6 tcp port 25 is translated to 192.168.1.6 tcp port 25 and so on.

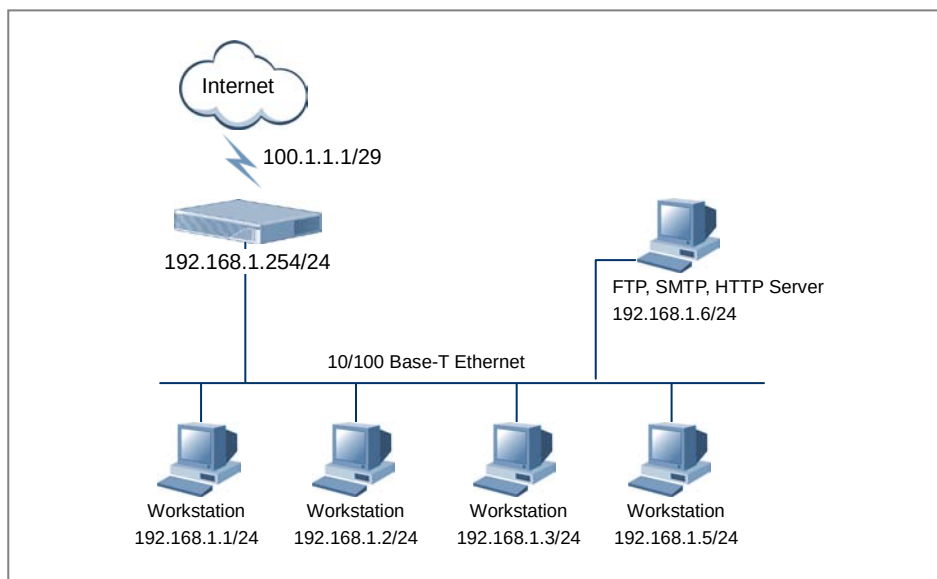


Figure 3.7 Dynamic and Static NAT

Configuration for Figure 23.7

```
Router# configure terminal
Router/configure# firewall corp
Router/configure/firewall corp# object
Router/configure/firewall corp/object# nat-pool staticNat
static 100.1.1.6 100.1.1.6
Router/configure/firewall corp/object# exit
Router/configure/firewall corp# policy 8 out address
192.168.1.6 32 any
Router/configure/firewall corp/policy 8 out# apply-object
nat-pool staticNat
Router/configure/firewall corp/policy 8 out# end
Router#
```

Figure 3.8 provides an example of static port mapping. TCP port 81 of the web server at private address 192.168.1.6 is mapped to the same TCP port of the public address.

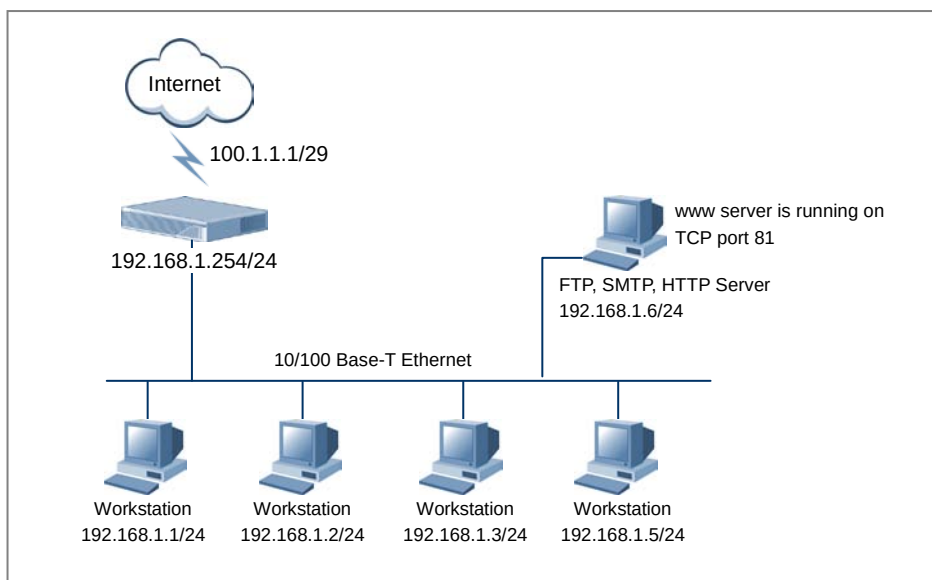


Figure 3.8 Mapping Ports

Configuration for Figure 23.8

```
Router# configure terminal
Router/configure# firewall corp
Router/configure/firewall corp# policy 8 out address
192.168.1.6 32 any protocol tcp port 81 any nat-ip 100.1.1.6
Router/configure/firewall corp# end
Router#
```

Reverse NAT

Reverse NAT could be used in a situation where one LAN is using private RFC 1918 IP addresses and a second LAN is using 'real' Internet routable IP addresses. Figure 3.9 illustrates how reverse NAT would be applied.

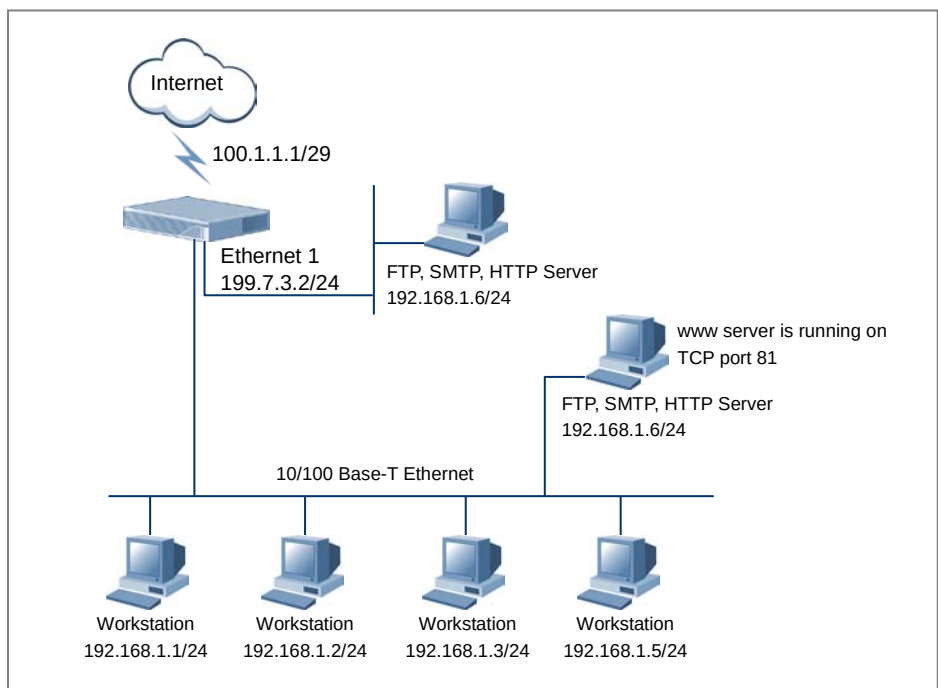


Figure 3.9 Reverse NAT

Configuration for Figure 23.9

```
Router# configure terminal
Router/configure# firewall corp
Router/configure/firewall corp# object
Router/configure/firewall corp/object# nat-pool revNat pat
192.168.1.6 192.168.1.6
Router/configure/firewall corp/object# exit
Router/configure/firewall corp# policy 9 in address any
100.1.1.6 32
Router/configure/firewall corp/policy 9 in# apply-object
nat-pool revNat
```

NAT-Failover for Firewalls

This feature enables failover from a primary interface (T1 wan bundle) to a backup interface (PPPoE or ISDN) when using Firewall-based Port Address Translation. This feature applies to firewall NAT policies which are configured with the interface name of the primary interface. The user must specify the primary and backup interface using the firewall global **nat-failover** command. When the primary interface is up, packets going out through it will be translated using the IP address of the primary interface. When it goes down, the IP address of the backup interface will be used and the stale firewall connections will be flushed. Without this feature, NAT translations will continue to use the IP address of the primary interface since firewall policies do not change when an interface goes up or down. Hence traffic will be blackholed.

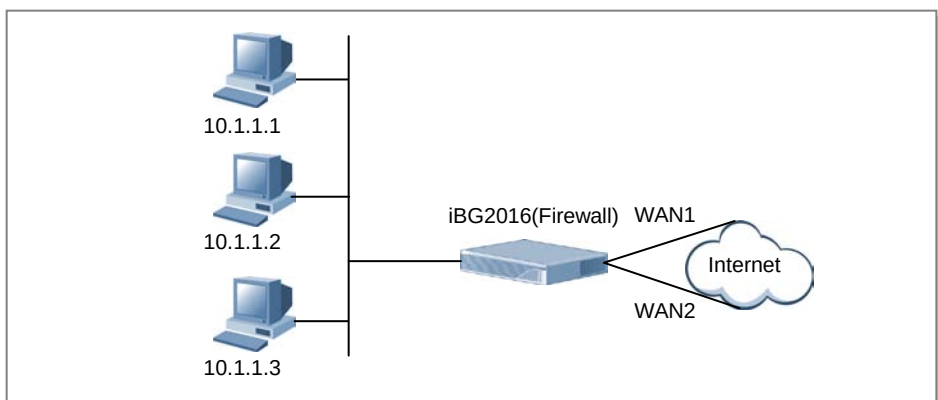


Figure 3.10 NAT-Failover for Firewalls



CHAPTER 4. GRE

Generic Routing Encapsulation (GRE) is a standards-based (RFC1701, RFC2784) tunneling protocol that can encapsulate a wide variety of protocol packet types inside IP tunnels, creating a virtual point-to-point link between routers at remote points over an IP network. A tunnel is a logical interface that provides a way to encapsulate passenger packets inside a transport protocol. Tunnels can be created using GRE (the default) or IPIP.

By connecting multiprotocol subnetworks in a single-protocol backbone environment, IP tunneling using GRE allows network expansion across a single-protocol backbone environment.

IPSec and GRE complement each other well, while IPSec provides a secure method of transporting data across the internet GRE provides the capability to transport routing protocols (for example: OSPF) that use broadcast and multicast.

GRE Configuration Examples

This example explains how to configure a basic GRE tunnel as shown in Figure 4.1.

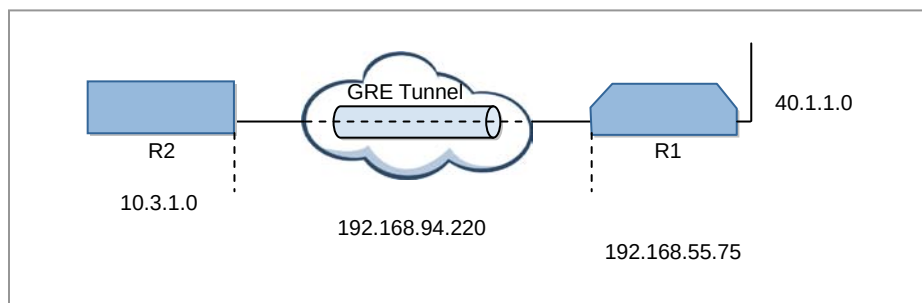


Figure 4.1 Simple GRE configuration

Configuring Site to Site Tunnel

To configure GRE in a site to site tunnel configuration:

1. Configure the interface.

```

Ubigate router# configure terminal
Router/configure# interface bundle wan1
Router/configure/interface/bundle wan1# link t1 0/2/0
Router/configure/interface/bundle wan1# encapsulation ppp
Router/configure/interface/bundle wan1# ip address
192.168.94.220 255.255.255.0
Router/configure/interface/bundle wan1# exit

```

2. Configure the tunnel.

```

Router/configure# interface tunnel t0
Router/configure/interface/tunnel t0# ip address 103.1.1.2 24
Router/configure/interface/tunnel t0# tunnel source
192.168.94.220
Router/configure/interface/tunnel t0# tunnel destination
192.168.55.75
Router/configure/interface/tunnel t0# exit

```


3. Configure the IP routes.

```
Router/configure# ip route 0.0.0.0 0.0.0.0 192.168.94.254
Router/configure# ip route 40.1.1.0 255.255.255.0 t0
```



The peer of a local WAN interface cannot be used as a tunnel destination.

4. Verify that the tunnel is up and running. (If it is not, check the Gateway and Source Address fields.)

```
Router# show ip interfaces
...
t0(unit number 5)
Type: TUNNEL
Flags:(0x74243) UP, RUNNING, MULTICAST-ROUTE
Internet Address: 103.1.1.2
Internet Netmask: 255.255.255.0
Internet Broadcast: 103.1.1.255
Maximum Transfer Unit: 1476 bytes
Source Address: 192.168.94.220
Destination Address: 192.168.55.75
Gateway: wan1
Protocol: GRE
Mac Address 00:50:52:60:00:00
...
```

For more information enter:

```
Router# show interface tunnel t0
Tunnel: t0                      Status: up
Internet Address: 103.1.1.2      Internet Netmask: 255.255.255.0
Source Address: 192.168.94.220
Destination Address: 192.168.55.75
MTU: 1476 bytes                 Protocol: GRE
ICMP unreachable: will be sent ICMP redirect: will be sent
Crypto type: not set            IPSEC/IKE: policy not set key not set
```

```

TTL: 30                      Keepalive: disabled
TOS: not set                  Path MTU discovery: disabled
Key Value: not set           Checksum: disabled
Sequence Datagrams: disabled
Tunnel Statistics:
    Bytes Rx                  0    Bytes Tx                  0
    Packets Rx                 0    Packets Tx                 0
    Err Packets Rx             0    Output Errs                0

```

5. Configure the Cisco-compatible router side:

```

cisco # config t
cisco(config)#interface Ethernet2/0
cisco(config-if)#ip address 192.168.55.75255.255.0
cisco(config-if)#exit

cisco(config)#interface Tunnel 0
cisco(config-if)#ip address 103.1.1.1 255.255.255.0
cisco(config-if)#tunnel source 192.168.55.75
cisco(config-if)#tunnel destination 192.168.94.220
cisco(config-if)#exit

cisco(config)#ip route 0.0.0.0 0.0.0.0 192.168.55.254
cisco(config)#ip route 10.3.1.0 255.255.255.0 Tunnel0

```

Configuring GRE Site to Site with IPSec

This example extends the first example by adding encryption to the tunnel.

1. Prepare the WAN link:

```

Router# configure terminal
Router/configure# interface bundle wan1
Router/configure/interface/bundle wan1# link t1 0/2/0
Router/configure/interface/bundle wan1# encapsulation ppp
Router/configure/interface/bundle wan1# ip address
192.168.94.220 255.255.255.0
Router/configure/interface/bundle wan1# crypto untrusted
Router/configure/interface/bundle wan1# exit

```

2. Configure the tunnel:

```
Router/configure# interface tunnel t0
Router/configure/interface/tunnel t0# ip address 103.1.1.2 24
Router/configure/interface/tunnel t0# tunnel source
192.168.94.220
Router/configure/interface/tunnel t0# tunnel destination
192.168.55.75
Router/configure/interface/tunnel t0# tunnel protection
greCisco secretkeyfortest
Router/configure/interface/tunnel t0# crypto untrusted
Router/configure/interface/tunnel t0# exit
```

3. Configure the routes:

```
Router/configure# ip route 0.0.0.0 0.0.0.0 192.168.94.254
Router/configure# ip route 40.1.1.0 255.255.255.0 t0
```

4. Define the policy:

```
Router/configure # firewall internet
Router/configure/firewall internet# policy 100 in proto gre
self
Router/configure/firewall internet/policy 100 in# exit
Router/configure/firewall internet# policy 101 in service
ike self
Router/configure/firewall internet/policy 101 in# exit 2
Router/configure# firewall corp
Router/configure/firewall corp# policy 100 in self
```

5. Check the status of the tunnel by entering:

```
Router# show interface tunnel t0
```

6. Validate the tunnel configuration by entering:

```
Router# show crypto ipsec policy all

Or enter:
Router# show crypto ike policy all
```

Configuring GRE Site to Site with IPSec and OSPF

This example extends the previous IPSec configuration example by enabling Open Shortest Path First (OSPF) protocol which provides redundant paths for the tunnel.

1. To enable OSPF, add to the Ubigate iBG router configuration above:

```
Router# configure terminal
Router/configure# router-id 2.2.2.2
Router/configure# router ospf
Router/configure/router/ospf# network 103.1.1.0/24 area 0
Router/configure/router/ospf# exit
```

2. Add to the Cisco-compatible configuration above:

```
cisco # config t
cisco(config)#router ospf 1
cisco(config-router)# network 103.1.1.0 0.0.0.255 area 0
```

3. To verify the OSPF configuration, enter:

```
Router# show ip ospf interface
```



NOTE

Using the redistribute connected command adds a recursive route to the tunnel destination. This will cause the tunnel to shut down. To prevent this, for example, add a 32-bit static route for the tunnel destination.



CHAPTER 5. IPSEC

Need to develop CLNS VPNs and Secure Packet Exchange topics-new material

Introduction to Security

SNOS introduces a wide range of robust industry-standard security features including:

- Virtual Private Networking
- IPSec encryption and tunneling
- Generalized Router Encryption
- Firewall with private network management (Network Address Translation and Port Address Translation)

This chapter explains each of these features in detail.

Securing Remote Access Using IPSec VPN

The features in SNOS allow administrators to form a security tunnel to join two private networks over the Internet. The following examples show how to set up an end-to-end tunnel with a single proposal and pre-shared key authentication, with multiple proposals and pre-shared key authentication, and with an SA Bundle, and pre-shared key authentication.

The corporate network no longer has a clearly defined perimeter inside secure building and locked equipment closets. Increasingly, companies have a need to provide remote access to their corporate resources for the employees on the move.

Traditionally, remote users could access the corporate LAN through dial-up and ISDN lines which were terminated in the corporate remote access servers. However, these point-to-point connection technologies do not scale well to the growing number of remote users and the corresponding increase in the infrastructure investments and maintenance costs.

A solution to meeting the needs of increasing numbers of remote users and for controlling access costs is to provide remote access through the Internet using firewalls and a Virtual Private Network (VPN). Internet Protocol Security (IPSec) keeps the connection safe from unauthorized users.

In a typical IPSec remote access scenario, the mobile user has connectivity to Internet and an IPSec VPN client loaded on their PC. The remote user connects to the Internet through their Internet service provider and then initiates a VPN connection to the IPSec security gateway (the VPN server) of the corporate office, which is typically an always-on Internet connection. One of the main limitations in providing remote access is the typical remote user connects with a dynamically assigned IP address provided by the ISP. IPSec uses the IP address of users as an index to apply the Internet Key Exchange (IKE) and IPSec policies to be used for negotiation with each peer. When the VPN client has a dynamic IP address, the VPN server cannot access the policies based on the IP address of the client. Instead, the VPN server uses the identity of the VPN client to access the policies.

Access Methods

Ubigate iBG router supports two types of IPSec remote access using VPNs.

Remote Access: User Group

One of the methods to achieve IPSec remote access in Ubigate iBG router is the user group method. In this method, the administrator creates an IKE policy for a logical group of users such as a department in an organization. Each user in the group is identified with unique information that is uniquely configured in the IKE policy. Also, an IPSec template is attached to the user group. Once the VPN user is authenticated using IKE, the users dynamically-assigned IP address is added to the destination address field in the IPSec template attached to the user group. The VPN user now has the required IPSec policy that allows access through the gateway to the corporate LAN.

Remote Access: Mode Configuration

The other method to achieve IPSec remote access in Ubigate iBG router is the mode configuration method.

This method makes the VPN client an extension of the LAN being accessed by the VPN client. The remote client appears as a network accessing some resource behind the VPN server.

The VPN client is allocated a private IP address by the VPN server and the client uses this as the source IP address in the inner IP header in tunnel mode. In tunnel mode, at each IKE end point, the IP traffic to be protected is completely encapsulated with another IP packet. In this, the inner IP header remains the same as seen in the original traffic to be protected. In the outer IP header, the source and destination addresses are the addresses of the tunnel end points.

Typically, for a remote user, the source address of the outer IP header is the dynamic public IP address provided by the ISP. When mode configuration is enabled, the source address of the inner IP header is the private address allocated by the VPN server to the VPN client.

As in the case of user group method, the administrator creates an IKE policy for a logical group of users such as a department in an organization. The identity information used to identify each user uniquely is configured in the IKE policy. The IKE policy is attached to a mode configuration record. The mode configuration record contains an IPSec policy template to be used for creating dynamic IPSec policy. Also, the record contains one or more pools of private IP addresses to be used for allocating the addresses to the VPN clients. Besides the private IP address, the VPN server can also provide WINS and DNS server addresses.

Upon successful IKE authentication of a VPN client, the server checks whether the IKE policy used to authenticate the VPN client is enabled for mode configuration. If so, the server allocates a private IP address from one of the IP pools in the mode configuration record to the VPN client. The destination address field in the IPSec template attached to the user group is filled in with the private IP address allocated to the VPN client and this is installed as an IPSec policy.

This guide provides information and examples on how to configure IPSec.

Securely Managing the Ubigate iBG Router Example

This example demonstrates how to manage a router through an IP security tunnel. Steps are presented for configuring the Router-1 and Router-2 routers to assist any host on the LAN side of Networks-2 to manage the Router-1 router through the IP security tunnel.

The security requirements are:

- Phase 1: 3DES with SHA1
- Phase 2: IPSec ESP with AES (128-bit) and HMAC-SHA1

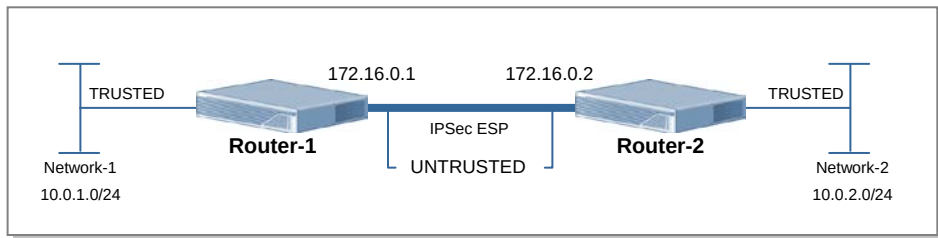


Figure 5.1 Tunnel Mode Between Two Security Gateways-Single Proposal

Router-1 Configuration

1. Configure a WAN bundle of network type untrusted.

```
Router-1/configure# interface bundle wan1
Router-1/configure/interface/bundle wan1# link t1 0/2/0
Router-1/configure/interface/bundle wan1# encapsulation ppp
Router-1/configure/interface/bundle wan1# ip address
172.16.0.1 24
Router-1/configure/interface/bundle wan1# crypto untrusted
Router-1/configure/interface/bundle wan1# exit
```

2. Configure the Ethernet interface with trusted network type.

```
Router-1/configure# interface ethernet 0/1
Router-1/configure interface/ethernet 0/1# ip address
10.0.1.1 24
Router-1/configure/interface/ethernet(0/1)# crypto trusted
Router-1/configure/interface/ethernet(0/1)# exit
```


3. Display the crypto interfaces.

```
Router-1# show crypto interfaces
Interface Network
Name Type
-----
ethernet 0/1 trusted
wan1 untrusted
```

4. Add the route to the peer LAN.

```
Router-1/configure# ip route 10.0.2.0 255.255.255.0 wan1
```

5. Configure IKE to the peer gateway.

```
Router-1/configure# crypto
Router-1/configure/crypto# ike policy NW2 172.16.0.2
Router-1/configure/crypto/ike/policy NW2 172.16.0.2# local-
address 172.16.0.1
Router-1/configure/crypto/ike/policy NW2 172.16.0.2# key
secretkey
Router-1/configure/crypto/ike/policy NW2 172.16.0.2#
proposal 1
Router-1/configure/crypto/ike/policy NW2 172.16.0.2/proposal
1# encryption-algorithm 3des-cbc
Router-1/configure/crypto/ike/policy NW2 172.16.0.2/proposal
1# exit
Router-1/configure/crypto/ike/policy NW2 172.16.0.2# exit
```

6. Display the IKE policies.

```
Router-1# show crypto ike policy all
Policy      Peer          Mode      Transform
-----
NW2 172.16.0.2 Main P1 pre-g1-3des-sha1
```

7. Display the IKE policies in detail.

```
Router-1# show crypto ike policy all detail

Policy name NW2, Local addr 172.16.0.1, Peer addr 172.16.0.2
Main mode, Response and Initiate, PFS is not enabled, Shared
Key is *****
Local ident 172.16.0.1(ip-address), Remote Ident
172.16.0.2(ip-address)

Proposal of priority 1
  Encryption algorithm: 3des
  Hash Algorithm: sha1
  Authentication Mode: pre-shared-key
  DH Group: group1
  Lifetime in seconds: 86400
  Lifetime in kilobytes: unlimited
```

8. Configure the IPSec tunnel to the remote host.

```
Router-1# configure terminal
Router-1/configure# crypto
Router-1/configure/crypto# ipsec policy NW2 172.16.0.2
Router-1/configure/crypto/ipsec policy NW2 172.16.0.2# match
address 172.16.0.1 32 10.0.2.0 24
Router-1/configure/crypto# ipsec policy NW2 172.16.0.2#
proposal 1
Router-1/configure/crypto# ipsec policy NW2 172.16.0.2/
proposal 1# encryption-algorithm aes128-cbc
Router-1/configure/crypto# ipsec policy NW2 172.16.0.2/
proposal 1# exit
Router-1/configure/crypto# ipsec policy NW2 172.16.0.2# exit
```



NOTE

For IPSec only-when you create an outbound tunnel, an inbound tunnel is automatically created. The inbound tunnel applies the name that you provide for the outbound tunnel and adds the prefix 'IN' to the name.

9. Display the policies.

```
Router-1# show crypto ipsec policy all
Policy Peer Match Proto Transform
-----
NW2 172.16.0.2 S 172.16.0.1/32/any Any P1 esp-aes-sha1-tunl
D 10.0.2.0/24/any
INN2 172.16.0.2 S 10.0.2.0/24/any Any P1 esp-aes-sha1-tunl
D 172.16.0.1/32/any
```

10. Display IPSec policies in detail.

```
Router-1# show crypto ipsec policy all detail

Policy name NW2 is enabled, Direction is outbound
Peer Address is 172.16.0.2, Action is Apply
Key Management is Automatic
PFS Group is disabled
Match Address:

    Protocol is Any
    Source ip
address(ip/mask/port):(172.16.0.1/255.255.255.255/any)
    Destination ip
address(ip/mask/port):(10.0.2.0/255.255.255.0/any)

Proposal of priority 1
    Protocol: esp
    Mode: tunnel
    Encryption Algorithm: aes128(key length=128 bits)
    Hash Algorithm: sha1
    Lifetime in seconds: 3600
    Lifetime in Kilobytes: 4608000

Policy name INN2 is enabled, Direction is inbound
Peer Address is 172.16.0.2, Action is Apply
Key Management is Automatic
PFS Group is disabled
Match Address:

    Protocol is Any
    Source ip
address(ip/mask/port):(10.0.2.0/255.255.255.0/any)
    Destination ip
address(ip/mask/port):(172.16.0.1/255.255.255.255/any)
```

```
Proposal of priority 1
  Protocol: esp
  Mode: tunnel
  Encryption Algorithm: aes128(key length=128 bits)
  Hash Algorithm: sha1
  Lifetime in seconds: 3600
  Lifetime in Kilobytes: 4608000
```

- 11.** Configure firewall policies to allow IKE negotiation through untrusted interface.

```
Router-1/configure# firewall internet
Router-1/configure/firewall internet# policy 100 in service
ike self
Router-1/configure/firewall internet/policy 100 in# exit
Router-1/configure/firewall internet# policy 101 out service
ike self
Router-1/configure/firewall internet/policy 101 out# exit
Router-1/configure/firewall internet# exit
```

- 12.** Configure firewall policies to allow desired services through untrusted interface to manage the router.

```
Router-1/configure# firewall internet
Router-1/configure/firewall internet# policy 1001 in service
snmp self
Router-1/configure/firewall internet/policy 1001 in# exit
Router-1/configure/firewall internet# policy 1002 in service
telnet self
Router-1/configure/firewall internet/policy 1002 in# exit
Router-1/configure/firewall internet# policy 1003 in
protocol icmp self
```

- 13.** Display firewall policies in the internet map.

```
Router-1# show firewall policy internet
Advanced:  S-Self Traffic, F-Ftp-Filter, H-Http-Filter,
           R-Rpc-Filter, N-Nat-Ip/Nat-Pool, L-Logging,
           E-Policy Enabled, M-Smtp-Filter
```

```

Pri Dir Source Addr Destination Addr Sport Dport Proto
Action Advanced
-----
-----
100 in any any ike PERMIT SE
101 out any any ike PERMIT SE
1000 in any any snmp PERMIT SE
1002 in any any telnet PERMIT SE
1003 in any any any any icmp PERMIT SE
1024 out any any any any any PERMIT SE

```

14. Display firewall policies in the internet map in detail.

```

Router-1# show firewall policy internet detail

Policy with Priority 100 is enabled, Direction is inbound
Action permit, Traffic is self
Logging is disable
Source Address is any, Dest Address is any
Source Port is any, Service Name is ike
Schedule is disabled, Ftp-Filter is disabled
Sntp-Filter is disabled, Http-Filter is disabled
Rpc-Filter is disabled, Nat is disabled
Bytes In 0, Bytes Out 0

Policy with Priority 101 is enabled, Direction is outbound
Action permit, Traffic is self
Logging is disable
Source Address is any, Dest Address is any
Source Port is any, Service Name is ike
Schedule is disabled, Ftp-Filter is disabled
Sntp-Filter is disabled, Http-Filter is disabled
Rpc-Filter is disabled, Nat is disabled
Bytes In 0, Bytes Out 0

Policy with Priority 1000 is enabled, Direction is inbound
Action permit, Traffic is self
Logging is disable
Source Address is any, Dest Address is any
Source Port is any, Service Name is ike
Schedule is disabled, Ftp-Filter is disabled
Sntp-Filter is disabled, Http-Filter is disabled
Rpc-Filter is disabled, Nat is disabled
Bytes In 0, Bytes Out 0

```

```
Policy with Priority 1001 is enabled, Direction is inbound
Action permit, Traffic is self
Logging is disable
```

```
Source Address is any, Dest Address is any
Source Port is any, Service Name is snmp
Schedule is disabled, Ftp-Filter is disabled
Smtp-Filter is disabled, Http-Filter is disabled
Rpc-Filter is disabled, Nat is disabled
Bytes In 0, Bytes Out 0
```

```
Policy with Priority 1002 is enabled, Direction is inbound
Action permit, Traffic is self
Logging is disable
Source Address is any, Dest Address is any
Source Port is any, Service Name is telnet
Schedule is disabled, Ftp-Filter is disabled
Smtp-Filter is disabled, Http-Filter is disabled
Rpc-Filter is disabled, Nat is disabled
Bytes In 0, Bytes Out 0
```

```
Policy with Priority 1003 is enabled, Direction is inbound
Action permit, Traffic is self
Logging is disable
Source Address is any, Dest Address is any
Source Port is any, Dest Port is any, Protocol is icmp
Schedule is disabled, Ftp-Filter is disabled
Smtp-Filter is disabled, Http-Filter is disabled
Rpc-Filter is disabled, Nat is disabled
Bytes In 0, Bytes Out 0
```

```
Policy with Priority 1024 is enabled, Direction is outbound
Action permit, Traffic is self
Logging is disable
Source Address is any, Dest Address is any
Source Port is any, Dest Port is any, any
Schedule is disabled, Ftp-Filter is disabled
Smtp-Filter is disabled, Http-Filter is disabled
```

15. Enable SNMP on the router.

```
Router-1/configure/crypto/# exit
Router-1/configure# snmp-server
Router-1/configure/snmp-server# community public rw
Router-1/configure/snmp-server# exit
```

16. Display SNMP communities.

```
Router-1# show snmp communities
Community = public, privilege=rw
```

Router-2 Configuration**1.** Configure a WAN bundle with untrusted network type.

```
Router-2/configure# interface bundle wan1
Router-2/configure/interface/bundle wan1# link t1 0/2/0
Router-2/configure/interface/bundle wan1# encapsulation ppp
Router-2/configure/interface/bundle wan1# ip address
172.16.0.2 24
Router-2/configure/interface/bundle wan1# crypto untrusted
Router-2/configure/interface/bundle wan1# exit
```

2. Configure the Ethernet interface with trusted network type.

```
Router-2/configure# interface ethernet 0/1
Router-2/configure interface/ethernet 0/1# ip address
10.0.2.1 24
Router-2/configure/interface/ethernet(0/1)# crypto trusted
Router-2/configure/interface/ethernet(0/1)# exit
```

3. Display the crypto interfaces.

```
Router-2# show crypto interfaces
Interface Network
Name Type
-----
ethernet 0/1 trusted
wan1 untrusted
```

4. Add the route to the peer LAN.

```
Router-2/configure# ip route 10.0.1.0 255.255.255.0 wan1
```

5. Configure IKE to the peer gateway.

```
Router-2/configure# crypto
Router-2/configure/crypto# ike policy NW1 172.16.0.1
Router-2/configure/crypto/ike/policy NW1 172.16.0.1# local-
address 172.16.0.2
Router-2/configure/crypto/ike/policy NW1 172.16.0.1# key
secretkey
Router-2/configure/crypto/ike/policy NW1 172.16.0.1#
proposal 1
Router-2/configure/crypto/ike/policy NW1 172.16.0.1/proposal
1# encryption-algorithm 3des-cbc
Router-2/configure/crypto/ike/policy NW1 172.16.0.1/proposal
1# exit
Router-2/configure/crypto/ike/policy NW1 172.16.0.1# exit
```

6. Display the IKE policies.

```
Router-2# show crypto ike policy all
Policy      Peer          Mode          Transform
-----
NW1 172.16.0.1 Main P1 pre-g1-3des-sha1
```

7. Display the IKE policies in detail.

```
Router-2# show crypto ike policy all detail

Policy name NW1, Local addr 172.16.0.2, Peer addr 172.16.0.1
Main mode, Response and Initiate, PFS is not enabled, Shared
Key is *****
Local ident 172.16.0.2(ip-address), Remote Ident
172.16.0.1(ip-address)

Proposal of priority 1
  Encryption algorithm: 3des
  Hash Algorithm: sha1
  Authentication Mode: pre-shared-key
  DH Group: group1
  Lifetime in seconds: 86400
  Lifetime in kilobytes: unlimited
```


8. Configure the IPSec tunnel to the remote host.

```
Router-2# configure terminal
Router-2/configure# crypto
Router-2/configure/crypto# ipsec policy NW1 172.16.0.1
Router-2/configure/crypto/ipsec policy NW1 172.16.0.1# match
address 172.16.0.2 32 10.0.1.0 24
Router-2/configure/crypto# ipsec policy NW1 172.16.0.1#
proposal 1
Router-2/configure/crypto# ipsec policy NW1 172.16.0.1/
proposal 1# encryption-algorithm aes128-cbc
Router-2/configure/crypto# ipsec policy NW1 172.16.0.1/
proposal 1# exit
Router-2/configure/crypto# ipsec policy NW1 172.16.0.1# exit
```



For IPSec only-when you create an outbound tunnel, an inbound tunnel is automatically created. The inbound tunnel applies the name that you provide for the outbound tunnel and adds the prefix 'IN' to the name.

9. Display the policies.

```
Router-2# show crypto ipsec policy all
Policy Peer Match Proto Transform
-----
NW1 172.16.0.1 S 172.16.0.2/32/any Any P1 esp-aes-sha1-tunl
D 10.0.1.0/24/any
INNW1 172.16.0.1 S 10.0.1.0/24/any Any P1 esp-aes-sha1-tunl
D 172.16.0.2/32/any
```

10. Display IPSec policies in detail.

```
Router-2# show crypto ipsec policy all detail

Policy name NW1 is enabled, Direction is outbound
Peer Address is 172.16.0.1, Action is Apply
Key Management is Automatic
PFS Group is disabled
Match Address:
```

```
        Protocol is Any
        Source ip
address(ip/mask/port):(172.16.0.2/255.255.255.255/any)
        Destination ip
address(ip/mask/port):(10.0.1.0/255.255.255.0/any)

Proposal of priority 1
        Protocol: esp
        Mode: tunnel
        Encryption Algorithm: aes128(key length=128 bits)
        Hash Algorithm: sha1
        Lifetime in seconds: 3600
        Lifetime in Kilobytes: 4608000

Policy name INNW1 is enabled, Direction is inbound
Peer Address is 172.16.0.1, Action is Apply
Key Management is Automatic
PFS Group is disabled
Match Address:
        Protocol is Any
        Source ip
address(ip/mask/port):(10.0.1.0/255.255.255.0/any)
        Destination ip
address(ip/mask/port):(172.16.0.2/255.255.255.255/
any)
Proposal of priority 1
        Protocol: esp
        Mode: tunnel
        Encryption Algorithm: aes128(key length=128 bits)
        Hash Algorithm: sha1
        Lifetime in seconds: 3600
        Lifetime in Kilobytes: 4608000
```

- 11.** Configure firewall policies to allow IKE negotiation through untrusted interface.

```
Router-2/configure# firewall internet
Router-2/configure/firewall internet# policy 100 in service
ike self
Router-2/configure/firewall internet/policy 100 in# exit
Router-2/configure/firewall internet# policy 101 out service
ike self
Router-2/configure/firewall internet/policy 101 out# exit
Router-2/configure/firewall internet# exit
```

- 12.** Configure firewall policies to allow desired services through untrusted interface to manage the router.

```
Router-2/configure# firewall corp
Router-2/configure/firewall corp# policy 1001 out service snmp
Router-2/configure/firewall corp/policy 1001 out# exit
Router-2/configure/firewall corp# policy 1002 out service telnet
Router-2/configure/firewall corp/policy 1002 out# exit
Router-2/configure/firewall corp# policy 1003 out protocol icmp
```

- 13.** Display firewall policies in the internet and corp maps.

```
Router-2# show firewall policy internet
Advanced: S-Self Traffic, F-Ftp-Filter, H-Http-Filter,
          R-Rpc-Filter, N-Nat-Ip/Nat-Pool, L-Logging,
          E-Policy Enabled, M-Smtp-Filter
Pri Dir Source Addr Destination Addr Sport Dport Proto
Action Advanced
-----
-
100 in    any any ike PERMIT SE
101 out   any any ike PERMIT SE
1024 out  any any any any PERMIT SE
```

```
Router-2# show firewall policy corp
Advanced: S-Self Traffic, F-Ftp-Filter, H-Http-Filter,
          R-Rpc-Filter, N-Nat-Ip/Nat-Pool, L-Logging,
          E-Policy Enabled, M-Smtp-Filter
Pri Dir Source Addr Destination Addr Sport Dport Proto
Action Advanced
-----
-
1000 out  any any snmp PERMIT E
1002 out  any any telnet PERMIT E
1003 out  any any any any icmp PERMIT E
1024 out  any any any any PERMIT E
```

14. Display firewall policies in the internet and corp maps in detail.

```
Router-2# show firewall policy internet detail
```

```
Policy with Priority 100 is enabled, Direction is inbound  
Action permit, Traffic is self
```

```
Logging is disable
```

```
Source Address is any, Dest Address is any
```

```
Source Port is any, Service Name is ike
```

```
Schedule is disabled, Ftp-Filter is disabled
```

```
Smtip-Filter is disabled, Http-Filter is disabled
```

```
Rpc-Filter is disabled, Nat is disabled
```

```
Bytes In 0, Bytes Out 0
```

```
Policy with Priority 101 is enabled, Direction is outbound
```

```
Action permit, Traffic is self
```

```
Logging is disable
```

```
Source Address is any, Dest Address is any
```

```
Source Port is any, Service Name is ike
```

```
Schedule is disabled, Ftp-Filter is disabled
```

```
Smtip-Filter is disabled, Http-Filter is disabled
```

```
Rpc-Filter is disabled, Nat is disabled
```

```
Bytes In 0, Bytes Out 0
```

```
Policy with Priority 1024 is enabled, Direction is outbound
```

```
Action permit, Traffic is self
```

```
Logging is disable
```

```
Source Address is any, Dest Address is any
```

```
Source Port is any, Dest Port is any, any
```

```
Schedule is disabled, Ftp-Filter is disabled
```

```
Smtip-Filter is disabled, Http-Filter is disabled
```

```
Router-2# show firewall policy corp detail
```

```
Policy with Priority 1001 is enabled, Direction is inbound
```

```
Action permit, Traffic is transit
```

```
Logging is disable
```

```
Source Address is any, Dest Address is any
```

```
Source Port is any, Service Name is snmp
```

```
Schedule is disabled, Ftp-Filter is disabled
```

```
Smtip-Filter is disabled, Http-Filter is disabled
```

```
Rpc-Filter is disabled, Nat is disabled
```

```
Bytes In 0, Bytes Out 0
```

```
Policy with Priority 1002 is enabled, Direction is inbound
Action permit, Traffic is transit
Logging is disable
Source Address is any, Dest Address is any
Source Port is any, Service Name is telnet
Schedule is disabled, Ftp-Filter is disabled
Sntp-Filter is disabled, Http-Filter is disabled
Rpc-Filter is disabled, Nat is disabled
Bytes In 0, Bytes Out 0
```

```
Policy with Priority 1003 is enabled, Direction is inbound
Action permit, Traffic is transit
Logging is disable
Source Address is any, Dest Address is any
Source Port is any, Dest Port is any, Protocol is icmp
Schedule is disabled, Ftp-Filter is disabled
Sntp-Filter is disabled, Http-Filter is disabled
Rpc-Filter is disabled, Nat is disabled
Bytes In 0, Bytes Out 0
```

```
Policy with Priority 1024 is enabled, Direction is outbound
Action permit, Traffic is transit
Logging is disable
Source Address is any, Dest Address is any
Source Port is any, Dest Port is any, any
Schedule is disabled, Ftp-Filter is disabled
Sntp-Filter is disabled, Http-Filter is disabled
```

Verifying The IPSec Tunnel

1. Test the IPSec tunnel for managing the Router-1 router from a host on Router-2's LAN.
2. When the SNMP manager starts managing Router-1 from Router-2's LAN, display the IKE and IPSec SA tables in Router-1 and Router-2.

```
Router-1# show crypto ike sa all
Policy      Peer      State    Bytes    Transform
-----
NW2 172.16.0.2  SA_MATURE  2020    pre-g1-3des-sha1
```

```
Router-1# show crypto ike sa all detail
```

```
Crypto Policy name: NW2
  Remote ident 172.16.0.2
  Peer Address is 172.16.0.2
  Transform: 3des, sha1, pre-shared-key
  DH Group: group1
  Bytes Processed 2020

  State is SA_MATURE
  Mode is Main
  Remaining Time in Sec: 86084
  Life Time in Sec: 86400, Life Time in Bytes is
  unlimited
```

```
Router-1# show crypto ipsec sa all
```

Policy	Dest IP	Spi	Bytes	Transform
-----	----	----	-----	-----
INNw2	172.16.0.1	0xe8453c2b	256	esp-aes-sha1-tunl
NW2	172.16.0.2	0xa1f673aa	256	esp-aes-sha1-tunl

```
Router-1# show crypto ipsec sa all detail
```

```
Crypto Policy name: INNw2
  Protocol is Any
  Local ident(ip/mask/port):(10.0.2.0/255.255.255.0/any)
  Remote
  ident(ip/mask/port):(172.16.0.1/255.255.255.255/any)
  Peer Address is 172.16.0.1, PFS Group is disabled
```

```
inbound ESP sas
```

```
  Spi: 0xe8453c2b
  Transform: aes128(key length=128 bits), sha1
  In use settings = {tunnel}
  Bytes Processed 256
  Hard lifetime in seconds 3290, Hard lifetime in
  kilobytes 413696
  Soft lifetime in seconds 0, Soft lifetime in
  kilobytes is unlimited
```

```
Crypto Policy name: NW2
```

```
  Protocol is Any
  Local ident(ip/mask/port):(172.16.0.1/255.255.255.255/
  any)
  Remote ident(ip/mask/port):(10.0.2.0/255.255.255.0/
  any)
  Peer Address is 172.16.0.2, PFS Group is disabled
```

```

outbound ESP sas
    Spi: 0xa1f673aa
    Transform: aes128(key length=128 bits), sha1
    In use settings = {tunnel}
    Bytes Processed 256
    Hard lifetime in seconds 3290, Hard lifetime in
    kilobytes 413695
    Soft lifetime in seconds 3200, Soft lifetime in
    kilobytes 37355
Router-2# show crypto ike sa all
Policy          Peer          State    Bytes    Transform
-----
NW1 172.16.0.1  SA_MATURE  2020    pre-g1-3des-sha1

```

```

Router-2# show crypto ike sa all detail

```

```

Crypto Policy name: NW1
Remote ident 172.16.0.1
Peer Address is 172.16.0.1
Transform: 3des, sha1, pre-shared-key
DH Group: group1
Bytes Processed 2020
State is SA_MATURE
Mode is Main
Remaining Time in Sec: 86084
Life Time in Sec: 86400, Life Time in Bytes is
unlimited

```

```

Router-2# show crypto ipsec sa all
Policy  Dest IP   Spi          Bytes  Transform
-----
INNW1  172.16.0.2  0xa1f673aa  256    esp-aes-sha1-tunl
NW1    172.16.0.1  0xe8453c2b  256    esp-aes-sha1-tunl

```

```

Router-2# show crypto ipsec sa all detail

```

```

Crypto Policy name: INNW1
Protocol is Any
Local ident(ip/mask/port):(10.0.1.0/255.255.255.0/any)
Remote
ident(ip/mask/port):(172.16.0.2/255.255.255.255/any)
Peer Address is 172.16.0.2, PFS Group is disabled

```

```

inbound ESP sas
  Spi: 0xa1f673aa
  Transform: aes128(key length=128 bits), sha1
  In use settings = {tunnel}
  Bytes Processed 256
  Hard lifetime in seconds 3290, Hard lifetime in
  kilobytes 413696
  Soft lifetime in seconds 0, Soft lifetime in
  kilobytes is unlimited
Crypto Policy name: NW1
Protocol is Any
Local ident(ip/mask/port):(172.16.0.2/255.255.255.255/
any)
  Remote ident(ip/mask/port):(10.0.1.0/255.255.255.0/
any)
  Peer Address is 172.16.0.1, PFS Group is disabled

outbound ESP sas
  Spi: 0xe8453c2b
  Transform: aes128(key length=128 bits), sha1
  In use settings = {tunnel}
  Bytes Processed 256
  Hard lifetime in seconds 3290, Hard lifetime in
  kilobytes 413695
  Soft lifetime in seconds 3200, Soft lifetime in
  kilobytes 37355

```

Joining Two Private Networks Example

The following example demonstrates how to form an IP security tunnel to join two private networks: 10.0.1.0/24 and 10.0.2.0/24. The security requirements are as follows:

- Phase 1: 3DES with SHA1
- Phase 2: IPSec ESP with AES (256-bit) and HMAC-SHA1

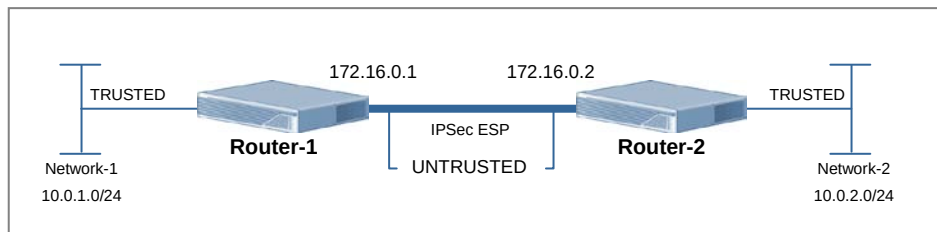


Figure 5.2 Tunnel Mode Between Two Security Gateways-Single Proposals

Router-1 Configuration

1. Configure a WAN bundle of network type untrusted.

```
Router-1/configure/interface/bundle wan1# link t1 0/2/0
Router-1/configure/interface/bundle wan1# encapsulation ppp
Router-1/configure/interface/bundle wan1# ip address
172.16.0.1 24
Router-1/configure/interface/bundle wan1# crypto untrusted
Router-1/configure/interface/bundle wan1# exit
```

2. Configure the Ethernet interface with trusted network type.

```
Router-1/configure# interface ethernet 0/1
message: Configuring existing Ethernet interface
Router-1/configure interface/ethernet(0/1)# ip address
10.0.1.1 24
Router-1/configure/interface/ethernet(0/1)# crypto trusted
Router-1/configure/interface/ethernet(0/1)# exit
```

3. Display the crypto interfaces.

```
Router-1# show crypto interfaces
```

Interface Name	Network Type
-----	-----
ethernet 0/1	trusted
wan1	untrusted

4. Add route to peer LAN.

```
Router-1/configure# ip route 10.0.2.0 255.255.255.0 wan1
```

5. Configure IKE to the peer gateway.

```
Router-1/configure# crypto
Router-1/configure/crypto# ike policy NW2 172.16.0.2
Router-1/configure/crypto/ike/policy NW2 172.16.0.2# local-
address 172.16.0.1
Router-1/configure/crypto/ike/policy NW2 172.16.0.2# key
secretkey
Router-1/configure/crypto/ike/policy NW2 172.16.0.2#
proposal 1
Router-1/configure/crypto/ike/policy NW2 172.16.0.2/proposal
1# encryption-algorithm 3des-cbc
Router-1/configure/crypto/ike/policy NW2 172.16.0.2/proposal
1# exit
```

6. Display the IKE policies.

```
Router-1# show crypto ike policy all
Policy      Peer          Mode          Transform
-----
NW2 172.16.0.2 Main P1 pre-g1-3des-sha1
```

7. Display the IKE policies in detail.

```
Router-1# show crypto ike policy all detail

Policy name NW2, Local addr 172.16.0.1, Peer addr 172.16.0.2
Main mode, Response and Initiate, PFS is not enabled, Shared
Key is *****
Local ident 172.16.0.1(ip-address), Remote Ident
172.16.0.2(ip-address)

Proposal of priority 1
  Encryption algorithm: 3des
  Hash Algorithm: sha1
  Authentication Mode: pre-shared-key
  DH Group: group1
  Lifetime in seconds: 86400
  Lifetime in kilobytes: unlimited
```

8. Configure IPSec tunnel to the remote host.

```
Router-1/configure/crypto# ipsec policy NW2 172.16.0.2
Router-1/configure/crypto/ipsec/policy NW2 172.16.0.2# match
address 10.0.1.0 24 10.0.2.0 24
Router-1/configure/crypto/ipsec/policy NW2 172.16.0.2#
proposal 1
Router-1/configure/crypto/ipsec/policy NW2
172.16.0.2/proposal
1# encryption-algorithm aes256-cbc
Router-1/configure/crypto/ipsec/policy NW2
172.16.0.2/proposal
1# exit
Router-1/configure/crypto/ipsec/policy NW2 172.16.0.2# exit
```



NOTE

For IPSec only-when you create an outbound tunnel, an inbound tunnel is automatically created. The inbound tunnel applies the name that you provide for the outbound tunnel and adds the prefix 'IN' to the name.

9. Display IPSec policies.

```
Router-1# show crypto ipsec policy all
Policy Peer Match Proto Transform
-----
NW2 172.16.0.2 S 10.0.1.0/24/any Any P1 esp-aes-sha1-tunl
D 10.0.2.0/24/any
INNW2 172.16.0.2 S 10.0.2.0/24/any Any P1 esp-aes-sha1-tunl
D 10.0.1.0/24/any
```

10. Router-1# show crypto ipsec policy all detail

```
Policy name NW2 is enabled, Direction is outbound
Peer Address is 172.16.0.2, Action is Apply
Key Management is Automatic
PFS Group is disabled
Match Address:
```

```

        Protocol is Any
        Source ip
address(ip/mask/port):(10.0.1.0/255.255.255.0/any)
        Destination ip
address(ip/mask/port):(10.0.2.0/255.255.255.0/any)

Proposal of priority 1
        Protocol: esp
        Mode: tunnel
        Encryption Algorithm: aes256(key length=256 bits)
        Hash Algorithm: sha1
        Lifetime in seconds: 3600
        Lifetime in Kilobytes: 4608000

Policy name INNW2 is enabled, Direction is inbound
Peer Address is 172.16.0.2, Action is Apply
Key Management is Automatic
PFS Group is disabled
Match Address:

        Protocol is Any
        Source ip
address(ip/mask/port):(10.0.2.0/255.255.255.0/any)
        Destination ip
address(ip/mask/port):(10.0.1.0/255.255.255.0/any)
Proposal of priority 1
        Protocol: esp
        Mode: tunnel
        Encryption Algorithm: aes256(key length=256 bits)
        Hash Algorithm: sha1
        Lifetime in seconds: 3600
        Lifetime in Kilobytes: 4608000

```

11. Configure firewall policies to allow IKE negotiation through untrusted interface.

```

Router-1/configure# firewall internet
Router-1/configure/firewall internet# policy 1000 in service
ike self
Router-1/configure/firewall internet/policy 1000 in# exit
Router-1/configure/firewall internet# policy 1001 out
service ike self
Router-1/configure/firewall internet/policy 1001 out# exit
Router-1/configure/firewall internet# exit

```

12. Display firewall policies in the internet map.

```
Router-1# show firewall policy internet

Advanced: S-Self Traffic, F-Ftp-Filter, H-Http-Filter,
          R-Rpc-Filter, N-Nat-Ip/Nat-Pool, L-Logging,
          E-Policy Enabled, M-Smtp-Filter

Pri Dir Source Addr      Destination Addr  Sport Dport Proto
Action Advanced
1000 in  any any          ike              PERMIT SE
1001 out any any          ike              PERMIT SE
1024 out any any          any any any PERMIT SE
```

13. Display firewall policies in the internet map in detail.

```
Router-1# show firewall policy internet detail

Policy with Priority 1000 is enabled, Direction is inbound
```

```
Action permit, Traffic is self
Logging is disable
Source Address is any, Dest Address is any
Source Port is any, Service Name is ike
Schedule is disabled, Ftp-Filter is disabled
Smtp-Filter is disabled, Http-Filter is disabled
Rpc-Filter is disabled, Nat is disabled
Bytes In 0, Bytes Out 0

Policy with Priority 1001 is enabled, Direction is outbound
Action permit, Traffic is self
Logging is disable
Source Address is any, Dest Address is any
Source Port is any, Service Name is ike
Schedule is disabled, Ftp-Filter is disabled
Smtp-Filter is disabled, Http-Filter is disabled
Rpc-Filter is disabled, Nat is disabled
Bytes In 0, Bytes Out 0

Policy with Priority 1024 is enabled, Direction is outbound
Action permit, Traffic is self
Logging is disable
Source Address is any, Dest Address is any
Source Port is any, Dest Port is any, any
Schedule is disabled, Ftp-Filter is disabled
Smtp-Filter is disabled, Http-Filter is disabled
Rpc-Filter is disabled, Nat is disabled
```

- 14.** Configure firewall policies to allow transit traffic between the remote LAN and the local LAN.

```
Router-1/configure# firewall corp
Router-1/configure/firewall corp# policy 1000 in address
10.0.2.0 24 10.0.1.0 24
Router-1/configure/firewall corp/policy 1000 in# exit
Router-1/configure/firewall corp# policy 1001 out address
10.0.1.0 24 10.0.2.0 24
Router-1/configure/firewall corp/policy 1001 out# exit
Router-1/configure/firewall corp# exit
```

- 15.** Display firewall policies in the corp map.

```
Router-1# show firewall policy corp
Advanced: S-Self Traffic, F-Ftp-Filter, H-Http-Filter,
R-Rpc-Filter, N-Nat-Ip/Nat-Pool, L-Logging,
E-Policy Enabled, M-Smtp-Filter
Pri Dir Source Addr Destination Addr Sport Dport Proto
Action Advanced
-----
-
1000 in 10.0.2.0/24 10.0.1.0/24 any any any PERMIT E
1001 out 10.0.1.0/24 10.0.2.0/24 any any any PERMIT E
1022 out any any any any any PERMIT SE
1023 in any any any any any PERMIT SE
1024 out any any any any any PERMIT E
```

- 16.** Display firewall policies in the corp map in detail.

```
Router-1# show firewall policy corp detail

Policy with Priority 1000 is enabled, Direction is inbound
Action permit, Traffic is transit
Logging is disable
Source Address is 10.0.2.0/24, Dest Address is 10.0.1.0/24
Source Port is any, Dest Port is any, any
Schedule is disabled, Ftp-Filter is disabled
Smtp-Filter is disabled, Http-Filter is disabled
Rpc-Filter is disabled, Nat is disabled
Max-Connections 1024, Connection-Rate is disabled
Policing is disabled, Bandwidth is disabled
Bytes In 0, Bytes Out 0
```

Policy with Priority 1001 is enabled, Direction is outbound
 Action permit, Traffic is transit
 Logging is disable
 Source Address is 10.0.1.0/24, Dest Address is 10.0.2.0/24
 Source Port is any, Dest Port is any, any
 Schedule is disabled, Ftp-Filter is disabled
 Sntp-Filter is disabled, Http-Filter is disabled
 Rpc-Filter is disabled, Nat is disabled
 Max-Connections 1024, Connection-Rate is disabled
 Policing is disabled, Bandwidth is disabled
 Bytes In 0, Bytes Out 0

Policy with Priority 1022 is enabled, Direction is outbound
 Action permit, Traffic is self
 Logging is disable
 Source Address is any, Dest Address is any
 Source Port is any, Dest Port is any, any
 Schedule is disabled, Ftp-Filter is disabled
 Sntp-Filter is disabled, Http-Filter is disabled
 Rpc-Filter is disabled, Nat is disabled
 Bytes In 0, Bytes Out 0

Policy with Priority 1023 is enabled, Direction is inbound
 Action permit, Traffic is self
 Logging is disable

Source Address is any, Dest Address is any
 Source Port is any, Dest Port is any, any
 Schedule is disabled, Ftp-Filter is disabled
 Sntp-Filter is disabled, Http-Filter is disabled
 Rpc-Filter is disabled, Nat is disabled
 Bytes In 0, Bytes Out 0

Policy with Priority 1024 is enabled, Direction is outbound
 Action permit, Traffic is transit
 Logging is disable
 Source Address is any, Dest Address is any
 Source Port is any, Dest Port is any, any
 Schedule is disabled, Ftp-Filter is disabled
 Sntp-Filter is disabled, Http-Filter is disabled
 Rpc-Filter is disabled, Nat is disabled
 Max-Connections 1024, Connection-Rate is disabled
 Policing is disabled, Bandwidth is disabled

Router-2 Configuration

1. Configure a WAN bundle with untrusted network type.

```
Router-2/configure/interface/bundle wan1# link t1 0/2/0
Router-2/configure/interface/bundle wan1# encapsulation ppp
Router-2/configure/interface/bundle wan1# ip address
172.16.0.2 24
Router-2/configure/interface/bundle wan1# crypto untrusted
Router-2/configure/interface/bundle wan1# exit
```

2. Configure the Ethernet interface with trusted network type.

```
Router-2/configure# interface ethernet 0/1
message: Configuring existing Ethernet interface
Router-2/configure interface/ethernet(0/1)# ip address
10.0.2.1 24
Router-2/configure/interface/ethernet(0/1)# crypto trusted
Router-2/configure/interface/ethernet(0/1)# exit
```

3. Display the crypto interfaces.

```
Router-2# show crypto interfaces
```

Interface Name	Network Type
-----	-----
ethernet 0/1	trusted
wan1	untrusted

4. Add route to peer LAN.

```
Router-2/configure# ip route 10.0.1.0 255.255.255.0 wan1
```


5. Configure IKE to the peer gateway.

```
Router-2/configure# crypto
Router-2/configure/crypto# ike policy NW1 172.16.0.1
Router-2/configure/crypto/ike/policy NW1 172.16.0.1# local-
address 172.16.0.2
Router-2/configure/crypto/ike/policy NW1 172.16.0.1# key
secretkey
Router-2/configure/crypto/ike/policy NW1 172.16.0.1#
proposal 1
Router-2/configure/crypto/ike/policy NW1 172.16.0.1/proposal
1# encryption-algorithm 3des-cbc
Router-2/configure/crypto/ike/policy NW1 172.16.0.1/proposal
1# exit
```

6. Display the IKE policies.

```
Router-2# show crypto ike policy all
Policy      Peer      Mode      Transform
-----
NW1 172.16.0.1 Main P1 pre-g1-3des-sha1
```

7. Display the IKE policies in detail.

```
Router-2# show crypto ike policy all detail

Policy name NW1, Local addr 172.16.0.2, Peer addr 172.16.0.1
Main mode, Response and Initiate, PFS is not enabled, Shared
Key is *****
Local ident 172.16.0.2(ip-address), Remote Ident
172.16.0.1(ip-address)

Proposal of priority 1
  Encryption algorithm: 3des
  Hash Algorithm: sha1
  Authentication Mode: pre-shared-key
  DH Group: group1
  Lifetime in seconds: 86400
  Lifetime in kilobytes: unlimited
```

8. Configure IPSec tunnel to the remote host.

```
Router-2/configure/crypto# ipsec policy NW1 172.16.0.1
Router-2/configure/crypto/ipsec/policy NW1 172.16.0.1# match
address 10.0.2.0 24 10.0.1.0 24
Router-2/configure/crypto/ipsec/policy NW1 172.16.0.1#
proposal 1
Router-2/configure/crypto/ipsec/policy NW1
172.16.0.1/proposal
1# encryption-algorithm aes256-cbc
Router-2/configure/crypto/ipsec/policy NW1
172.16.0.1/proposal
1# exit
Router-2/configure/crypto/ipsec/policy NW1 172.16.0.1# exit
```



NOTE

For IPSec only-when you create an outbound tunnel, an inbound tunnel is automatically created. The inbound tunnel applies the name that you provide for the outbound tunnel and adds the prefix 'IN' to the name.

9. Display IPSec policies.

```
Router-2# show crypto ipsec policy all
Policy Peer Match Proto Transform
-----
NW1 172.16.0.1 S 10.0.2.0/24/any Any P1 esp-aes-sha1-tunl
D 10.0.1.0/24/any
INNW1 172.16.0.1 S 10.0.1.0/24/any Any P1 esp-aes-sha1-tunl
D 10.0.2.0/24/any
```

10. Router-2# show crypto ipsec policy all details.

```
Policy name NW1 is enabled, Direction is outbound
Peer Address is 172.16.0.1, Action is Apply
Key Management is Automatic
PFS Group is disabled
Match Address:
```

```

        Protocol is Any
        Source ip
address(ip/mask/port):(10.0.2.0/255.255.255.0/any)
        Destination ip
address(ip/mask/port):(10.0.1.0/255.255.255.0/any)

Proposal of priority 1
    Protocol: esp
    Mode: tunnel
    Encryption Algorithm: aes256(key length=256 bits)
    Hash Algorithm: sha1
    Lifetime in seconds: 3600
    Lifetime in Kilobytes: 4608000

Policy name INNW1 is enabled, Direction is inbound
Peer Address is 172.16.0.1, Action is Apply
Key Management is Automatic
PFS Group is disabled
Match Address:

        Protocol is Any
        Source ip

```

```

address(ip/mask/port):(10.0.1.0/255.255.255.0/any)
        Destination ip
address(ip/mask/port):(10.0.2.0/255.255.255.0/any)
Proposal of priority 1
    Protocol: esp
    Mode: tunnel
    Encryption Algorithm: aes256(key length=256 bits)
    Hash Algorithm: sha1
    Lifetime in seconds: 3600
    Lifetime in Kilobytes: 4608000

```

11. Configure firewall policies to allow IKE negotiation through untrusted interface.

```

Router-2/configure# firewall internet
Router-2/configure/firewall internet# policy 1000 in service
ike self
Router-2/configure/firewall internet/policy 1000 in# exit
Router-2/configure/firewall internet# policy 1001 out
service ike self
Router-2/configure/firewall internet/policy 1001 out# exit
Router-2/configure/firewall internet# exit

```

12. Display firewall policies in the internet map.

```
Router-2# show firewall policy internet

Advanced: S-Self Traffic, F-Ftp-Filter, H-Http-Filter,
          R-Rpc-Filter, N-Nat-Ip/Nat-Pool, L-Logging,
          E-Policy Enabled, M-Smtp-Filter

Pri Dir Source Addr      Destination Addr Sport Dport
Proto Action Advanced
1000 in  any any      ike              PERMIT SE
1001 out any any      ike              PERMIT SE
1024 out any any      any any any PERMIT SE
```

13. Display firewall policies in the internet map in detail.

```
Router-2# show firewall policy internet detail

Policy with Priority 1000 is enabled, Direction is inbound
Action permit, Traffic is self
Logging is disable
Source Address is any, Dest Address is any
Source Port is any, Service Name is ike
Schedule is disabled, Ftp-Filter is disabled
Smtp-Filter is disabled, Http-Filter is disabled
Rpc-Filter is disabled, Nat is disabled
Bytes In 0, Bytes Out 0

Policy with Priority 1024 is enabled, Direction is outbound
Action permit, Traffic is self
Logging is disable
Source Address is any, Dest Address is any
Source Port is any, Dest Port is any, any
```

```
Schedule is disabled, Ftp-Filter is disabled
Smtp-Filter is disabled, Http-Filter is disabled
Rpc-Filter is disabled, Nat is disabled
```

- 14.** Configure firewall policies to allow transit traffic between the remote LAN and the local LAN.

```
Router-2/configure# firewall corp
Router-2/configure/firewall corp# policy 1000 in address
10.0.2.0 24 10.0.1.0 24
Router-2/configure/firewall corp/policy 1000 in# exit
Router-2/configure/firewall corp# policy 1001 out address
10.0.1.0 24 10.0.2.0 24
Router-2/configure/firewall corp/policy 1001 out# exit
Router-2/configure/firewall corp# exit
```

- 15.** Display firewall policies in the corp map.

```
Router-2# show firewall policy corp
Advanced: S-Self Traffic, F-Ftp-Filter, H-Http-Filter,
R-Rpc-Filter, N-Nat-Ip/Nat-Pool, L-Logging,
E-Policy Enabled, M-Smtp-Filter
Pri Dir Source Addr Destination Addr Sport Dport Proto
Action Advanced
-----
-
1000 in 10.0.2.0/24 10.0.1.0/24 any any any PERMIT E
1001 out 10.0.1.0/24 10.0.2.0/24 any any any PERMIT E
1022 out any any any any any PERMIT SE
1023 in any any any any any PERMIT SE
1024 out any any any any any PERMIT E
```

- 16.** Display firewall policies in the corp map in detail.

```
Router-2# show firewall policy corp detail

Policy with Priority 1000 is enabled, Direction is inbound
Action permit, Traffic is transit
Logging is disable
Source Address is 10.0.2.0/24, Dest Address is 10.0.1.0/24
Source Port is any, Dest Port is any, any
Schedule is disabled, Ftp-Filter is disabled
Smtp-Filter is disabled, Http-Filter is disabled
Rpc-Filter is disabled, Nat is disabled
Max-Connections 1024, Connection-Rate is disabled
Policing is disabled, Bandwidth is disabled
Bytes In 0, Bytes Out 0
```

Policy with Priority 1001 is enabled, Direction is outbound
Action permit, Traffic is transit
Logging is disable
Source Address is 10.0.1.0/24, Dest Address is 10.0.2.0/24
Source Port is any, Dest Port is any, any
Schedule is disabled, Ftp-Filter is disabled
Sntp-Filter is disabled, Http-Filter is disabled
Rpc-Filter is disabled, Nat is disabled
Max-Connections 1024, Connection-Rate is disabled
Policing is disabled, Bandwidth is disabled
Bytes In 0, Bytes Out 0

Policy with Priority 1022 is enabled, Direction is outbound
Action permit, Traffic is self
Logging is disable
Source Address is any, Dest Address is any
Source Port is any, Dest Port is any, any
Schedule is disabled, Ftp-Filter is disabled
Sntp-Filter is disabled, Http-Filter is disabled
Rpc-Filter is disabled, Nat is disabled
Bytes In 0, Bytes Out 0

Policy with Priority 1023 is enabled, Direction is inbound
Action permit, Traffic is self
Logging is disable

Source Address is any, Dest Address is any
Source Port is any, Dest Port is any, any
Schedule is disabled, Ftp-Filter is disabled
Sntp-Filter is disabled, Http-Filter is disabled
Rpc-Filter is disabled, Nat is disabled
Bytes In 0, Bytes Out 0

Policy with Priority 1024 is enabled, Direction is outbound
Action permit, Traffic is transit
Logging is disable
Source Address is any, Dest Address is any
Source Port is any, Dest Port is any, any
Schedule is disabled, Ftp-Filter is disabled
Sntp-Filter is disabled, Http-Filter is disabled
Rpc-Filter is disabled, Nat is disabled
Max-Connections 1024, Connection-Rate is disabled
Policing is disabled, Bandwidth is disabled

Verifying The IPSec Tunnel

1. Test the IPSec tunnel between Router-1 and Router-2 by passing traffic from the 10.0.1.0 to the 10.0.2.0 network.
2. After transit traffic is passed through the tunnel, display the IKE and IPSec SA tables in Router-1 and Router-2.

```
Router-1# show crypto ike sa all
Policy          Peer          State      Bytes      Transform
-----
NW2 172.16.0.2  SA_MATURE   1796       pre-g1-3des-sha1
```

```
Router-1# show crypto ike sa all detail
```

```
Crypto Policy name: NW2
Remote      ident 172.16.0.2
Peer Address is 172.16.0.2
Transform: 3des, sha1, pre-shared-key
DH Group: group1
Bytes Processed 1796
State is SA_MATURE
Mode is Main
Remaining Time in Sec: 86376
Life Time in Sec: 86400, Life Time in Bytes is
unlimited
```

```
Router-1# show crypto ipsec sa all
Policy  Dest IP  Spi  Bytes  Transform
-----
INNW2 172.16.0.1 0xd603a513 256 esp-aes-sha1-tunl
NW2 172.16.0.2 0xb013de87 256 esp-aes-sha1-tunl
```

```
Router-1# show crypto ipsec sa all detail
```

```
Crypto Policy name: INNW2
Protocol is Any
Local
ident(ip/mask/port):(10.0.2.0/255.255.255.0/any)
Remote
ident(ip/mask/port):(10.0.1.0/255.255.255.0/any)
Peer Address is 172.16.0.1, PFS Group is disabled
```

```

inbound ESP sas
  Spi: 0xd603a513
  Transform: aes256(key length=256 bits), sha1
  In use settings = {tunnel}
  Bytes Processed 256
  Hard lifetime in seconds 3560, Hard lifetime in
  kilobytes 413696
  Soft lifetime in seconds 0, Soft lifetime in
  kilobytes is unlimited

Crypto Policy name: NW2
  Protocol is Any
  Local
  ident(ip/mask/port):(10.0.1.0/255.255.255.0/any)
  Remote
  ident(ip/mask/port):(10.0.2.0/255.255.255.0/any)
  Peer Address is 172.16.0.2, PFS Group is disabled

outbound ESP sas
  Spi: 0xb013de87
  Transform: aes256(key length=256 bits), sha1
  In use settings = {tunnel}
  Bytes Processed 256
  Hard lifetime in seconds 3560, Hard lifetime in
  kilobytes 413695
  Soft lifetime in seconds 3470, Soft lifetime in
  kilobytes 41492

```

```

Router-2# show crypto ike sa all
Policy      Peer      State      Bytes      Transform
-----
NW1 172.16.0.2  SA_MATURE  1796      pre-g1-3des-sha1

```

```

Router-2# show crypto ike sa all detail

Crypto Policy name: NW1
  Remote      ident 172.16.0.2
  Peer Address is 172.16.0.2
  Transform: 3des, sha1, pre-shared-key
  DH Group: group1
  Bytes Processed 1796
  State is SA_MATURE
  Mode is Main
  Remaining Time in Sec: 86376
  Life Time in Sec: 86400, Life Time in Bytes is
  unlimited

```



```
Router-2# show crypto ipsec sa all
Policy  Dest IP  Spi  Bytes  Transform
-----  -
INNw1 172.16.0.1 0xd603a513 256 esp-aes-sha1-tunl
NW1 172.16.0.2 0xb013de87 256 esp-aes-sha1-tunl
```

```
Router-2# show crypto ipsec sa all detail

Crypto Policy name: INNw1
Protocol is Any
Local
ident(ip/mask/port):(10.0.2.0/255.255.255.0/any)
Remote
ident(ip/mask/port):(10.0.1.0/255.255.255.0/any)
Peer Address is 172.16.0.1, PFS Group is disabled

inbound ESP sas
Spi: 0xd603a513
Transform: aes256(key length=256 bits), sha1
In use settings = {tunnel}
Bytes Processed 256
Hard lifetime in seconds 3560, Hard lifetime in
kilobytes 413696
Soft lifetime in seconds 0, Soft lifetime in
kilobytes is unlimited

Crypto Policy name: NW1
Protocol is Any
Local
ident(ip/mask/port):(10.0.1.0/255.255.255.0/any)
Remote
ident(ip/mask/port):(10.0.2.0/255.255.255.0/any)
Peer Address is 172.16.0.2, PFS Group is disabled

outbound ESP sas
Spi: 0xb013de87
Transform: aes256(key length=256 bits), sha1
In use settings = {tunnel}
Bytes Processed 256
Hard lifetime in seconds 3560, Hard lifetime in
kilobytes 413695
Soft lifetime in seconds 3470, Soft lifetime in
kilobytes 41492
```

Joining Two Networks using Multiple IPsec Proposals Example

The following example demonstrates how a security gateway can use multiple IPsec (phase2) proposals to form an IP security tunnel to join two private networks: 10.0.1.0/24 and 10.0.2.0/24.

IKE Proposal offered by both Router-1 and Router-2:

- Phase 1: 3DES and SHA1

IPsec Proposals offered by Router-1:

- Phase 2: Proposal1: IPsec ESP with DES and HMAC-SHA1
 - Phase 2: Proposal2: IPsec ESP with AES (256-bit) and HMAC-SHA1
- IPsec

Proposal offered by Router-2:

- Phase 2: Proposal1: IPsec ESP with AES (256-bit) and HMAC-SHA1

In this example, the Router-1 router offers two IPsec proposals to the peer while the Router-2 router offers only one proposal. As a result of quick mode negotiation, the two routers are expected to converge on a mutually acceptable proposal, which is the proposal 'IPsec ESP with AES (256-bit) and HMAC-SHA1' in this example.

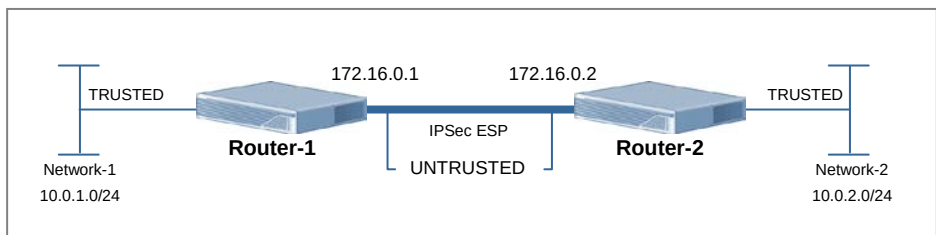


Figure 5.3 Tunnel Mode Between Two Security Gateways-Multiple Proposals

Router-1 Configuration

1. Configure a WAN bundle of network type untrusted.

```
Router-1/configure/interface/bundle wan1# link t1 0/2/0
Router-1/configure/interface/bundle wan1# encapsulation ppp
Router-1/configure/interface/bundle wan1# ip address
172.16.0.1 24
Router-1/configure/interface/bundle wan1# crypto untrusted
Router-1/configure/interface/bundle wan1# exit
```

2. Configure the Ethernet interface with trusted network type.

```
Router-1/configure# interface ethernet 0/1
Configuring existing Ethernet interface
Router-1/configure interface/ethernet(0/1)# ip address
10.0.1.1 24
Router-1/configure/interface/ethernet(0/1)# crypto trusted
Router-1/configure/interface/ethernet(0/1)# exit
```

3. Display the crypto interfaces.

```
Router-1# show crypto interfaces
Interface Network
Name Type
-----
ethernet0/1 trusted
wan1      untrusted
```

4. Add the route to the peer LAN.

```
Router-1/configure# ip route 10.0.2.0 255.255.255.0 wan1
```

5. Configure IKE to the peer gateway.

```
Router-1/configure# crypto
Router-1/configure/crypto# ike policy NW2 172.16.0.2
Router-1/configure/crypto/ike/policy NW2 172.16.0.2# local-
address 172.16.0.1
Router-1/configure/crypto/ike/policy NW2 172.16.0.2# key
secretkey
Router-1/configure/crypto/ike/policy NW2 172.16.0.2# proposal
1
Router-1/configure/crypto/ike/policy NW2 172.16.0.2/proposal
1# encryption-algorithm 3des-cbc
Router-1/configure/crypto/ike/policy NW2 172.16.0.2/proposal
1# exit
Router-1/configure/crypto/ike/policy NW2 172.16.0.2# exit
```

6. Display the IKE policies.

```
Router-1# show crypto ike policy all
Policy      Peer          Mode          Transform
-----
NW2 172.16.0.2 Main P1 pre-g1-3des-sha1
```

7. Display the IKE policies in detail.

```
Router-1# show crypto ike policy all detail

Policy name NW2, Local addr 172.16.0.1, Peer addr 172.16.0.2
Main mode, Response and Initiate, PFS is not enabled, Shared
Key is *****
Local ident 172.16.0.1(ip-address), Remote Ident
172.16.0.2(ip-address)

Proposal of priority 1
  Encryption algorithm: 3des
  Hash Algorithm: sha1
  Authentication Mode: pre-shared-key
  DH Group: group1
  Lifetime in seconds: 86400
  Lifetime in kilobytes: unlimited
```

8. Configure IPSec tunnel to the remote host.

```
Router-1/configure/crypto# ipsec policy NW2 172.16.0.2
Router-1/configure/crypto/ipsec/policy NW2 172.16.0.2# match
address 10.0.1.0 24 10.0.2.0 24
Router-1/configure/crypto/ipsec/policy NW2 172.16.0.2#
proposal 1
Router-1/configure/crypto/ipsec/policy NW2
172.16.0.2/proposal 1# encryption-algorithm des-cbc
Router-1/configure/crypto/ipsec/policy NW2
172.16.0.2/proposal 1# exit
Router-1/configure/crypto/ipsec/policy NW2 172.16.0.2#
proposal 2
Router-1/configure/crypto/ipsec/policy NW2
172.16.0.2/proposal 2# encryption-algorithm aes256-cbc
Router-1/configure/crypto/ipsec/policy NW2
172.16.0.2/proposal 2# exit
Router-1/configure/crypto/ipsec/policy NW2 172.16.0.2# exit
Router-1/configure/crypto# exit
Router-1/configure#
```



For IPSec only-when you create an outbound tunnel, an inbound tunnel is automatically created. The inbound tunnel applies the name that you provide for the outbound tunnel and adds the prefix 'IN' to the name.

9. Configure IPSec tunnel to the remote host.

```
Router-1# show crypto ipsec policy all
Policy Peer Match Proto Transform
-----
NW2 172.16.0.2 S 10.0.1.0/24/any Any P1 esp-des-sha1-tunl
D 10.0.2.0/24/any P2 esp-aes-sha1-tunl
INNW2 172.16.0.2 S 10.0.2.0/24/any Any P1 esp-des-sha1-tunl
D 10.0.1.0/24/any P2 esp-aes-sha1-tunl
```

```
Router-1# show crypto ipsec policy all detail

Policy name NW2 is enabled, Direction is outbound
Peer Address is 172.16.0.2, Action is Apply
Key Management is Automatic
PFS Group is disabled
Match Address:

    Protocol is Any
    Source ip
address(ip/mask/port):(10.0.1.0/255.255.255.0/any)
    Destination ip
address(ip/mask/port):(10.0.2.0/255.255.255.0/any)

Proposal of priority 1
    Protocol: esp
    Mode: tunnel
    Encryption Algorithm: des
    Hash Algorithm: sha1
    Lifetime in seconds: 3600
    Lifetime in Kilobytes: 4608000

Proposal of priority 2
    Protocol: esp
    Mode: tunnel
    Encryption Algorithm: aes256(key length=256 bits)
    Hash Algorithm: sha1
    Lifetime in seconds: 3600
    Lifetime in Kilobytes: 4608000
Policy name INNW2 is enabled, Direction is inbound
Peer Address is 172.16.0.2, Action is Apply
Key Management is Automatic
PFS Group is disabled
Match Address:
    Protocol is Any
    Source ip
address(ip/mask/port):(10.0.2.0/255.255.255.0/any)
    Destination ip
address(ip/mask/port):(10.0.1.0/255.255.255.0/any)

Proposal of priority 1
    Protocol: esp
    Mode: tunnel
    Encryption Algorithm: des
    Hash Algorithm: sha1
    Lifetime in seconds: 3600
    Lifetime in Kilobytes: 4608000
```

```
Proposal of priority 2
Protocol: esp
Mode: tunnel
Encryption Algorithm: aes256(key length=256 bits)
Hash Algorithm: sha1
Lifetime in seconds: 3600
Lifetime in Kilobytes: 4608000
```

10. Configure firewall policies to allow IKE negotiation through untrusted interface.

```
Router-1/configure# firewall internet
Router-1/configure/firewall internet# policy 1000 in service
ike self
Router-1/configure/firewall internet/policy 1000 in# exit
Router-1/configure/firewall internet# policy 1001 out
service ike self
Router-1/configure/firewall internet/policy 1001 out# exit
Router-1/configure/firewall internet# exit
```

11. Display firewall policies in the internet map.

```
Router-1# show firewall policy internet

Advanced: S-Self Traffic, F-Ftp-Filter, H-Http-Filter,
          R-Rpc-Filter, N-Nat-Ip/Nat-Pool, L-Logging,
          E-Policy Enabled, M-Smtp-Filter
```

Pri	Dir	Source Addr	Destination Addr	Sport	Dport	Proto
1000	in	any any	ike			PERMIT SE
1001	out	any any	ike			PERMIT SE
1024	out	any any	any any any			PERMIT SE

12. Display firewall policies in the internet map in detail.

```
Router-1# show firewall policy internet detail

Policy with Priority 1000 is enabled, Direction is inbound
Action permit, Traffic is self
Logging is disable
Source Address is any, Dest Address is any
Source Port is any, Service Name is ike
Schedule is disabled, Ftp-Filter is disabled
Sntp-Filter is disabled, Http-Filter is disabled
Rpc-Filter is disabled, Nat is disabled
Bytes In 0, Bytes Out 0

Policy with Priority 1000 is enabled, Direction is outbound
Action permit, Traffic is self
Logging is disable
Source Address is any, Dest Address is any
Source Port is any, Service Name is ike
Schedule is disabled, Ftp-Filter is disabled
Sntp-Filter is disabled, Http-Filter is disabled
Rpc-Filter is disabled, Nat is disabled
Bytes In 0, Bytes Out 0

Policy with Priority 1024 is enabled, Direction is outbound
Action permit, Traffic is self
Logging is disable
Source Address is any, Dest Address is any
Source Port is any, Dest Port is any, any
Schedule is disabled, Ftp-Filter is disabled
Sntp-Filter is disabled, Http-Filter is disabled
Rpc-Filter is disabled, Nat is disabled
```

13. Configure firewall policies to allow transit traffic from remote LAN to the local LAN.

```
Router-1/configure# firewall corp
Router-1/configure/firewall corp# policy 1000 in address
10.0.2.0 24 10.0.1.0 24
Router-1/configure/firewall corp/policy 1000 in# exit
Router-1/configure/firewall corp# exit
```


14. Display firewall policies in the corp map.

```

Router-1# show firewall policy corp
Advanced: S-Self Traffic, F-Ftp-Filter, H-Http-Filter,
R-Rpc-Filter, N-Nat-Ip/Nat-Pool, L-Logging,
E-Policy Enabled, M-Smtp-Filter
Pri Dir Source Addr Destination Addr Sport Dport Proto
Action Advanced
-----
1000 in 10.0.2.0/24 10.0.1.0/24 any any any PERMIT E
1022 out any any any any any PERMIT SE
1023 in any any any any any PERMIT SE
1024 out any any any any any PERMIT E

```

15. Display firewall policies in the corp map in detail.

```

Router-1# show firewall policy corp detail

Policy with Priority 1000 is enabled, Direction is inbound
Action permit, Traffic is transit
Logging is disable
Source Address is 10.0.2.0/24, Dest Address is 10.0.1.0/24
Source Port is any, Dest Port is any, any
Schedule is disabled, Ftp-Filter is disabled
Smtp-Filter is disabled, Http-Filter is disabled
Rpc-Filter is disabled, Nat is disabled
Max-Connections 1024, Connection-Rate is disabled
Policing is disabled, Bandwidth is disabled
Bytes In 0, Bytes Out 0

Policy with Priority 1022 is enabled, Direction is outbound
Action permit, Traffic is self
Logging is disable
Source Address is any, Dest Address is any
Source Port is any, Dest Port is any, any
Schedule is disabled, Ftp-Filter is disabled
Smtp-Filter is disabled, Http-Filter is disabled
Rpc-Filter is disabled, Nat is disabled
Bytes In 0, Bytes Out 0

Policy with Priority 1023 is enabled, Direction is inbound
Action permit, Traffic is self
Logging is disable

```

```

Source Address is any, Dest Address is any
Source Port is any, Dest Port is any, any
Schedule is disabled, Ftp-Filter is disabled
Smtp-Filter is disabled, Http-Filter is disabled
Rpc-Filter is disabled, Nat is disabled
Bytes In 0, Bytes Out 0
Policy with Priority 1024 is enabled, Direction is outbound
Action permit, Traffic is transit
Logging is disable
Source Address is any, Dest Address is any
Source Port is any, Dest Port is any, any
Schedule is disabled, Ftp-Filter is disabled
Smtp-Filter is disabled, Http-Filter is disabled
Rpc-Filter is disabled, Nat is disabled
Max-Connections 1024, Connection-Rate is disabled
Policing is disabled, Bandwidth is disabled
Bytes In 11258, Bytes Out 5813

```

Router-2 Configuration

1. Configure the Ethernet interface with trusted network type.

```
Router-2/configure# interface ethernet 0/1
```

2. Configuring existing Ethernet interface.

```

Router-2/configure interface/ethernet (0/1)# ip address
10.0.2.1 24
Router-2/configure/interface/ethernet (0/1)# crypto trusted
Router-2/configure/interface/ethernet (0/1)# exit

```

3. Display the crypto interfaces.

```
Router-2# show crypto interfaces
```

Interface Name	Network Type
-----	-----
ethernet0/1	trusted
wan1	untrusted

4. Add the route to the peer LAN.

```
Router-2/configure# ip route 10.0.1.0 24 wan1
```

5. Configure IKE to the peer gateway.

```
Router-2/configure# crypto
Router-2/configure/crypto# ike policy NW1 172.16.0.1
Router-2/configure/crypto/ike/policy NW1 172.16.0.1# local-
address 172.16.0.2

Default proposal created with priority1-des-sha1-pre_shared-g1
Key String has to be configured by the user
Router-2/configure/crypto/ike/policy NW1 172.16.0.1# key
secretkey
Router-2/configure/crypto/ike/policy NW1 172.16.0.1# proposal 1
Router-2/configure/crypto/ike/policy NW1 172.16.0.1/proposal
1# encryption-algorithm 3des-cbc
Router-2/configure/crypto/ike/policy NW1 172.16.0.1/proposal
1# exit
Router-2/configure/crypto/ike/policy NW1 172.16.0.1# exit
```

6. Display the IKE policies.

```
Router-2# show crypto ike policy all
Policy      Peer          Mode          Transform
-----
NW1 172.16.0.1 Main P1 pre-g1-3des-sha1
```

7. Display the IKE policies in detail.

```
Router-2# show crypto ike policy all detail

Policy name NW1, Local addr 172.16.0.1, Peer addr 172.16.0.2
Main mode, Response and Initiate, PFS is not enabled, Shared
Key is *****
Local ident 172.16.0.1 (ip-address), Remote Ident 172.16.0.2
(ip-address)
```

```
Proposal of priority 1
  Encryption algorithm: 3des
  Hash Algorithm: sha1
  Authentication Mode: pre-shared-key
  DH Group: group1
  Lifetime in seconds: 86400
  Lifetime in kilobytes: unlimited
```

8. Configure IPSec tunnel to the remote host.

```
Router-2/configure/crypto# ipsec policy NW1 172.16.0.1
Router-2/configure/crypto/ipsec/policy NW1 172.16.0.1# match
address 10.0.2.0 24 10.0.1.0 24

Default proposal created with priority1-esp-3des-sha1-tunnel
and activated.

Router-2/configure/crypto/ipsec/policy NW1 172.16.0.1#
proposal 1
Router-2/configure/crypto/ipsec/policy NW1
172.16.0.1/proposal 1# encryption-algorithm aes256-cbc
Router-2/configure/crypto/ipsec/policy NW1
172.16.0.1/proposal 1# mode tunnel
Router-2/configure/crypto/ipsec/policy NW1 172.16.0.1# exit
Router-2/configure/crypto# exit
Router-2/configure#
```

Verifying The IPSec Tunnel

1. Test the IPSec tunnel between Router-1 and Router-2 by passing traffic from the 10.0.1.0 network to the 10.0.2.0 network.
2. After traffic is passed through the tunnel, display the IKE and IPSec SA tables.

```
Router-1# show crypto ike sa all
Policy          Peer          State    Bytes    Transform
-----
NW2 172.16.0.2  SA_MATURE    1796     pre-g1-3des-sha1
```

```
Router-1# show crypto ike sa all detail

Crypto Policy name: NW2
  Remote ident 172.16.0.2
  Peer Address is 172.16.0.2
  Transform: 3des, sha1, pre-shared-key
  DH Group: group1
  Bytes Processed 1796
  State is SA_MATURE
  Mode is Main
  Remaining Time in Sec: 86380
  Life Time in Sec: 86400, Life Time in Bytes is
  unlimited
```

```
Router-1# show crypto ipsec sa all
Policy Dest IP Spi Bytes Transform
-----
INNW2 172.16.0.1 0x8eabe4b3 256 esp-aes-sha1-tunl
NW2 172.16.0.2 0xa9a506f9 256 esp-aes-sha1-tunl
```

```
Router-1# show crypto ipsec sa all detail

Crypto Policy name: INNW2
  Protocol is Any
  Local ident(ip/mask/port):(10.0.2.0/255.255.255.0/any)
  Remote ident(ip/mask/port):(10.0.1.0/255.255.255.0/any)
  Peer Address is 172.16.0.1, PFS Group is disabled
```

```
inbound    ESP sas
Spi: 0x8eabe4b3
Transform: aes256(key length=256 bits), sha1
In use settings = {tunnel}
Bytes Processed 256
Hard lifetime in seconds 3570, Hard lifetime in
kilobytes 413696
Soft lifetime in seconds 0, Soft lifetime in
kilobytes is unlimited

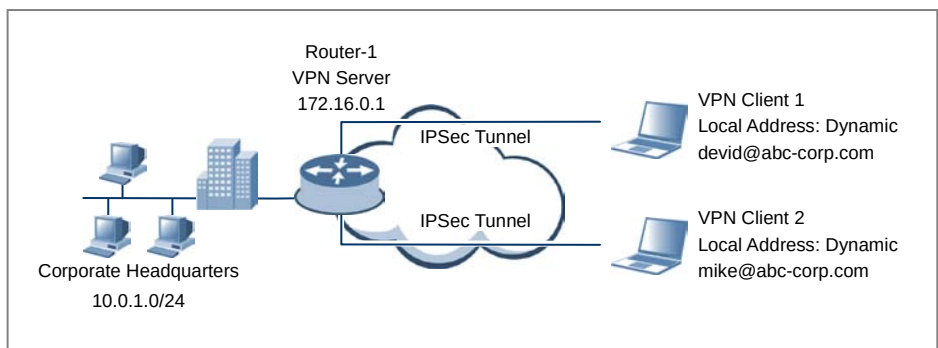
Crypto Policy name: NW2
Protocol is Any
Local ident(ip/mask/port):(10.0.1.0/255.255.255.0/any)
Remote ident(ip/mask/port):(10.0.2.0/255.255.255.0/any)
Peer Address is 172.16.0.2, PFS Group is disabled

outbound ESP sas
Spi: 0xa9a506f9
Transform: aes256(key length=256 bits), sha1 In use
settings = {tunnel}
Bytes Processed 256
Hard lifetime in seconds 3570, Hard lifetime in
kilobytes 413695
Soft lifetime in seconds 3540, Soft lifetime in
kilobytes 20233
```

Supporting Remote User Access Example

The following example demonstrates how to configure a router to be an IPsec VPN server using user group method with extended authentication (XAUTH) for remote VPN clients. The client could be any standard IPsec VPN client. In this example, the client needs to access the corporate private network 10.0.1.0/24 through the VPN tunnel. The security requirements are as follows:

- Phase 1: 3DES with SHA1, Xauth (Radius PAP)
- Phase 2: IPsec ESP tunnel with AES256 and HMAC-SHA1



1. Configure a WAN bundle of network type untrusted.

```
Router-1/configure# interface bundle wan1
Router-1/configure/interface/bundle wan1# link t1 0/2/0
Router-1/configure/interface/bundle wan1# encapsulation ppp
Router-1/configure/interface/bundle wan1# ip address
172.16.0.1 24
Router-1/configure/interface/bundle wan1# crypto untrusted
Router-1/configure/interface/bundle wan1# exit
```

2. Configure the Ethernet interface with trusted network type.

```
Router-1/configure# interface ethernet 0/1
message: Configuring existing Ethernet interface
Router-1/configure interface/ethernet(0/1)# ip address
10.0.1.1 24
Router-1/configure/interface/ethernet(0/1)# crypto trusted
Router-1/configure/interface/ethernet(0/1)# exit
```

3. Display the crypto interfaces.

```
Router-1# show crypto interfaces
```

Interface Name	Network Type
-----	----
ethernet0/1	trusted
wan1	untrusted

4. Configure dynamic IKE policy for a group of mobile users.

```
Router-1/configure# crypto
Router-1/configure/crypto# dynamic
Router-1/configure/crypto/dynamic# ike policy sales
Router-1/configure/crypto/dynamic/ike/policy sales# local-
address 172.16.0.1
Router-1/configure/crypto/dynamic/ike/policy sales# remote-
id email-id david@abc-corp.com david
New user david is added to the group sales
Default proposal created with priority1-des-sha1-pre_shared-g1

Key String has to be configured by the user

Router-1/configure/crypto/dynamic/ike/policy sales# remote-
id email-id mike@abc-corp.com mike
New user mike is added to the group sales

Router-1/configure/crypto/dynamic/ike/policy sales# key
secretkeyforsalesusers
Router-1/configure/crypto/dynamic/ike/policy sales# proposal 1
Router-1/configure/crypto/dynamic/ike/policy sales/proposal 1#
encryption-algorithm 3des-cbc
Router-1/configure/crypto/dynamic/ike/policy sales/proposal
1# exit
Router-1/configure/crypto/dynamic/ike/policy sales# client
authentication radius pap
Router-1/configure/crypto/dynamic/ike/policy sales# exit
Router-1/configure/crypto/dynamic#
```


5. Display dynamic IKE policies.

```
Router-1# show crypto dynamic ike policy all
Policy Remote-id Mode Transform Address-Pool
-----
sales U david@tabc... Aggressive P1 pre-g1-3des-sha1
```

6. Display dynamic IKE policies in detail.

```
Router-1# show crypto dynamic ike policy all detail

Policy name sales, User group name sales
Aggressive mode, Response Only, PFS is not enabled, Shared
Key is *****
Client authentication is Radius(PAP)
Local addr: 172.16.0.1, Local ident 172.16.0.1(ip-address)
Remote ids are david@abc-corp.com(email-id), mike@abc-
corp.com(email
id)

Proposal of priority 1
  Encryption algorithm: 3des
  Hash Algorithm: sha1
  Authentication Mode: pre-shared-key
  DH Group: group1
  Lifetime in seconds: 86400
  Lifetime in kilobytes: unlimited
```

7. Configure dynamic IPsec policy for a group of mobile users.

```
Router-1/configure/crypto/dynamic# ipsec policy sales

Router-1/configure/crypto/dynamic/ipsec/policy sales# match
address 10.0.1.0 24

Default proposal created with priority1-esp-3des-sha1-tunnel
and activated.

Router-1/configure/crypto/dynamic/ipsec/policy sales# proposal 1
Router-1/configure/crypto/dynamic/ipsec/policy
sales/proposal 1#
encryption-algorithm aes256-cbc
Router-1/configure/crypto/dynamic/ipsec/policy
sales/proposal 1# exit
Router-1/configure/crypto/dynamic/ipsec/policy sales# exit
Router-1/configure/crypto/dynamic#
```

8. Display dynamic IPsec policies.

```
Router-1# show crypto dynamic ipsec policy all

Policy   Match                Proto Transform
-----
sales    S 10.0.1.0/24/any Any   P1 esp-aes-sha1-tunl
         D any/any/any

INsales  S any/any/any      Any   P1 esp-aes-sha1-tunl
         D 10.0.1.0/24/any
```

9. Display dynamic IPsec policies in detail.

```
Router-1# show crypto dynamic ipsec policy all detail

Policy sales is enabled, User group name sales
Direction is outbound, Action is Apply
Key Management is Automatic
PFS Group is disabled
Match Address:
    Protocol is Any
    Source ip
address(ip/mask/port):(10.0.1.0/255.255.255.0/any)
    Destination ip address(ip/mask/port):(any/any/any)

Proposal of priority 1
    Protocol: esp
    Mode: tunnel
    Encryption Algorithm: aes256(key length=256 bits)
    Hash Algorithm: sha1
    Lifetime in seconds: 3600
    Lifetime in Kilobytes: 4608000

Policy INsales is enabled, User group name sales
Direction is inbound, Action is Apply
Key Management is Automatic
PFS Group is disabled
Match Address:
    Protocol is Any
    Source ip address(ip/mask/port):(any/any/any)
    Destination ip
address(ip/mask/port):(10.0.1.0/255.255.255.0/any)
```

```

Proposal of priority 1
  Protocol: esp
  Mode: tunnel
  Encryption Algorithm: aes256(key length=256 bits)
  Hash Algorithm: sha1
  Lifetime in seconds: 3600
  Lifetime in Kilobytes: 4608000

```

- 10.** Configure RADIUS server (applicable only if client authentication is configured in dynamic IKE policy).

```

Router-1/configure# aaa
Router-1/configure/aaa# radius
Router-1/configure/aaa/radius# primary_server 172.168.2.1
Primary Radius server configured.
Router-1/configure/aaa/radius# secondary_server 192.168.2.1
Secondary Radius server configured.
Router-1/configure/aaa/radius# enable radius
Router-1/configure/aaa/radius# exit
Router-1/configure/aaa# exit

```

- 11.** Configure firewall policies to allow IKE negotiation through untrusted interface.

```

Router-1/configure# firewall internet
Router-1/configure/firewall internet# policy 1000 in service
ike self
Router-1/configure/firewall internet/policy 1000 in# exit
Router-1/configure/firewall internet# exit

```

- 12.** Display firewall policies in the internet map.

```

Router-1# show firewall policy internet

Advanced: S-Self Traffic, F-Ftp-Filter, H-Http-Filter,
R-Rpc-Filter, N-Nat-Ip/Nat-Pool, L-Logging,
E-Policy Enabled, M-Smtp-Filter

Pri  Dir Source Addr Destination Addr Sport Dport Proto
Action Advanced
---  -
1000 in   any    any    ike    PERMIT    SE
1024 out  any    any    any    any any    PERMIT    SE

```

13. Display firewall policies in the internet map in detail.

```
Router-1# show firewall policy internet detail

Policy with Priority 1000 is enabled, Direction is inbound
Action permit, Traffic is self
Logging is disable
Source Address is any, Dest Address is any
Source Port is any, Service Name is ike
Schedule is disabled, Ftp-Filter is disabled
Sntp-Filter is disabled, Http-Filter is disabled
Rpc-Filter is disabled, Nat is disabled
Bytes In 0, Bytes Out 0

Policy with Priority 1024 is enabled, Direction is outbound
Action permit, Traffic is self
Logging is disable
Source Address is any, Dest Address is any
Source Port is any, Dest Port is any, any
Schedule is disabled, Ftp-Filter is disabled
Sntp-Filter is disabled, Http-Filter is disabled
Rpc-Filter is disabled, Nat is disabled
Bytes In 0, Bytes Out 0
```

14. Configure firewall policies for a group of mobile users to allow access to the local LAN.

```
Router-1/configure/firewall corp#
Router-1/configure/firewall corp# policy 1000 in user-group
sales address any any 10.0.1.0 24
Router-1/configure/firewall corp/policy 1000 in# exit
Router-1/configure/firewall corp#
```



NOTE

Be sure to match the user group name in the policy command with the name used in Step 4 (the dynamic IKE policy).

15. Display firewall policies in the corp map.

```
Router-1# show firewall policy corp

Advanced: S-Self Traffic, F-Ftp-Filter, H-Http-Filter,
R-Rpc-Filter, N-Nat-Ip/Nat-Pool, L-Logging,
E-Policy Enabled, M-Smtp-Filter

Pri Dir Source Addr   Destination Addr   Sport Dport Proto
Action Advanced

1000 in  any           10.0.1.0/24       any any  any PERMIT E
1022 out any           any any any    any PERMIT SE
1023 in  any           any any any    any PERMIT SE
1024 out any           any any any    any PERMIT E
```

16. Display firewall policies in the corp map in detail.

```
Router-1# show firewall policy corp detail

Policy with Priority 1000 is enabled, Direction is inbound
Action permit, Traffic is transit
User Group is sales, Logging is disable
Source Address is any, Dest Address is 10.0.1.0/24
Source Port is any, Dest Port is any, any
Schedule is disabled, Ftp-Filter is disabled
Smtp-Filter is disabled, Http-Filter is disabled
Rpc-Filter is disabled, Nat is disabled
Max-Connections 1024, Connection-Rate is disabled
Policing is disabled, Bandwidth is disabled
Bytes In 0, Bytes Out 0

Policy with Priority 1022 is enabled, Direction is outbound
Action permit, Traffic is self
Logging is disable
Source Address is any, Dest Address is any
Source Port is any, Dest Port is any, any
Schedule is disabled, Ftp-Filter is disabled
Smtp-Filter is disabled, Http-Filter is disabled
Rpc-Filter is disabled, Nat is disabled
Bytes In 0, Bytes Out 0
```

```
Policy with Priority 1023 is enabled, Direction is inbound
Action permit, Traffic is self
Logging is disable
Source Address is any, Dest Address is any
Source Port is any, Dest Port is any, any
Schedule is disabled, Ftp-Filter is disabled
Smtp-Filter is disabled, Http-Filter is disabled
Rpc-Filter is disabled, Nat is disabled
Bytes In 0, Bytes Out 0

Policy with Priority 1024 is enabled, Direction is outbound
Action permit, Traffic is transit
Logging is disable
Source Address is any, Dest Address is any
Source Port is any, Dest Port is any, any
Schedule is disabled, Ftp-Filter is disabled
Smtp-Filter is disabled, Http-Filter is disabled
Rpc-Filter is disabled, Nat is disabled
Max-Connections 1024, Connection-Rate is disabled
Policing is disabled, Bandwidth is disabled
Bytes In 11258, Bytes Out 5813
```

- 17.** Test the IPSec tunnel between the VPN client and the server by passing traffic from the client to the 10.0.1.0 network.
- 18.** After passing traffic through the tunnel, display the list of clients logged onto the VPN server and the IKE and IPSec SA tables.

```
Router-1# show crypto dynamic clients
Client Address Client Id Policy Advanced
-----
192.168.107.105 david@abc-corp... sales UserGrp
```

```
Router-1# show crypto ike sa all
Policy Peer State Bytes Transform
-----
sales 192.168.107.105 SA_MATURE 1580 pre-g1-3des-sha1
```

```
Router-1# show crypto ike sa all detail
```

```
Crypto Policy name: sales
  Remote ident david@abc-corp.com
  Peer Address is 192.168.107.105
  Transform: 3des, sha1, pre-shared-key
  DH Group: group1
  Bytes Processed 1772
  State is SA_MATURE
  Mode is Aggressive
  Life Time in Sec is unlimited, Life Time in Bytes is
  unlimited
```

```
Router-1# show crypto ipsec sa all
```

Policy	Dest IP	Spi	Bytes	Transform
INsales	172.16.0.1	0xf43c5e3b	360	esp-aes-sha1-tunl
sales	192.168.107.105	0xcfea8435	240	esp-aes-sha1-tunl

```
Router-1# show crypto ipsec sa all detail
```

```
Crypto Policy name: INsales
  Protocol is Any
  Local
  ident(ip/mask/port):(192.168.107.105/255.255.255.255/any)
```

```
Remote ident(ip/mask/port):(10.0.1.0/255.255.255.0/any)
Peer Address is 172.16.0.1, PFS Group is disabled
inbound ESP sas
Spi: 0xf43c5e3b
Transform: aes256(key length=256 bits), sha1
In use settings = {tunnel}
Bytes Processed 360
Hard lifetime in seconds 28780, Hard lifetime in
kilobytes is unlimited
Soft lifetime in seconds 0, Soft lifetime in
kilobytes is unlimited
```

```
Crypto Policy name: sales
  Protocol is Any
  Local ident(ip/mask/port):(10.0.1.0/255.255.255.0/any)
  Remote ident(ip/mask/port):(192.168.107.105/255.255.
  255.255/any)
  Peer Address is 192.168.107.105, PFS Group is
  disabled
```

```

outbound ESP sas
  Spi: 0xcfea8435
  Transform: aes256(key length=256 bits), sha1
  In use settings = {tunnel}
  Bytes Processed 240
  Hard lifetime in seconds 28780, Hard lifetime in
  kilobytes is unlimited
  Soft lifetime in seconds 28690, Soft lifetime in
  kilobytes is unlimited

```

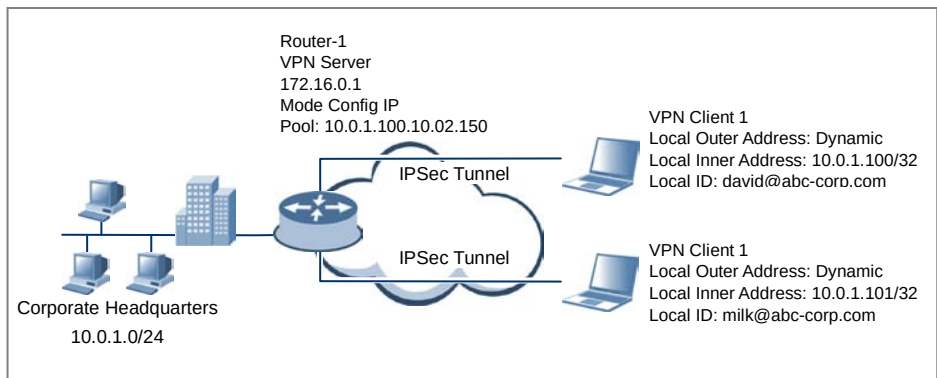
Configuring IPsec Remote Access Example

The following example demonstrates how to configure a router to be an IPsec VPN server using mode-configuration method. The client could be any standard mode configuration enabled IPsec VPN client.

In this example, the client needs to access the corporate private network 10.0.1.0/24 through the VPN tunnel. The server has a pool of ip addresses from 20.1.1.100 through 20.1.1.150 to be allocated for mode configuration enabled VPN clients. The assigned IP address will be used by the VPN client as the source address in the inner IP header. The outer IP header will carry the dynamic IP address assigned by the Internet Service Provider as the source address.

The security requirements are as follows:

- Phase 1: 3DES with SHA1, Mode Configuration
- Phase 2: IPsec ESP tunnel with AES256 and HMAC-SHA1



1. Configure a WAN bundle of network type untrusted.

```
Router-1/configure# interface bundle wan1
Configuring new bundle
Router-1/configure/interface/bundle wan1# link t1 1/1
Router-1/configure/interface/bundle wan1# encapsulation ppp
Router-1/configure/interface/bundle wan1# ip address
172.16.0.1 24
Router-1/configure/interface/bundle wan1# crypto untrusted
Router-1/configure/interface/bundle wan1# exit
```

2. Configure the Ethernet interface with trusted network type.

```
Router-1/configure# interface ethernet 0/1
Configuring existing Ethernet interface
Router-1/configure interface/ethernet(0/1)# ip address
10.0.1.1 24
Router-1/configure/interface/ethernet(0/1)# crypto trusted
Router-1/configure/interface/ethernet(0/1)# exit
```

3. Display the crypto interfaces.

```
Router-1# show crypto interfaces
```

Interface	Network
Name	Type
-----	-----
ethernet 0/1	trusted
wan1	untrusted

4. Configure dynamic IKE policy for a group of mobile users.

```
Router-1/configure# crypto
Router-1/configure/crypto# dynamic
Router-1/configure/crypto/dynamic# ike policy sales modecfg-
group
Router-1/configure/crypto/dynamic/ike/policy sales# local-
address 192.168.55.52
Router-1/configure/crypto/dynamic/ike/policy sales# remote-
id email david@abc-corp.com
```

```
Default proposal created with priority1-des-sha1-pre_shared-g1

Key String has to be configured by the user
Default ipsec proposal 'sales' added with priority1-3des-sha1-tunnel

Router-1/configure/crypto/dynamic/ike/policy sales# remote-id
email mike@abc-corp.com
Router-1/configure/crypto/dynamic/ike/policy sales# key
secretkeyforsales
Router-1/configure/crypto/dynamic/ike/policy sales# proposal 1
Router-1/configure/crypto/dynamic/ike/policy sales/proposal 1#
encryption-algorithm 3des-cbc
Router-1/configure/crypto/dynamic/ike/policy sales/proposal 1#
exit
Router-1/configure/crypto/dynamic/ike/policy sales# client
configuration
Router-1/configure/crypto/dynamic/ike/policy sales/client/
configuration# address-pool 1 20.1.1.100 20.1.1.150
Router-1/configure/crypto/dynamic/ike/policy sales/client/
configuration# exit
Router-1/configure/crypto/dynamic/ike/policy sales# exit
Router-1/configure/crypto/dynamic# exit
```

5. Display dynamic IKE policies.

```
Router-1# show crypto dynamic ike policy all
Policy Remote-id      Mode      Transform
Address-Pool
sales U david@abc-... Aggressive P1 pre-g1-3des-sha1
1 S 20.1.1.100
  E 20.1.1.150
```

6. Display dynamic IKE policies in detail.

```
Router-1# show crypto dynamic ike policy all detail

Policy name sales, Modeconfig group
Aggressive mode, Response Only, PFS is not enabled, Shared
Key is *****
Local addr: 192.168.55.52, Local ident 192.168.55.52
(ip-address)
```

```
Remote idents are david@abc-corp.com(email-id), mike@abc-
corp.comm(email
id)
```

Address Pool:

```
Pool# 1: 20.1.1.100 to 20.1.1.150
```

Proposal of priority 1

```
Encryption algorithm: 3des
```

```
Hash Algorithm: sha1
```

```
Authentication Mode: pre-shared-key
```

```
DH Group: group1
```

```
Lifetime in seconds: 86400
```

```
Lifetime in kilobytes: unlimited
```

7. Configure dynamic IPSec policy for a group of mobile users.

```
Router-1/configure/crypto#
Router-1/configure/crypto# dynamic
Router-1/configure/crypto/dynamic# ipsec policy sales
modecfg-group
Router-1/configure/crypto/dynamic/ipsec/policy sales# match
address 10.0.1.0 24
Router-1/configure/crypto/dynamic/ipsec/policy sales#
proposal 1
Router-1/configure/crypto/dynamic/ipsec/policy
sales/proposal 1#
encryption-algorithm aes256-cbc
Router-1/configure/crypto/dynamic/ipsec/policy
sales/proposal 1#
exit
Router-1/configure/crypto/dynamic/ipsec/policy sales# exit
Router-1/configure/crypto/dynamic# exit
```

8. Display dynamic IPSec policies.

```
Router-1# show crypto dynamic ipsec policy all
```

Policy	Match	Proto	Transform
sales	S 10.0.1.0/24/any D any/any/any	Any	P1 esp-aes-sha1-tunl

9. Display dynamic IPsec policies in detail.

```
Router-1# show crypto dynamic ipsec policy all detail

Policy sales is enabled, Modeconfig Group
Action is Apply
Key Management is Automatic
PFS Group is disabled
Match Address:
  Protocol is Any
  Source ip address(ip/mask/port):(10.0.1.0/255.255.
  255.0/any)
  Destination ip address(ip/mask/port):(any/any/any)

Proposal of priority 1
  Protocol: esp
  Mode: Tunnel
  Encryption Algorithm: aes256(key length=256 bits)
  Hash Algorithm: sha1
  Lifetime in seconds: 3600
  Lifetime in Kilobytes: 4608000
```

10. Configure firewall policies to allow IKE negotiation through untrusted interface.

```
Router-1/configure# firewall internet
Router-1/configure/firewall internet# policy 1000 in service
ike self
Router-1/configure/firewall internet/policy 1000 in# exit
```

11. Display firewall policies in the internet map.

```
Router-1# show firewall policy internet

Advanced: S-Self Traffic, F-Ftp-Filter, H-Http-Filter,
R-Rpc-Filter, N-Nat-Ip/Nat-Pool, L-Logging,
E-Policy Enabled, M-Smtp-Filter

Pri  Dir Source Addr Destination Addr Sport Dport Proto
Action Advanced
-----
1000 in  any    any    ike
1024 out any    any    any    any    PERMIT SE
```

12. Display firewall policies in the internet map in detail.

```
Router-1# show firewall policy internet detail

Policy with Priority 1000 is enabled, Direction is inbound
Action permit, Traffic is self
Logging is disable
Source Address is any, Dest Address is any
Source Port is any, Service Name is ike
Schedule is disabled, Ftp-Filter is disabled
Sntp-Filter is disabled, Http-Filter is disabled
Rpc-Filter is disabled, Nat is disabled
Bytes In 0, Bytes Out 0

Policy with Priority 1024 is enabled, Direction is outbound
Action permit, Traffic is self
Logging is disable
Source Address is any, Dest Address is any
Source Port is any, Dest Port is any, any
Schedule is disabled, Ftp-Filter is disabled
Sntp-Filter is disabled, Http-Filter is disabled
Rpc-Filter is disabled, Nat is disabled
Bytes In 0, Bytes Out 0
```

13. Configure firewall policies for a group of mobile users to allow access to the local LAN.

```
Router-1/configure# firewall corp
Router-1/configure/firewall corp# policy 1000 in address
20.1.1.100 20.1.1.150 10.0.1.0 24
Router-1/configure/firewall corp/policy 1000 in# exit
```



NOTE

The address range in this command typically matches the address range configured in the dynamic IKE policy (see Step 4).

14. Display firewall policies in the corp map.

```
Router-1# show firewall policy corp

Advanced: S-Self Traffic, F-Ftp-Filter, H-Http-Filter,
          R-Rpc-Filter, N-Nat-Ip/Nat-Pool, L-Logging,
          E-Policy Enabled, M-Smtp-Filter

Pri   Dir Source Addr  Destination Addr  Sport Dport Proto
Action Advanced
-----
1000  in  20.1.1.100  10.0.1.0/24      any   any   any
PERMIT E
      20.1.1.150
1022  out any          any              any   any   any
PERMIT SE
1023  in  any          any              any   any   any
PERMIT SE
1024  out any          any              any   any   any
PERMIT E
```

15. Display firewall policies in the corp map in detail.

```
Router-1# show firewall policy corp detail

Policy with Priority 1000 is enabled, Direction is inbound
Action permit, Traffic is transit
Logging is disable
Source Address is 20.1.1.100-20.1.1.150, Dest Address is
10.0.1.0/24

Source Port is any, Dest Port is any, any
Schedule is disabled, Ftp-Filter is disabled
Smtp-Filter is disabled, Http-Filter is disabled
Rpc-Filter is disabled, Nat is disabled
Max-Connections 1024, Connection-Rate is disabled
Policing is disabled, Bandwidth is disabled
Bytes In 0, Bytes Out 0

Policy with Priority 1022 is enabled, Direction is outbound
Action permit, Traffic is self
Logging is disable
Source Address is any, Dest Address is any
Source Port is any, Dest Port is any, any
Schedule is disabled, Ftp-Filter is disabled
Smtp-Filter is disabled, Http-Filter is disabled
Rpc-Filter is disabled, Nat is disabled
Bytes In 0, Bytes Out 0
```

```
Policy with Priority 1023 is enabled, Direction is inbound
Action permit, Traffic is self
Logging is disable
Source Address is any, Dest Address is any
Source Port is any, Dest Port is any, any
Schedule is disabled, Ftp-Filter is disabled
Sntp-Filter is disabled, Http-Filter is disabled
Rpc-Filter is disabled, Nat is disabled
Bytes In 0, Bytes Out 0
```

```
Policy with Priority 1024 is enabled, Direction is outbound
Action permit, Traffic is transit
Logging is disable
Source Address is any, Dest Address is any
Source Port is any, Dest Port is any, any
Schedule is disabled, Ftp-Filter is disabled
Sntp-Filter is disabled, Http-Filter is disabled
Rpc-Filter is disabled, Nat is disabled
Max-Connections 1024, Connection-Rate is disabled
Policing is disabled, Bandwidth is disabled
Bytes In 11258, Bytes Out 5813
```

16. Test the IPSec tunnel between the VPN client and the server by passing traffic from the client to the 10.0.1.0 network.
17. After passing traffic through the tunnel, display the list of clients logged onto the VPN server and the IKE and IPSec SA tables.

```
Router-1# show crypto dynamic clients
Client Address      Client Id           Policy             Advanced
-----
192.168.107.105    david@abc-corp...  sales:20.1.1.1    ModecfgGrp
```

```
Router-1#show crypto ike sa all
Policy Peer State Bytes Transform
-----
sales 192.168.107.105 SA_MATURE 2052 pre-g1-3des-sha1
```

```
Router-1# show crypto ike sa all detail
```

```
Crypto Policy name: sales
Remote   ident david@abc-corp.com
Peer Address is 192.168.107.105
Transform: 3des, sha1, pre-shared-key
DH Group: group1
Bytes Processed 2052
State is SA_MATURE
Mode is Aggressive
Life Time in Sec is unlimited, Life Time in Bytes is
unlimited
```

```
Router-1# show crypto ipsec sa all
```

Policy	Dest IP	Spi	Bytes	Transform
INsales	172.16.0.10xbba97427	840	esp-aes-sha1-tunl	
sales	192.168.107.1050xcb0e23f3	560	esp-aes-sha1-tunl	

```
Router-1# show crypto ipsec sa all
```

Policy	Dest IP	Spi	Bytes	Transform
INsales	172.16.0.1 0xbba97427	840	esp-aes-sha1-tunl	
sales	192.168.107.105 0xcb0e23f3	560	esp-aes-sha1-tunl	

```
Router-1#
```

```
Router-1# show crypto ipsec sa all detail
```

```
Crypto Policy name: INsales
Protocol is Any
Local ident(ip/mask/port):(20.1.1.1/255.255.255.255/any)
Remote ident(ip/mask/port):(10.0.1.0/255.255.255.0/any)
Peer Address is 172.16.0.1, PFS Group is disabled
```

```
inbound ESP sas
```

```
Spi: 0xbba97427
Transform: aes256(key length=256 bits), sha1
In use settings = {tunnel}
Bytes Processed 840
Hard lifetime in seconds 28750, Hard lifetime in
kilobytes is unlimited
Soft lifetime in seconds 0, Soft lifetime in kilobytes
is unlimited
```



```
Crypto Policy name: sales
  Protocol is Any
  Local ident(ip/mask/port):(10.0.1.0/255.255.255.0/any)
  Remote ident(ip/mask/port):(20.1.1.1/255.255.255.255/any)
  Peer Address is 192.168.107.105, PFS Group is disabled

outbound ESP sas
  Spi: 0xcb0e23f3
  Transform: aes256(key length=256 bits), sha1
  In use settings = {tunnel}
  Bytes Processed 560
  Hard lifetime in seconds 28750, Hard lifetime in
  kilobytes is unlimited
  Soft lifetime in seconds 28720, Soft lifetime in
  kilobytes is unlimited
```



This page is intentionally left blank.



CHAPTER 6. SSL VPN Configuration

Overview

Ubigate SSL VPN solution provides a seamless and secure remote-access to a corporate network from any internet-enabled location using a web browser which natively supports SSL encryption.

Applications running inside a corporate network and corporate network resources can be accessed from remote locations by authorized and authenticated party or personnel through a secure connection. Therefore, telecommuters, business partners and customers can access email, files and applications on a company's intranet or within a private local area network. Although the SSL VPN technology is described as clientless, a typical SSL VPN portal consists of Java and/or ActiveX components which are downloaded from the SSL VPN gateway transparently. This makes the SSL VPN a solution to deploy and manage in a simple manner, compared to IPSEC VPN solution which requires IPSec client SW to be carried by clients. Using Ubigate SSL VPN solution, users can connect to the corporate network from Windows OS with Internet Explorer.

Deployment

The SSL VPN is generally, deployed in the demilitarized zone (DMZ), which is a network between the untrusted network (Internet) and a trusted network. It can also be deployed in intranet to provide access to wireless clients and mission critical applications.

SSL VPN Modes

The Ubigate SSL VPN solution has the following three modes of operation:

- Clientless mode
- Port Forwarding mode
- Tunnel Mode

Clientless mode

Clientless mode also known as WebVPN enables remote clients to access to intranet web resources using a web browser such as Internet Explorer and Firefox. This mode also provides access to service like FTP, Telnet, SSH, RDP5, VNC and online collaboration tools, through the web interface. The Secure RDP client allows an exclusive access of administrator-defined windows applications, through the Windows Terminal Service.

This mode is very useful in scenarios, where only a restricted client access environment is preferred.

Port Forwarding mode

Port Forwarding mode also known as Thin-Client SSL VPN extends the capability of the web browser to enable remote access to TCP-based applications. Port Forwarding offers port based tunneling to applications in a transparent way.

This mode can be used in scenarios, where a company wants to hide its internal IP addresses from the VPN clients. The Port Forwarding also supports the hostname aliasing to enable the application access using DNS names.

Notes

1. It only supports applications which use TCP as transport layer on fixed ports.
2. It redirects individual data streams over the Port Forwarding connections. Port Forwarding has a very small footprint and can be installed more quickly.

3. Individual applications and resources such as FTP, Telnet, and SSH configured by the administrator will be available to users.
4. If the SSL VPN client is behind a web proxy or a NAT device, the remote client should choose the java version of the Port Forwarding in the SSL VPN portal, which has proxy transversal support.

Tunnel Mode

Tunnel mode offers extensive application support through its dynamically-downloaded SSL VPN tunnel client. Tunnel client is a software extension that enables remote users to securely establish an IP based tunnel.

Using the Tunnel mode, the SSL VPN users can directly access the corporate network without any limitation and can use diverse types of network applications using TCP/UDP. For instance, a VoIP service can be provided to remote SSL VPN users using the corporate network resources in this mode.

Tunnel mode works in two different ways:

- Split Tunneling
- Full Tunneling

In Split Tunneling, if an SSL VPN user tries to access any server in the public network, then the traffic is directly sent to the internet server. However, if the user tries to access any internal server behind the SSL VPN gateway, then the traffic is tunneled via the SSL VPN tunnel established between the client and the SSL VPN gateway.

On the contrary, in Full Tunneling, all the traffic destined to both public and private networks are tunneled into the SSL VPN gateway, and then the traffic destined to public networks are going out through the corporate gateway. This mode allows the corporate network administrator to perform content filtering and monitoring against traffic incurred by the VPN users.

Configuring SSL VPN Gateway

The SSL VPN gateway acts as a proxy for connections originated from an untrusted network and destined to protected resources. Protected resources are accessed through an SSL-encrypted connection using industry-accepted strong ciphers between the gateway and a web browser on a remote system. The following configuration needs to be executed in order to enable SSL VPN gateway:

Required Steps:

1. Enter the configuration mode.
2. Enter SSL VPN gateway mode.
3. Configure SSL VPN ip address
4. Enable SSL VPN gateway service (using inservice)

Optional Steps:

1. Host name configuration
A fully-qualified domain name can be set for the SSL VPN gateway.
2. WINS server configuration
The windows names can be resolved in the Tunnel mode, by configuring the WINS server.
3. DNS server configuration
The hostnames can be resolved by configuring the DNS server for the SSL VPN gateway.
4. CIFS server configuration
The CIFS file shares can be enabled globally by configuring the CIFS server for the SSL VPN gateway.

5. Trustpoint configuration

A Trustpoint is a representation of a set of digital certificates and the associated certificate authority information. Using this, we can set the SSL VPN gateway to use the required certificate set.

6. Encryption configuration

The encryption algorithms available for the SSL negotiation are set in the SSL VPN gateway.

Step-by-Step Configuration

Step	Command	Purpose
1	Router# configure terminal	Enter the terminal configuration mode
2	Router/configure# ssl-vpn gateway	Enter the SSL VPN gateway configuration mode
3	Router/configure/ssl-vpn/gateway# ip address [gateway address]	Configure SSL VPN gateway proxy ip address
4	Router/configure/ssl-vpn/gateway# hostname [gateway host name]	Configure SSL VPN gateway host name
5	Router/configure/ssl-vpn/gateway# wins_server ip_address [primary-server] {secondary_address [secondary server address]}	Configure Windows Internet Name Service (WINS) servers
6	Router/configure/ssl-vpn/gateway# dns_server ip_address [primary-server] {secondary_address [secondary server address]}	Configure the SSL VPN gateway to resolve the specified fully qualified DNS names through the tunnel
7	Router/configure/ssl-vpn/gateway# cifs_server ip_address [ip address]	Configure the SSL VPN gateway CIFS server
8	Router/configure/ssl-vpn/gateway# trustpoint [selfsignedcert/ or trust point name]	Configure SSL VPN gateway trust point
9	Router/configure/ssl-vpn/gateway# encryption [encryption alg]	Configure the cipher suite for SSL VPN data Encryption/Decryption
10	Router/configure/ssl-vpn/gateway# inservice	Enable SSL VPN gateway
11	Router # show ssl-vpn gateway	Display SSL VPN gateway configuration

Command Examples

The following example shows the commands used to configure SSL VPN gateway.

```
Router# configure terminal
Router/configure# ssl-vpn gateway
Router/configure/ssl-vpn/gateway# ip address 191.1.1.5
Router/configure/ssl-vpn/gateway# hostname securegateway
Router/configure/ssl-vpn/gateway# inservice
Router/configure/ssl-vpn/gateway# wins_server ip_address
107.108.72.58 secondary_address 107.108.72.101
Router/configure/ssl-vpn/gateway# dns_server ip_address
107.108.72.100 secondary-address 107.108.72.110
Router/configure/ssl-vpn/gateway# cifs_server ip_address
10.1.1.100
Router/configure/ssl-vpn/gateway# encryption AES128-SHA
Router/configure/ssl-vpn/gateway# encryption RC4-SHA
Router/configure/ssl-vpn/gateway# encryption DES-CBC-MD5
```



NOTE

One can configure a cipher suite that makes different encryption algorithms available for negotiation, by entering encryption command multiple times with required algorithms.

Configuring Trustpoint

Ubigate SSL VPN solution requires Certificate Authority (CA) information for mutual authentication. Certificate Authority is an entity that issues digital certificates.

Two approaches are supported for trustpoint configuration:

1. Self signed CA
2. Third party CA

Currently the client authentication using digital certificates is only supported in the third party CA approach. It is recommended to use third party CA for higher security and strict regulatory compliance.

Self Signed CA approach

The following example explains configuration of trustpoint by using self signed certificate.

```
Router# configure terminal
Router/configure# crypto
Router/configure/crypto# ca selfsignedcert test-cert
country-code IN state KA organization SISO unit TND ip-
address 191.1.1.5 fqdn samsung.com e-mail test@samsung.com
algo 1 keylen 1
Router/configure/crypto# exit
Router/configure# ssl-vpn gateway
Router/configure/ssl-vpn/gateway# trustpoint selfsignedcert
```

Third party CA approach

The following example shows the commands used to configure a trustpoint using third party CA.

```
Router# configure terminal
Router/configure# crypto
Router/configure/crypto# ca trustpoint test
Router/configure/crypto/ca/trustpoint/test#
Router/configure/crypto/ca/trustpoint test# enrollment
terminal
Router/configure/crypto/ca/trustpoint test# ip-address
191.1.1.1
Router/configure/crypto/ca/trustpoint test# fqdn
rsa1.torpedo6.com
Router/configure/crypto/ca/trustpoint test# email
admin@rsa1.torpedo6.com
Router/configure/crypto/ca/trustpoint test# keypair test rsa
2048
Router/configure/crypto/ca/trustpoint test# exit
```

The following example shows the command used to get the third party CA certificate from third party CA server and import into Ubigate iBG.

```
Router/configure/crypto#
Router/configure/crypto#ca authenticate test
```

The command line console prompts

```
Enter the base 64 encoded CA Certificate

Copy the Root CA certificate
-----BEGIN CERTIFICATE-----
MIIDtTCCAp2gAwIBAgIJAj4LN1KRSk3NMA0GCSqGSIb3DQEBAUAMEUxCzAJ
BgNV
BAYTAKFVMRMwEQYDVQIQIEwpTb21lLVN0YXRlMSEwHwYDVQQKEWhJbnRlcm5l
dCBX
awRnaXRzIFB0eSBMdGQwHhcNMDcwNzI0MjEYODQ2WhcNMDgwNzIzMDQ2
WjBF
MQswCQYDVQQGEwJBVTETMBEGA1UECBMKU29tZS1TdGF0ZTEhMB8GA1UEChMY
SW50
ZXJuZXQgV2lkZ2l0cyBQdHkgTHRkMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8A
MIIB
CgKCAQEA13RhQ0XFZLM73ts2c/B8y4LhYrcYFeCuFd195MH2Tz9ixaxARCD8
glFn
```

```

V8ck7tZz2JFs0qGXQ41jfrR0oJsiedM4wGCaXS0oY0xhz95ZQxkLwa60aUrt
3YvH
gR2Y5lBHNUCfnKAFQZJRPE5libVBYvQmGFjg0XYPFCG7sw0kwwHrjYTB1cCP
0MMg
xCH1Qs50dLlYe40mLooRLPeDyGbnKKILHi1gjG3+kA1wXk5UA8wkDN/oX5x1
x3ZE
eAe2hIRg92WwBskCaSVNHWRr0g9Bw7e1p5PBerqUqvS5KVlbkk5rCa+S3u85
TPGM
NBhlTT475aRbHNNl10euWCEchTwvQIDAQABo4GnMIGkMB0GA1UdDgQWBTR
/EFC
Liw6oP8c4Lmlk5kmwKcInDB1BgNVHSMEbjBsgBTR/EFCLiw6oP8c4Lmlk5km
wKcI
nKFJpEcwRTElMAkGA1UEBhMCVUxEzARBgNVBAgTc1NvbWUtdU3RhdGUxITAf
BgNV
BAoTGEldGVybmV0IFdpZGdpdHMgUHR5IEEx0ZIIJAJ4LN1KRSk3NMAwGA1Ud
EwQF
MAMBAf8wDQYJKoZIhvcNAQEEBQADggEBAAPxHEQ7v1Eg6XgrHB8z99o5AHW5
ALmU
OUP6ws+NPuiVvYwxHC0keGiivG5Y297rm5Q/3vxipkzFKfzj0l6wXV7YtOQN
f9q9
guIDUCC+DEg089HHKDDDD80ryoQx0A7+rxZ1JKzCfRRU9J38qYgBkKmbFs+Bz
cFjX
dTXzPgVzMNI2CGzCUp0jcq/CpILRuuvNVAH9fcI2aDbmXwL3sNEAKKdpoxi
+0s9
uGue0cqWrGdw/ApSeGsMHI1AAPsXj/lg3IB9+MwDCjHwH2BtC5r3VAZJBuKJ
SYdx
IFTZ/AfU9QB+uLY5VHeF5gsz4d5epNmn3j+dUFMsrxMT780UyvErHTo=
-----END CERTIFICATE-----

```

```

CA Certificate has the following attributes
MD5 Fingerprint =
73:36:A6:F8:26:63:DC:44:E9:C6:DE:F0:03:2D:7B:33
CA Certificate imported successfully

```

Generate a Certificate Signing Request and submit it to the Certification Authority and get it signed by the Certification Authority:

```

Router/configure/crypto#
Router/configure/crypto#ca enroll test

```

```

Start certificate enrollment...
The subject name in the certificate will be:
cn=rsa1.torpedo6,ou=tnd,o=samsung,s=suwon,c=kr
The fully-qualified domain name in the certificate will be:
rsa1.torpedo6.com
The Email address in the certificate will be:
admin@rsa1.torpedo6.com
The IP address in the certificate will be: 191.1.1.5

Generating the Certificate Request...
-----BEGIN CERTIFICATE REQUEST-----
MIICzzCCAbcCAQAwVTElMAkGA1UEBhMCa3IxZDJBMBgNVBAGTBXN1d29uMRAw
DgYD
VQKKEwdzYW1zdW5nMQwwCgYDVQQLEWNoYXNjaXJlbnBAMTDXJzYTEudG9y
cGVk
bzYwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDw6Nngs4JhxnSb
AqX1
ZbtAYaMWbqjAq7BmqTx+yIxib4YX6a5MvIg/QhfgDd8GxldqcjEvY0oN9PR1
lbXD
V5+bcj9fK5Btu/R8t262LTs0Mo4AwYuufaCBB0aV4iIbnAEZmmgnC2u6duf1
CwGQ
U7lR5i/rv+BBIY/jD+scF0Ydllnre4P/2dIqo/y6Rq+IsjBbre0dGEXdfMB9
0+hX
CaY0wKBPPn1RKoqFupyFIc0J4+RgybjVk+U/J3mQB40S8ekXUEwJwgfPGILx
C70b
YGYK607xdTzbo8gizv+S9ZwrcpL3TFYS7J9sDmteEsm1VPT2R43WOCF6vUE1
S/1S
QGodAgMBAAGgNTAzBgkqhkiG9w0BCQ4xJjAkMCIGA1UdEQQbMBHBL8BAQWC
EXJz
YTEudG9ycGVkbzYuY29tMA0GCSqGSIb3DQEBAQUAA4IBAQA87mh0sFwq5piv
k3EC
XMRA2PbJAL2mNJR2BXDPq0yyUwF3vZoFuerLn0AzPvxAYKhY82rVAFNKTcP
OATB
bxaRdn04GWS9IQJ0j0jj+NpmN+aiawNEve/CQfS7vEDDepuBGEzrvktbD/sw
vn1Y
qYP7QNZPPNXDy1Khp+NYsNJw72iZ23a5Ihis49d5eBenroubZ0F/P/DEi/Mu
De1/
Q/qsc5FT3czrLevcv2i0+0FiP72geffIAUNFFHGwxflrGRFM6VkJVm/N0gfw
u607
thZfDM0FDHHZyua3YTxfaDiuc4h9njTpu1w/rnc+KzUyUKpeTphVgussT3fY
jwW8
K9QF
-----END CERTIFICATE REQUEST-----

```

The following example shows the commands used to get the Router Certificate from the Certification Authority:

```
Router/configure/crypto#
Router/configure/crypto#ca import test
Router/configure/crypto/ca/import test# router-certificate
Enter the base 64 encoded Router Certificate
-----BEGIN CERTIFICATE-----
MIIDkDCCAnigAwIBAgIBBTANBgkqhkiG9w0BAQUFADBFMQswCQYDVQQGEwJB
VTET
MBEGA1UECBMKU29tZS1TdGF0ZTEhMB8GA1UEChMYSW50ZXJuZXQgV2lkZ2l0
cyBQ
dHkgTHRkMB4XDTA3MDcyNDIxMzIxOFoXDTA4MDCyMzIxMzIxOFowVTElMAKG
A1UE
BhMCA3IxDjAMBgNVBAGTBXN1d29uMRAwDgYDVQQKEwdzYW1zdW5nMQwwCgYD
VQQL
EwN0bmQxYjFjAUBgNVBAMTDXJzYTEudG9ycGVkbzYwggEiMA0GCSqGSIb3DQEB
AQUA
A4IBDwAwggEKAoIBAQDW6Nggs4JhxnSbAqX1ZbtAYaMWBqjAq7BmqTx+yIxi
b4YX
6a5MvIg/QhfgDd8Gxldqcjevy0oN9PRLlbXDV5+bcj9fK5Btu/R8t262LTs0
Mo4A
wYuufaCBB0aV4iIbnAEZmmgnC2u6duf1CwGQU7lR5i/rv+BBiY/jD+scF0Yd
llnr
e4P/2dIqo/y6Rq+IsjBbre0dGEXdfMB90+hxCaY0wKBpPn1RkoqFupyFicOJ
4+Rg
ybjVk+U/J3mQB40S8ekXUEwJwgfPGIlxC70bYGYK607xdTzbo8gizv+S9Zwr
cpl3
TFYS7J9sDmteEsm1VPT2R43W0CF6vUE1S/1SQGodAgMBAAGj ezB5MAKGA1Ud
EwQC
MAAwLAYJYIZIAy b4QgENBB8WHU9wZW5TU0wgr2VuZXJhdGVkIENlcnRpZmlj
YXRl
MB0GA1UdDgQWBBy7SmDjTJsxkt/AXRYLHEL3/1vDjAFBgNVHSMEGDAWgBTR
/EFC
Liw6oP8c4LMlk5kmwKcInDANBgkqhkiG9w0BAQUFAAOCAQEA rPcNmooPC3UV
9zWH
ctawb+PT4Mog00z1NRHmd2XqhXwwBhPLHPLR09XhoWJ0FG+LVtRl0m7HT+90
iqRL
LjzWjobUIvbyCJursPZQdvBd+/AgVT/TRHyYOD7AYMLlpActmmc41wxBXYzn
jys0
IVHvisdhG+Gsj+z5xKS4rDxtZYJEEk++YX9QekD2Fz/dBy0mXlenSpAkxtj
rjox
+6d76qgXyFyLwW4c80hsM/ZrAdVX6vtwQprCU0S2HzZYyZvoQqThUcFf10+M
S9Ch
yz4Z/BuULPGyq3482+Rrfr9zSeYlYeXwyE7lqF27ppSN9y0KeY+RwHNqaz/
WYkc
0pPycA==
-----END CERTIFICATE-----
```

```
Router Certificate imported successfully
Router/configure/crypto/ca/import test# exit
Router/configure/crypto# exit
Router/configure# ssl-vpn gateway
Router/configure/ssl-vpn/gateway#trustpoint test
```

Configuring SSL VPN EPS policy

The End Point Security (EPS) is a pre-authentication verification check for SSL VPN client system environment. A remote client is allowed to access the corporate network using SSL VPN only if the actual client environment meets the requirements in the policies configured by the administrator. The host integrity values are parsed from the SSL VPN client system by the digitally-signed ActiveX code, which is downloaded in to the client system.

End point security helps customers to thwart security threats from unsecure client systems which connect through SSL VPN gateway.

Supported Host integrity values:

1. Operating system: Windows XP, Service Pack 2, Updates enabled for OS
2. Browser: Internet Explorer 6 SP2, Internet Explorer 7
3. Patches: Any patch for OS
4. Register Key: Any register key of any software
5. Antivirus software: McAfee antivirus, Norton antivirus, Norton Internet Security, Kaspersky antivirus, Kaspersky Internet Security, and Trend Micro PC-cillin Internet Security 2007
6. Version check for each anti-virus software supported: Scanning enabled check for each anti-virus supported, Product updates enabled check for each anti-virus supported. Definition version check for each anti-virus supported.

7. Windows XP Firewall: Version check for each firewall supported (except XP firewall), Firewall enabled check for each firewall supported.

Required Steps to configure EPS:

1. Enter the configuration mode.
2. Enter the SSL VPN EPS policy mode
3. Configure policy.
4. Associate EPS policy to group. (Refer Group policies)
5. Enable EPS policy for portal (Refer Portal)

Optional Steps to configure EPS:

1. Configure patch.
2. Configure browser.
3. Configure registry key.
4. Configure antivirus.
5. Configure firewall.

Step-by-Step Configuration:

Step	Command	Purpose
1	Router# configure terminal	Enter the terminal configuration mode
2	Router/configure# ssl-vpn eps-policy test [policy- name]	Enter the SSL VPN EPS policy configuration mode
3	Router/configure/ssl-vpn/eps-policy test# OS WinXP servicePack SP2 enableUpdates 0	Configure policy for Operating System, Service Pack and enable/disable up-to-date verification
4	Router/configure/ssl-vpn/eps-policy test# patch-list	Enter the patch policy configuration mode
5	Router/configure/ssl-vpn/eps-policy test/patch-list# patch [patch-name]	Configure patch policy
6	Router/configure/ssl-vpn/eps-policy test# browser-list	Enter the browser policy configuration mode
7	Router/configure/ssl-vpn/eps-policy test/browser-list# browser [browser-name]	Configure browser patch policy
8	Router/configure/ssl-vpn/eps-policy test# registrykey-list	Enter the registry key policy configuration mode
9	Router/configure/ssl-vpn/eps-policy test/registrykey-list# registrykey [registry-display-name] [registrykey-name] [registrykey-value-name] [registry-value]	Configure policy for registry key by entering display name, registry key name, registry key value name and registry key.
10	Router/configure/ssl-vpn/eps-policy test# antivirus-list	Enter the antivirus policy configuration mode
11	Router/configure/ssl-vpn/eps-policy test/antivirus-list# antivirus [antivirus-type] [antivirus-version] [antivirus-definition version] versioncheck 0/1 definitionversioncheck 0/1 scanningcheck 0/1uptodatecheck 0/1	Configure policy for antivirus by entering antivirus type, version, definition version, enable/disable version verification, enable/disable definition version verification, enable/disable scanning check, enable/disable up-to-date verification
12	Router/configure/ssl-vpn/eps-policy test# firewall-list	Enter the firewall policy configuration mode
13	Router/configure/ssl-vpn/eps-policy test/firewall-list# firewall [firewall-type] [firewall-version] versioncheck 0/1 firewallenablecheck 0/1	Configure policy for firewall by entering firewall type, version, enable/disable version verification and enable/disable firewall enable check

Command Examples

The following example shows the commands used to configure SSL VPN EPS policy.

```
Router# configure terminal
Router/configure# ssl-vpn eps_policy test
Router/configure/ssl-vpn/eps_policy test#OS WinXP
servicePack SP2 enableUpdates 0
Router/configure/ssl-vpn/eps-policy test#browser-list
Router/configure/ssl-vpn/eps-policy test/browser-list#
browser IE6_SP2
Router/configure/ssl-vpn/eps-policy test/browser-list# exit
Router/configure/ssl-vpn/eps-policy test# registrykey-list
Router/configure/ssl-vpn/eps-policy test/registrykey-list#
registrykey Key1
HKEY__LOCAL__MACHINE\SYSTEM\CurrentControlSet\Control
CurrentUser USERNAME
Router/configure/ssl-vpn/eps-policy test/registrykey-list#
exit
Router/configure/ssl-vpn/eps-policy test# antivirus-list
Router/configure/ssl-vpn/eps-policy test/antivirus-list#
antivirus McAfee 11.2 2007/06/20 versioncheck 1
definitionversioncheck 1 scanningcheck 1 updatecheck 1
Router/configure/ssl-vpn/eps-policy test/registrykey-list#
exit
Router/configure/ssl-vpn/eps-policy test# firewall-list
Router/configure/ssl-vpn/eps-policy test/firewall-list#
firewall McAfee 10.0 versioncheck 1 firewallenablecheck 1
```

Configuring SSL VPN Portal

A remote user can access the SSL VPN portal by launching a browser and connecting to the SSL VPN gateway. The remote user must be authenticated successfully in order to get to the SSL VPN portal page.

The user can select one of the services available in the SSL VPN. The administrator can run multiple virtual portals with different access restrictions for different types of users.

The individual portal can be accessed by appending the portal name to the end of the SSL VPN gateway URL. e.g.

https://<ip_address>/portal/<portal_name>



NOTE

Home page for a particular user is provided with the access links corresponding to the features enabled for that user on the SSL VPN gateway.

Required Steps:

1. Enter the configuration mode.
2. Enter the SSL VPN portal mode.

Step-by-Step Configuration:

Step	Command	Purpose
1	Router# configure terminal	Enter the terminal configuration mode
2	Router/configure# ssl-vpn portal [portal name]	Enter the SSL VPN portal configuration mode
3	Router/configure/ssl-vpn/portal Samsung# banner-message [message string]	Add portal banner message
4	Router/configure/ssl-vpn/portal Samsung# banner-title [message]	Add portal banner title
5	Router/configure/ssl-vpn/portal Samsung# site-title [message]	Add portal site title
6	Router/configure/ssl-vpn/portal Samsung# cache-cleaner [flag]	Configure web cache cleaner
7	Router/configure/ssl-vpn/portal Samsung# set-cache [flag]	Configuring service page for portal cache control
8	Router/configure/ssl-vpn/portal Samsung# home-page-title [message]	Set title for home page
9	Router/configure/ssl-vpn/portal Samsung# homepage-msg [message]	Set message for home page
10	Router/configure/ssl-vpn/portal Samsung# enable-eps [flag]	Enable/Disable EPS
11	Router/configure/ssl-vpn/portal Samsung# virtual-host-name [host name]	Add virtual host/domain name

(Continued)

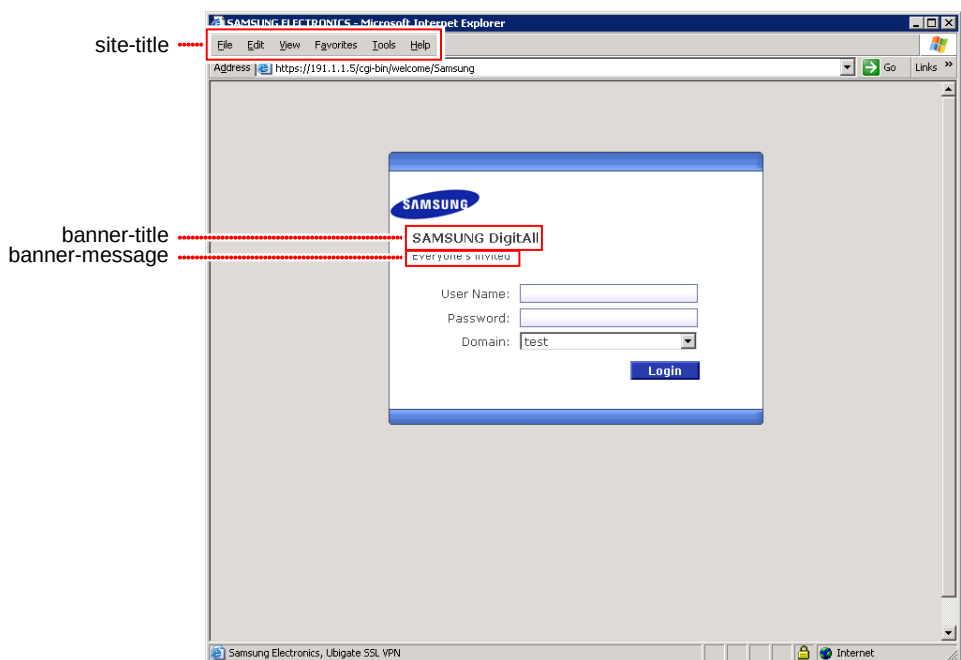
Step	Command	Purpose
12	Router/configure/ssl-vpn/portal Samsung# display-banner-message [message]	Display banner message
13	Router/configure/ssl-vpn/portal Samsung# display-desktop-page [flag]	Display desktop page
14	Router/configure/ssl-vpn/portal Samsung# display-fulltunnel-page [flag]	Display full tunnel page
15	Router/configure/ssl-vpn/portal Samsung# display-home-page [flag]	Display home page
16	Router/configure/ssl-vpn/portal Samsung# display-homepage-msg-flag [flag]	Display home page message flag
17	Router/configure/ssl-vpn/portal Samsung# display-network-place-page [flag]	Display network places page
18	Router/configure/ssl-vpn/portal Samsung# display-online-help [flag]	Display online help page
19	Router/configure/ssl-vpn/portal Samsung# display-portforward-page [flag]	Display port forwarding page
20	Router/configure/ssl-vpn/portal Samsung# display-service-page [flag]	Display service page
21	Router/configure/ssl-vpn/portal Samsung# display-terminal-service- page [flag]	Display terminal service page

The following example shows the commands used to configure SSL VPN portal.

```
Router# configure terminal
Router/configure# ssl-vpn portal Samsung
stylewhitebluegrey
Router/configure/ssl-vpn portal Samsung# banner-message
"Everyone's invited"
Router/configure/ssl-vpn portal Samsung# banner-title
"SAMSUNG DigitAll"
Router/configure/ssl-vpn portal Samsung# cache-cleaner 1
Router/configure/ssl-vpn portal Samsung# display-banner-
message 1
Router/configure/ssl-vpn portal Samsung# display-desktop-
page 1
Router/configure/ssl-vpn portal Samsung# display-fulltunnel-
page 1
Router/configure/ssl-vpn portal Samsung# display-home-page 1
Router/configure/ssl-vpn portal Samsung# display-homepage-
msg-flag 1
Router/configure/ssl-vpn portal Samsung# display-network-
place-page 1
Router/configure/ssl-vpn portal Samsung# display-online-help
1
Router/configure/ssl-vpn portal Samsung# display-
portforward-page 1
Router/configure/ssl-vpn portal Samsung# display-service-
page 1
Router/configure/ssl-vpn/portal Samsung# display-terminal-
service-page 1
Router/configure/ssl-vpn portal Samsung# enable-eps 1
Router/configure/ssl-vpn portal Samsung# home-page-title
"Welcome to SSL VPN portal"
Router/configure/ssl-vpn portal Samsung# homepage-msg
"Explore the world using SSL-VPN"
Router/configure/ssl-vpn portal Samsung# set-cache 1
Router/configure/ssl-vpn portal Samsung# site-title "SAMSUNG
ELECTRONICS "
```

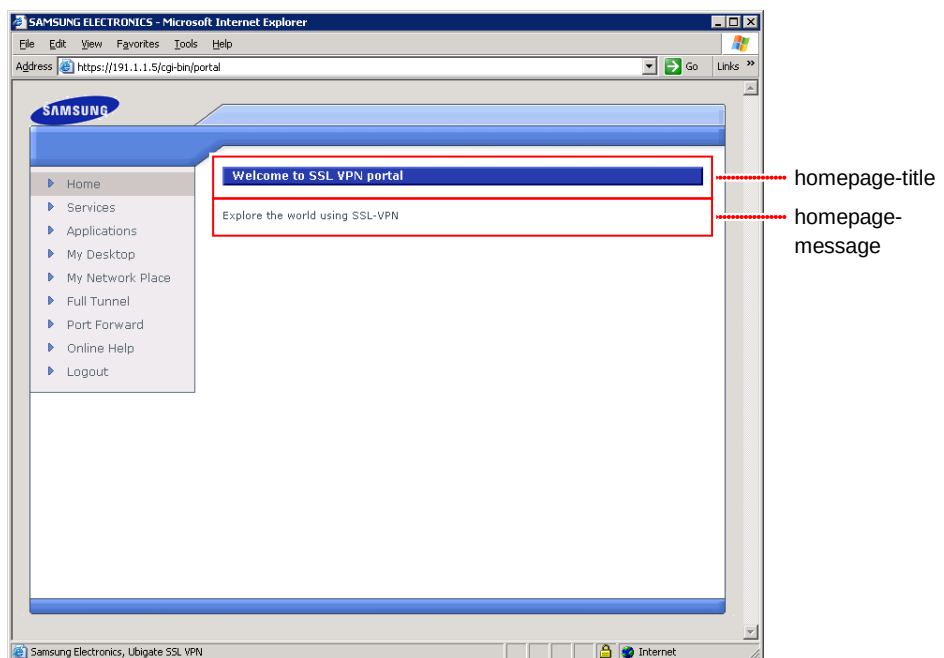
The following example shows the commands used to configure SSL VPN portal **Banner title**, **Site title** and **Banner message**.

```
Router/configure/ssl-vpn portal Samsung# banner-title  
"SAMSUNG DigitAll"  
Router/configure/ssl-vpn portal Samsung# banner-message  
"Everyone's invited"  
Router/configure/ssl-vpn portal Samsung# display-banner-  
message 1  
Router/configure/ssl-vpn portal Samsung# site-title "SAMSUNG  
SECURE NETWORK"
```



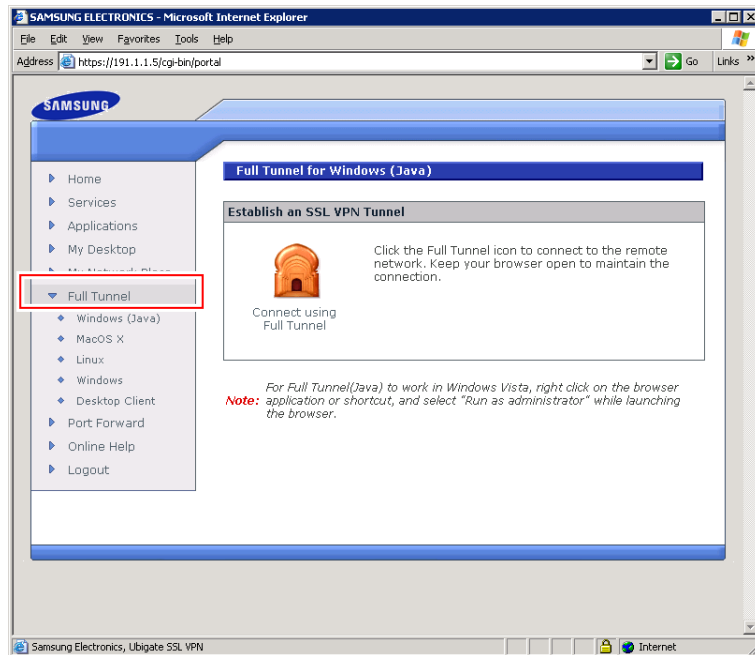
The following example shows the commands used to configure SSL VPN portal **home page** and **home page message**.

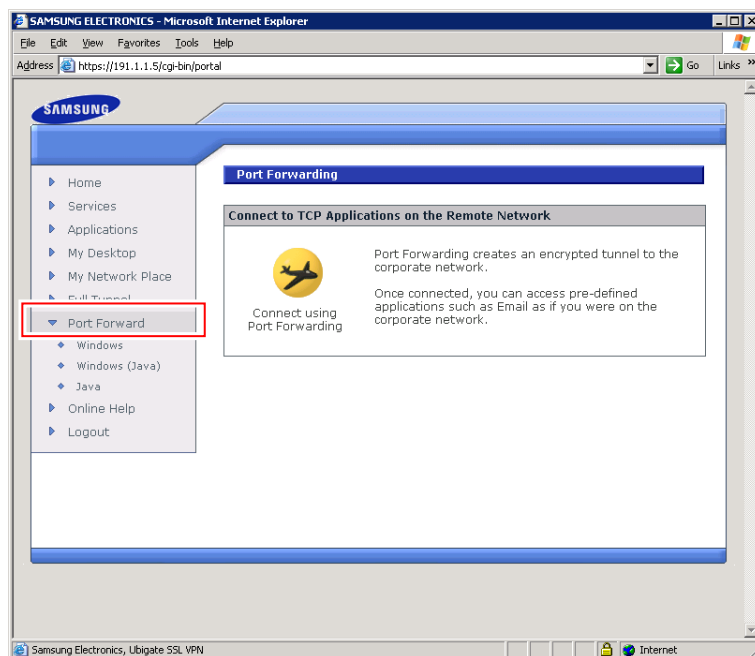
```
Router/configure/ssl-vpn portal Samsung# display-home-page 1
Router/configure/ssl-vpn portal Samsung# home-page-title
"Welcome to SAMSUNG HOME PAGAE"
Router/configure/ssl-vpn portal Samsung# homepage-msg
"Explore the world using SAMSUNG SSL-VPN"
Router/configure/ssl-vpn portal Samsung# display-homepage-
msg-flag 1
```



The following example shows the commands used to configure SSL VPN portal **full tunnel** and **port forwarding** page.

```
Router/configure/ssl-vpn portal Samsung# display-fulltunnel-  
page 1  
Router/configure/ssl-vpn portal Samsung# display-  
portforward-page1
```





Configuring SSL VPN Resource

SSL VPN resources are groups of host names, IP addresses, and IP address range. The most frequently-used server IP addresses and the service ports in the SSL VPN network can be defined in the form of resource objects. This simplifies the policy creation process for the administrator, as the predefined resource object names can be used, while creating multiple firewall policies. User and group policies can be configured to enable/disable access to the resources created.



NOTE

The firewall policies for the Tunnel mode and the Port Forwarding mode can be only configured using the SSL VPN resources.

Required Steps:

1. Enter the configuration mode.
2. Enter the SSL VPN resource mode.

Step-by-Step Configuration

Step	Command	Purpose
1	Router# configure terminal	Enter the terminal configuration mode
2	Router/configure# ssl-vpn resource [service type] [resource name]	Enter the SSL VPN resource configuration mode. In the following steps, we will be configuring a resource with HTTP as the chosen service.
3	Router/configure/ssl-vpn/resource http webserver# addhost [hostname] {port [application port number]}	Resource host name and application port number
4	Router/configure/ssl-vpn/resource http webserver# addipaddr [ipaddress] {port [number/range of numbers]}	Resource ip address
5	Router/configure/ssl-vpn/resource http webserver# addipnetwork [ip address] [mask bits] {[port [application port number]}	Resource ip network address, number of mask bits and application port number

Command Examples

The following example shows the commands used to configure SSL VPN resource.

```
Router# configure terminal
Router/configure# ssl-vpn resource http webserver
Router/configure/ssl-vpn/resource http webserver# addhost
samsung.web.com

Router/configure/ssl-vpn/resource http webserver# addipaddr
191.2.3.4
Router/configure/ssl-vpn/resource http webserver# addipaddr
191.2.3.4 port 23
Router/configure/ssl-vpn/resource http webserver# addipaddr
191.2.3.4 port 20-40
```

```
Router/configure/ssl-vpn/resource http webserver#  
addipnetwork 191.2.3.0 24  
Router/configure/ssl-vpn/resource https appacheserver#  
addhost 10.1.1.100  
Router/configure/ssl-vpn/resource https appacheserver#  
addhost 10.1.1.100 443  
Router/configure/ssl-vpn/resource https appacheserver#  
addipnetwork 10.1.1.0 24 443
```

Configuring SSL VPN Domain

The SSL VPN domain defines the virtual instances of authentication and policy configuration of the SSL VPN system.



NOTE

Maximum 8 domains can be configured for the system.

Required Steps:

1. Enter the configuration mode.
2. Enter SSL VPN domain mode by associating domain with authentication method.
3. Configure max concurrent users per domain.
4. Enter the group mode to configure group parameters.

Optional Steps:

1. Enable client certificate verification flag.
2. Associate domain with customized portal.

Step-by-Step Configuration

Step	Command	Purpose
1	Router# configure terminal	Enter the terminal configuration mode
2	Router/configure# ssl-vpn domain [domain name] authType [authentication type]	Enter the SSL VPN domain configuration Mode, associate domain with authentication method
3	Router/configure/ssl-vpn/domain Samsung authType localusrd# max_concurrent_users [integer 0-50]	Configure the maximum concurrent users for the domain
4	Router/configure/ssl-vpn/domain Samsung authType localusrd# group [group name]	Enter the SSL VPN domain group configuration mode
5	Router/configure/ssl-vpn/domain Samsung authType localusrd# cert_verify [integer 0-1]	Enable/Disable client certificate verification
6	Router/configure/ssl-vpn/domain Samsung authType localusrd# portal [portal name]	Associate the domain with customized portal

**NOTE**

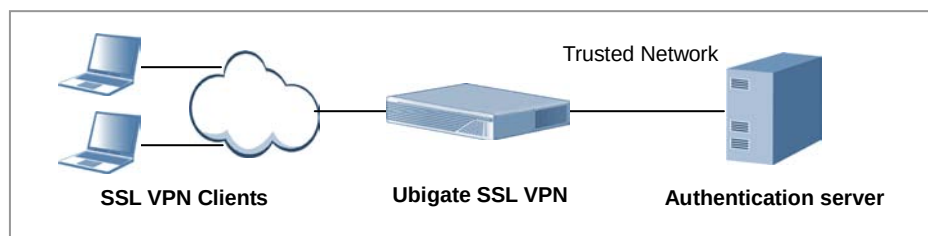
Total concurrent users for all the configured domains shall not exceed the licensed maximum number of concurrent users.

A newly created domain will have maximum concurrent users as zero, by default. The SSL VPN administrator can scale the concurrent users in the newly created domain as per the IT requirements.

Command Examples

The following example shows the commands used to configure SSL VPN domain with local user database authentication.

```
Router# configure terminal
Router/configure# ssl-vpn domain Samsung authType localusrdp
Router/configure/ssl-vpn/domain Samsung authType localusrdp#
max_concurrent_users 10
Router/configure/ssl-vpn/domain Samsung authType localusrdp#
portal Samsung
Router/configure/ssl-vpn/domain Samsung authType localusrdp#
cert_verify 1
Router/configure/ssl-vpn/domain Samsung authType localusrdp#
group devgroup
Router/configure/ssl-vpn/domain Samsung authType localusrdp/
group devgroup#
```



The following example shows the commands used to configure SSL VPN domain with radius authentication.

```
Router# configure terminal
Router/configure# aaa
Router/configure/aaa# radius
Router/configure/aaa/radius# primary_server 10.10.1.1
Router/configure/aaa/radius# shared_key
samsungradiusauthentication
Router/configure/aaa/radius# exit
Router/configure/aaa# exit
Router/configure# ssl-vpn domain Samsung-1 authType
radiusmschapv2
Router/configure/ssl-vpn/domain Samsung-1/authType
radiusmschapv2#
```

Configure rest of the parameters as shown in the above example.

Configuring Groups within SSL VPN Domain

A single SSL VPN domain can contain multiple groups in it.



Maximum 4 groups can be configured per domain.

Required Steps:

1. Enter the configuration mode.
2. Enter the SSL VPN domain mode.
3. Enter the SSL VPN domain group mode.
4. Configure group name.
5. Configure group users.

Optional Steps:

1. Inactive timeout value configuration for the group.
2. Policy configuration for the group.
3. EPS policy association with group.
4. Bookmark configuration for the group.

Step-by-Step Configuration

Step	Command	Purpose
1	Router# configure terminal	Enter the terminal configuration mode
2	Router/configure# ssl-vpn domain [domain name] authType [authentication type]	Enter the SSL VPN domain configuration mode
3	Router/configure/ssl-vpn/domain Samsung authType localusrdb# group [group name]	Enter the SSL VPN domain group configuration mode
4	Router/configure/ssl-vpn/domain Samsung authType localusrdb/ group devgroup# inactive_time[0-999 min]	Configure the group inactive timeout value
5	Router/configure/ssl-vpn/domain Samsung authType localusrdb/ group devgroup# user [user name]	Enter the SSL VPN group user configuration mode
6	Router/configure/ssl-vpn/domain Samsung authType localusrdb/ group devgroup# policy	Enter the SSL VPN domain group policy configuration mode
7	Router/configure/ssl-vpn/domain Samsung authType localusrdb/ group devgroup# eps-policy [eps policy name]	Associate group with the existing eps policy
8	Router/configure/ssl-vpn/domain Samsung authType localusrdb/ group devgroup# group-bookmark	Enter the SSL VPN domain group group-bookmark configuration mode.

Command Examples

The following example shows the commands used to configure SSL VPN group.

```
Router# configure terminal
Router/configure# ssl-vpn domain Samsung authType localusrdb
Router/configure/ssl-vpn/domain Samsung authType localusrdb#
group devgroup
Router/configure/ssl-vpn/domain Samsung authType localusrdb/
group devgroup# inactive_time 10
Router/configure/ssl-vpn/domain Samsung authType localusrdb/
group devgroup# eps_policy test
```

```
Router/configure/ssl-vpn/domain Samsung authType localusrdp/  
group devgroup#user John  
Router/configure/ssl-vpn/domain Samsung authType  
localusrdp/group devgroup/user John# exit  
Router/configure/ssl-vpn/domain Samsung authType  
localusrdp/group devgroup# policy  
Router/configure/ssl-vpn/domain Samsung authType  
localusrdp/group devgroup/policy# exit  
Router/configure/ssl-vpn/domain Samsung authType  
localusrdp/group devgroup# group-bookmark  
Router/configure/ssl-vpn/domain Samsung authType  
localusrdp/group devgroup/group-bookmark# exit
```

Configuring Group Policies

The SSL VPN group policy creates network access restrictions for the group. Administrator can provide or restrict access to VPN network resources by configuring group policies.

In SSL VPN, policies can be defined based on the following criteria:

- Client IP address
- IP address range
- All client IP addresses
- Resources (like telnet, ftp, web servers).

Required Steps:

1. Enter the configuration mode.
2. Enter the SSL VPN domain mode.
3. Enter the SSL VPN domain group mode.
4. Enter the SSL VPN domain group policy mode.

Step-by-Step Configuration:

Step	Command	Purpose
1	Router# configure terminal	Enter the terminal configuration mode
2	Router/configure# ssl-vpn domain [domain name] authType [authentication type]	Enter the SSL VPN domain configuration mode
3	Router/configure/ssl-vpn/domain Samsung authType localusrdb# group [group name]	Enter the SSL VPN domain group configuration mode
4	Router/configure/ssl-vpn/domain Samsung authType localusrdb/ group devgroup# policy	Enter the SSL VPN domain group policy configuration mode
5	Router/configure/ssl-vpn/domain Samsung authType localusrdb/ group devgroup/policy# all_ip_address [policy name] [Policy Priority 1-1024] [service type] [policy action]	Configure the group policy on all client ip address
6	Router/configure/ssl-vpn/domain Samsung authType localusrdb/ group devgroup/policy# ip_address [policy name] [Policy Priority 1-1024] [ip address][service type][policy action]	Configure the group policy on a client ip address
7	Router/configure/ssl-vpn/domain Samsung authType localusrdb/ group devgroup/policy# ip_address_range [policy name] [Policy Priority 1-1024] [ip address][network mask][service type][policy action]	Configure the group policy on a client ip address range
8	Router/configure/ssl-vpn/domain Samsung authType localusrdb/ group devgroup/ policy# resource_name [policy name] [Policy Priority 1-1024] [resource name] [policy action]	Configure the group policy using already configured SSL VPN resource

Command Examples

The following example shows the commands used to configure SSL VPN group policies.

```
Router# configure terminal
Router/configure# ssl-vpn domain Samsung authType localusrdB
Router/configure/ssl-vpn/domain Samsung authType localusrdB#
group devgroup
Router/configure/ssl-vpn/domain Samsung authType localusrdB
group devgroup# policy
Router/configure/ssl-vpn/domain Samsung authType localusrdB/
group devgroup/policy# all_ip_address telnetpolicy 1 Telnet
deny
Router/configure/ssl-vpn/domain Samsung authType
localusrdB/group devgroup/policy# ip_address ftppolicy 2
10.1.1.1 FTP permit
Router/configure/ssl-vpn/domain Samsung authType
localusrdB/group devgroup/policy# ip_address_range
webserverpolicy 3 10.1.1.0 32 HTTP permit
Router/configure/ssl-vpn/domain Samsung authType
localusrdB/group devgroup/policy# resource_name secure-
policy 4 server-Newtons deny
```

Configuring SSL VPN Users within a Group

SSL VPN group can contain multiple users in it.



NOTE

Maximum 50 users can be configured per group.

Required Steps:

1. Enter the configuration mode.
2. Enter the SSL VPN domain mode.
3. Enter the SSL VPN domain group mode.
4. Enter the SSL VPN domain group user mode.

5. Configure username.

6. Configure password.

Optional Steps:

1. User timeout value configuration.

2. User policy configuration.

3. User bookmark configuration.

Step-by-Step Configuration

Step	Command	Purpose
1	Router# configure terminal	Enter the terminal configuration mode
2	Router/configure# ssl-vpn domain [domain name] authType [authentication type]	Enter the SSL VPN domain configuration mode
3	Router/configure/ssl-vpn/domain Samsung authType localusrdb# group [group name]	Enter the SSL VPN domain group configuration mode
4	Router/configure/ssl-vpn/domain Samsung authType localusrdb/ group devgroup# user [user name]	Enter the SSL VPN domain group user configuration mode
5	Router/configure/ssl-vpn/domain Samsung authType localusrdb/ group devgroup/user John# inactive_time[0- 999 min]	Configure the User timeout value
6	Router/configure/ssl-vpn/domain Samsung authType localusrdb/ group devgroup/user John # password <password>	Configures password for the SSL VPN user
7	Router/configure/ssl-vpn/domain Samsung authType localusrdb/ group devgroup/user John # user-bookmark	Configures user-bookmark for the SSL VPN user

Command Examples

The following example shows the commands used to configure SSL VPN user.

```
Router# configure terminal
Router/configure# ssl-vpn domain Samsung authType localusrdb

Router/configure/ssl-vpn/domain Samsung authType localusrdb#
group devgroup
Router/configure/ssl-vpn/domain Samsung authType localusrdb
group devgroup# user John
Router/configure/ssl-vpn/domain Samsung authType localusrdb/
group devgroup/user John# inactive_time 10
Router/configure/ssl-vpn/domain Samsung authType localusrdb/
group devgroup/user John# password complex-password
Router/configure/ssl-vpn/domain Samsung authType localusrdb/
group devgroup/user John# user-bookmark
Router/configure/ssl-vpn/domain Samsung authType localusrdb/
group devgroup/user John/ user-bookmark # exit
```

Configuring SSL VPN Group Bookmark

The most frequently used clientless mode services like RDP, VNC, HTTP, HTTPS, Telnet, FTP and SSH can be bookmarked in form of shortcut links in the SSLVPN portal. The administrator can configure bookmarks, which will be available to all users of group.

Required Steps:

1. Enter the configuration mode.
2. Enter the SSL VPN domain mode.
3. Enter the SSL VPN domain group mode.
4. Enter the SSL VPN domain group group-bookmark mode.
5. Configure the required services for bookmarking.

Step-by-Step Configuration

Step	Command	Purpose
1	Router# configure terminal	Enter the terminal configuration mode.
2	Router/configure# ssl-vpn domain [domain name] authType [authentication type]	Enter the SSL VPN domain configuration mode
3	Router/configure/ssl-vpn/domain Samsung authType localusrdb# group [group name]	Enter the SSL VPN domain group configuration mode
4	Router/configure/ssl-vpn/domain Samsung authType localusrdb/ group devgroup # group-bookmark	Enter the SSL VPN domain group group-bookmark configuration mode.
5	Router/configure/ssl-vpn/domain Samsung authType localusrdb/group devgroup /group-bookmark# desktop- bookmark-rdp [bookmark name] [ip address] [screen-size]	Configure the desktop RDP as a group bookmark.
6	Router/configure/ssl-vpn/domain Samsung authType localusrdb/group devgroup /group-bookmark# desktop- bookmark-vnc [bookmark name] [ip address]	Configure the desktop VNC as a group bookmark.
7	Router/configure/ssl-vpn/domain Samsung authType localusrdb/group devgroup /group-bookmark# service- bookmark [bookmark name] [ip address] [service-type]	Configure the services(ftp, http, https, ssh and telnet) as a service bookmark.

Command Examples

The following example shows the commands used to configure SSL VPN Group Bookmark.

```
Router# configure terminal
Router/configure# ssl-vpn domain Samsung authType localusrdb
Router/configure/ssl-vpn/domain Samsung authType localusrdb#
group devgroup
Router/configure/ssl-vpn/domain Samsung authType localusrdb#
group devgroup# group-bookmark
```

```

Router/configure/ssl-vpn/domain Samsung authType localusrd#
group devgroup/group-bookmark# desktop-bookmark-rdp RDP
10.1.1.1 800x600
Router/configure/ssl-vpn/domain Samsung authType localusrd#
group devgroup/group-bookmark# desktop-bookmark-vnc VNC
10.1.1.1
Router/configure/ssl-vpn/domain Samsung authType localusrd#
group devgroup/group-bookmark# service-bookmark HTTP
10.1.1.1 http

```

Configuring User Policies

Required Steps:

1. Enter the configuration mode.
2. Enter the SSL VPN domain mode.
3. Enter the SSL VPN domain group mode.
4. Enter the SSL VPN domain group user mode.
5. Enter the SSL VPN domain group user policy mode.

Step-by-Step Configuration

Step	Command	Purpose
1	Router# configure terminal	Enter the terminal configuration mode
2	Router/configure# ssl-vpn domain [domain name] authType [authentication type]	Enter the SSL VPN domain configuration mode
3	Router/configure/ssl-vpn/domain Samsung authType localusrd# group [group name]	Enter the SSL VPN domain group configuration mode
4	Router/configure/ssl-vpn/domain Samsung authType localusrd# group devgroup# user [user name]	Enter the SSL VPN domain group user configuration mode

(Continued)

Step	Command	Purpose
5	Router/configure/ssl-vpn/domain Samsung authType localusrdb/ group devgroup/user John# policy	Enter the SSL VPN domain group user policy configuration mode
6	Router/configure/ssl-vpn/domain Samsung authType localusrdb/ group devgroup/policy/user John# all_ip_address [policy name] [Policy Priority 1-1024] [service type] [policy action]	Configure the user policy on all client ip address
7	Router/configure/ssl-vpn/domain Samsung authType localusrdb/ group devgroup/policy/user John# ip_address [policy name] [Policy Priority 1-1024] [ip address][service type][policy action]	Configure the user policy on a client ip address
8	Router/configure/ssl-vpn/domain Samsung authType localusrdb/ group devgroup/policy /user John# ip_address_range [policy name] [Policy Priority 1-1024] [ip address][network mask][service type][policy action]	Configure the user policy on a client ip address range
9	Router/configure/ssl-vpn/domain Samsung authType localusrdb/ group devgroup/policy/user John# resource_name [policy name] [Policy Priority 1-1024] [resource name] [policy action]	Configure the user policy on configured SSL VPN resource

Command Examples

The following example shows the commands used to configure SSL VPN user policies.

```
Router# configure terminal
Router/configure# ssl-vpn domain Samsung authType localusrd
Router/configure/ssl-vpn/domain Samsung authType localusrd
group devgroup
Router/configure/ssl-vpn/domain Samsung authType localusrd
group devgroup# user John
Router/configure/ssl-vpn/domain Samsung authType localusrd
group devgroup/user John/policy# all_ip_address telnetpolicy
5 Telnet permit
Router/configure/ssl-vpn/domain Samsung authType
localusrd/group devgroup/user John/policy# ip_address
ftppolicy 6 10.1.1.1 FTP permit
Router/configure/ssl-vpn/domain Samsung authType
localusrd/group devgroup/user John/policy# ip_address_range
webserverpolicy 7 10.1.1.0 32 http permit
Router/configure/ssl-vpn/domain Samsung authType
localusrd/group devgroup/user John/policy# resource_name
secure-policy 100 server-Einstein deny
```

Configuring User Login Policies

Required Steps:

1. Enter the configuration mode.
2. Enter the SSL VPN domain mode.
3. Enter the SSL VPN domain group mode.
4. Enter the SSL VPN domain group user mode.
5. Enter the SSL VPN domain group user login-policy mode.

Step-by-Step Configuration

Step	Command	Purpose
1	Router# configure terminal	Enter the terminal configuration mode
2	Router/configure# ssl-vpn domain [domain name] authType [authentication type]	Enter the SSL VPN domain configuration mode
3	Router/configure/ssl-vpn/domain Samsung authType localusrdb# group [group name]	Enter the SSL VPN domain group configuration mode
4	Router/configure/ssl-vpn/domain Samsung authType localusrdb/ group devgroup# user [user name]	Enter the SSL VPN domain group user configuration mode
5	Router/configure/ssl-vpn/domain Samsung authType localusrdb/ group devgroup/ user John# login-policy	Enter the SSL VPN domain group user login-policy configuration mode
6	Router/configure/ssl-vpn/domain Samsung authType localusrdb/ group devgroup/ user John# login-policy# browse_access_policy [policy action]	Allow/Deny the SSL VPN domain group user to login from the configured browser.
7	Router/configure/ssl-vpn/domain Samsung authType localusrdb/ group devgroup/user John# login-policy# browser [browser type]	Configure the user login policy on browser type for SSL VPN domain group user.

(Continued)

Step	Command	Purpose
8	Router/configure/ssl-vpn/domain Samsung authType localusrdb/ group devgroup/ user John# login-policy# ip_access_policy [policy action]	Allow/deny the SSL VPN domain group user to login from the configured ip address or from ip network
9	Router/configure/ssl-vpn/domain Samsung authType localusrdb/ group devgroup/ user John# login-policy# ip_address [ip address]	Configure the user login policy on ip address type for SSL VPN domain group user.
10	Router/configure/ssl-vpn/domain Samsung authType localusrdb/ group devgroup/ user John# login-policy# ip_network [ip address] [subnet mask 0-32]	Configure the user login policy on ip network type for SSL VPN domain group user.
11	Router/configure/ssl-vpn/domain Samsung authType localusrdb/ group devgroup/ user John# login-policy# login_disable	Disable the login for SSL VPN domain group user
12	Router/configure/ssl-vpn/domain Samsung authType localusrdb/ group devgroup/ user John# login-policy# require_user_client_cert	Enable the require client certificate for login for SSL VPN domain group user.

Command Examples

The following example shows the commands used to configure SSL VPN user login policies.

```
Router# configure terminal
Router/configure# ssl-vpn domain Samsung authType localusrdb
Router/configure/ssl-vpn/domain Samsung authType localusrdb#
group devgroup
Router/configure/ssl-vpn/domain Samsung authType localusrdb
group devgroup# user John
Router/configure/ssl-vpn/domain Samsung authType
localusrdb/group devgroup/user John# login-policy
Router/configure/ssl-vpn/domain Samsung authType
localusrdb/group devgroup/user John/login-policy#
browse_access_policy allow
```

```
Router/configure/ssl-vpn/domain Samsung authType
localusrdB/group devgroup/user John/login-policy# browser IE
Router/configure/ssl-vpn/domain Samsung authType
localusrdB/group devgroup/user John/login-policy#
ip_access_policy deny
Router/configure/ssl-vpn/domain Samsung authType
localusrdB/group devgroup/user John/login-policy# ip_address
10.1.1.1
Router/configure/ssl-vpn/domain Samsung authType
localusrdB/group devgroup/user John/login-policy# ip_network
10.1.1.0 24
Router/configure/ssl-vpn/domain Samsung authType
localusrdB/group devgroup/user John/login-policy#
login_disable
Router/configure/ssl-vpn/domain Samsung authType
localusrdB/group devgroup/user John/login-policy#
require_user_client_cert
```

Configuring SSL VPN User Bookmark

The most frequently used clientless mode services like RDP, VNC, HTTP, HTTPS, Telnet, FTP and SSH can be bookmarked in form of shortcut links in the SSLVPN portal. The administrator can configure bookmarks, which will be available to particular user.

Required Steps:

1. Enter the configuration mode.
2. Enter the SSL VPN domain mode.
3. Enter the SSL VPN domain group mode.
4. Enter the SSL VPN domain group user mode.
5. Enter the SSL VPN domain group user user-bookmark mode
6. Configure the required services for bookmarking.

Step-by-Step Configuration

Step	Command	Purpose
1	Router# configure terminal	Enter the terminal configuration mode.
2	Router/configure# ssl-vpn domain [domain name] authType [authentication type]	Enter the SSL VPN domain configuration mode
3	Router/configure/ssl-vpn/domain Samsung authType localusrdb# group [group name]	Enter the SSL VPN domain group configuration mode
4	Router/configure/ssl-vpn/domain Samsung authType localusrdb/ group devgroup # user [user-name]	Enter the SSL VPN domain group user configuration mode.
5	Router/configure/ssl-vpn/domain Samsung authType localusrdb /group devgroup/ user John# user-bookmark	Enter the SSL VPN domain group user user-bookmark configuration mode.
6	Router/configure/ssl-vpn/domain Samsung authType localusrdb/group devgroup / user John/ user-bookmark # desktop-bookmark-rdp [bookmark name] [ip address] [screen-size]	Configure the desktop RDP as a user bookmark.
7	Router/configure/ssl-vpn/domain Samsung authType localusrdb/group / user John/ user-bookmark # desktop- bookmark-vnc [bookmark name] [ip address]	Configure the desktop VNC as a user bookmark.
8	Router/configure/ssl-vpn/domain Samsung authType localusrdb/group devgroup / user John/ user-bookmark # service-bookmark [bookmark name] [ip address] [service-type]	Configure the services(ftp, http, https, ssh and telnet) as a service bookmark.

Command Examples

The following example shows the commands used to configure SSL VPN User Bookmark.

```
Router# configure terminal
Router/configure# ssl-vpn domain Samsung authType localusrdb
Router/configure/ssl-vpn/domain Samsung authType localusrdb#
group devgroup
Router/configure/ssl-vpn/domain Samsung authType localusrdb#
group devgroup# user John
Router/configure/ssl-vpn/domain Samsung authType localusrdb#
group devgroup# user John# user-bookmark
Router/configure/ssl-vpn/domain Samsung authType localusrdb#
group devgroup/ user John/ user-bookmark # desktop-bookmark-
rdp RDP 10.1.1.1 800x600
Router/configure/ssl-vpn/domain Samsung authType localusrdb#
group devgroup/ user John/ user-bookmark # desktop-bookmark-
vnc VNC 10.1.1.1
Router/configure/ssl-vpn/domain Samsung authType localusrdb#
group devgroup/ user John/ user-bookmark # service-bookmark
HTTP 10.1.1.1 http
```

Configuring SSL VPN Clientless mode

The Clientless mode will provide access to the network services using web browser, eliminating the need for downloading the VPN client. This mode can be used for very restricted computing environments like Kiosk etc.

The services like HTTP, HTTPS, FTP, VNC, TELNET, SSH and Terminal Services can be enabled for clientless access through a web browser.

Required Steps:

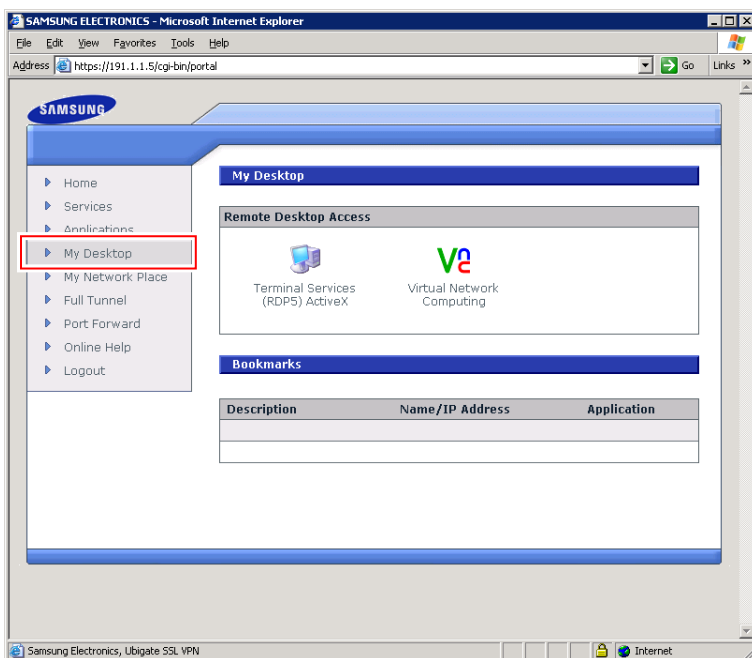
1. Enter the configuration mode.
2. Enter the SSL VPN portal mode.

Step-by-Step Configuration:

Step	Command	Purpose
1	Router/configure/ssl-vpn portal Samsung# desktop-page-terminal- service-activex-flag [flag]	Configure desktop page for Terminal service ActiveX
2	Router/configure/ssl-vpn/portal Samsung# desktop-page-vnc-flag [flag]	Configure desktop page for VNC
3	Router/configure/ssl-vpn/portal Samsung# http-proxy [flag]	Configuring service page for HTTP proxy
4	Router/configure/ssl-vpn/portal Samsung# https-proxy [flag]	Configuring service page for HTTPS proxy
5	Router/configure/ssl-vpn/portal Samsung# ftp-service [flag]	Configuring service page for FTP
6	Router/configure/ssl-vpn/portal Samsung# ssh-service [flag]	Configuring service page for SSH
7	Router/configure/ssl-vpn portal Samsung# telnet-service 1	Configure service page for Telnet
8	Router/configure/ssl-vpn/portal Samsung# add-service-application [application name] ["application path"] ["application working dir"] [icon type][host address]	To add a terminal service application to the SSL VPN

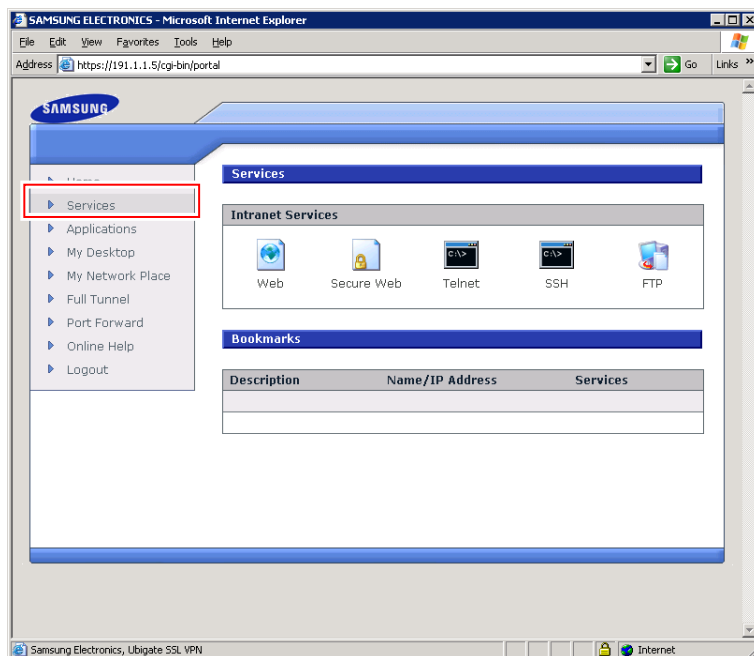
The following example shows the commands used to configure SSL VPN portal **desktop** page.

```
Router/configure/ssl-vpn portal Samsung# desktop-page-vnc-flag 1
Router/configure/ssl-vpn portal Samsung# desktop-page-terminal-service-activex-flag 1
```



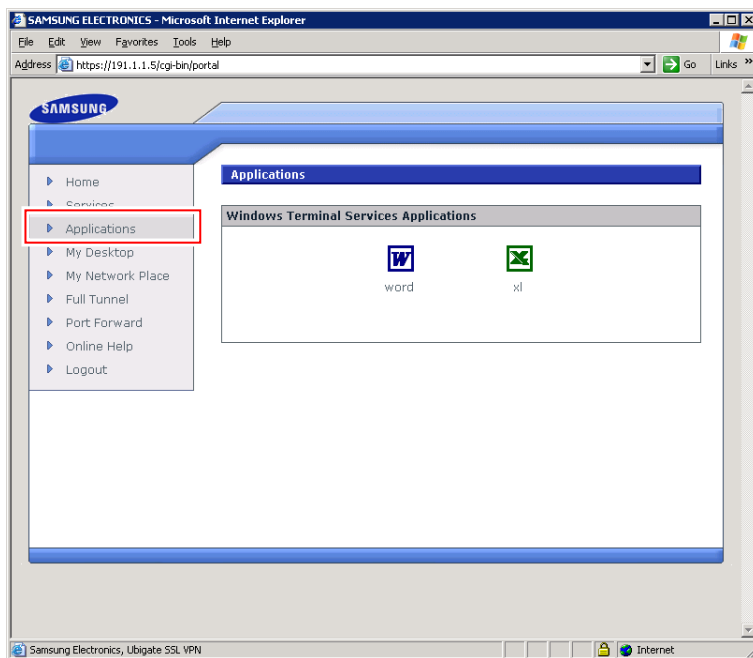
The following example shows the commands used to configure SSL VPN clientless services.

```
Router/configure/ssl-vpn portal Samsung# https-proxy 1
Router/configure/ssl-vpn portal Samsung# http-proxy 1
Router/configure/ssl-vpn portal Samsung# telnet-service 1
Router/configure/ssl-vpn portal Samsung# ftp-service 1
Router/configure/ssl-vpn portal Samsung# ssh-service 1
```



The following example shows the commands used to configure SSL VPN portal **applications** page.

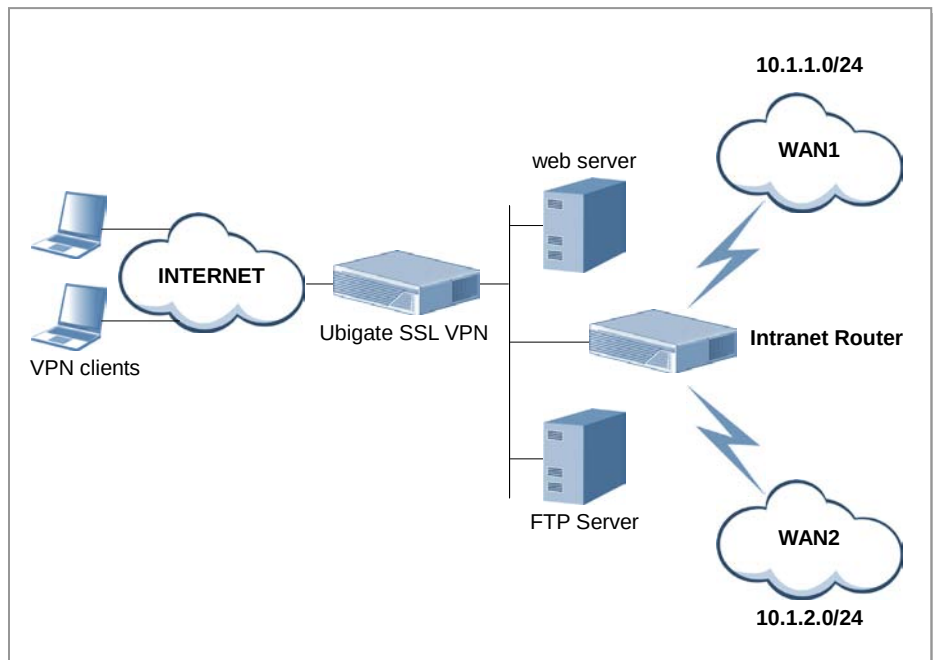
```
Router/configure/ssl-vpn portal Samsung# add-service-  
application word "C:\Program Files\Microsoft  
Office\OFFICE11\WINDOWRD" "D:\SECUREDATA\word files"  
wordicon  
Router/configure/ssl-vpn portal Samsung# add-service-  
application xl "C:\Program Files\Microsoft  
Office\OFFICE11\EXCEL" "D:\SECUREDATA\exel files" excelicon  
10.1.11.1
```



Configuring SSL VPN Tunnel mode

Many complex network applications such as VoIP, DCOM, and NFS use a bidirectional traffic flow model and uses dynamic ports for communication. These applications fail to work in conventional SSL VPN modes like Clientless mode and Port Forward mode.

In order to support those complex network applications, the tunnel mode is made available in the Ubigate SSL VPN solution. The functionality is achieved using a virtual dialup adapter interface. During tunnel setup, a virtual network interface is configured automatically for a remote user, and a dynamic IP address is assigned to the virtual network interface. Administrator should configure the IP address range used for this purpose.



NOTE

Split Tunneling is used in the SSL VPN gateway by default.

Client routes should be configured in the SSL VPN gateway, to allow the VPN clients to access networks, other than the corporate network, e.g., VLANs or WAN sites behind a router. In the above network topology, for the VPN clients to access network resources in WAN1 and WAN2, the static routes should be added in the Ubigate router pointing to the Intranet router for remote destination networks. In addition to this, the client routes should be configured in the Ubigate SSL VPN for accessing the remote networks via the tunnel mode.

Required Steps:

1. Enter the configuration mode.
2. Enter the SSL VPN Full Tunnel mode.
3. Configure client dynamically assigned ip address range.
4. Configure client routes.

Step-by-Step Configuration

Step	Command	Purpose
1	Router# configure terminal	Enter the terminal configuration mode
2	Router/config# ssl-vpn fulltunnel	Enters the SSL VPN full tunnel configuration mode
3	Router/config/ ssl-vpn/ fulltunnel# client-ip [start ip-address] [end of ip-address] [subnet-mask]	Configuring dynamically assigned client ip address
4	Router/config/ ssl-vpn/ fulltunnel# client routes [network-address] [subnet-mask]	Configuring client routes for full tunnel clients
5	Router/config/ ssl-vpn/ fulltunnel# full-tunnel enable	Enabling the SSL VPN full tunnel Default full tunnel is split tunnel.

Command Examples

The following example shows the commands used to configure SSL VPN full tunnel.

```
Router# configure terminal
Router/configure# ssl-vpn fulltunnel
Router/configure/ssl-vpn fulltunnel# client-ip 192.168.0.1
192.168.0.10 255.255.255.0
Router/configure/ssl-vpn fulltunnel# client-routes 10.1.1.0
255.255.255.0
Router/configure/ssl-vpn fulltunnel# client-routes 10.1.2.0
255.255.255.0
Router/configure/ssl-vpn fulltunnel# full-tunnel enable
```

Configuring SSL VPN Port Forwarding mode

Using Port forwarding mode, remote users can access applications like email, ftp, telnet etc. The administrator needs to configure the port forwarding rules to provide access to remote users. The applications can be accessed using server IP address along with application TCP port, or using loopback IP address with port using the java client.

Required Steps:

1. Enter the configuration mode.
2. Enter the SSL VPN Port Forwarding Mode.
3. Configure TCP port.
4. Configure hostname resolution for the Port Forward.

Step-by-Step Configuration

Step	Command	Purpose
1	Router# configure terminal	Enter the terminal configuration mode
2	Router/config#ssl-vpn portforward	Enter the SSL VPN Port Forwarding configuration mode
3	Router/config/ssl-vpn/portforward# tcp-port [ip address] [port] {[local port number]}	Configure internal server ip address and TCP port number of the application, and local port number
4	Router/config/ssl-vpn/portforward# hostname-resolution [ip-address] [fully qualified domain name]	Map an internal ip address to a full qualified DNS name for use in the Port Forwarding mode.



NOTE

Two types of port number arguments have to be given while the administrator configures a Port Forwarding rule. One is service port number for server application. For instance, the Telnet service port is 23. The other is local port which is a unique port number within 5000-65535 range. The local port number should be unique for each Port Forwarding rule. The local port number is used by the Java Port Forwarding to tunnel the traffic streams using the loopback IP address.

For example, if the service port is 23 (Telnet) and the local port is configured as 55000, then the clients using the Java Port Forwarding have to connect to the telnet service in the following manner:

```
C:\>telnet 127.0.0.1 55000
```

Command Examples

The following example shows the commands used to configure SSL VPN Port Forward.

```
Router# configure terminal
Router/configure# ssl-vpn portforward
Router/configure/ssl-vpn portforward# tcp-port 10.1.1.80 25
50010
Router/configure/ssl-vpn portforward# hostname-resolution
10.1.1.80 mail.samsung.com
```



The administrator can provide ftp service using Port Forwarding mode, but the FTP server and the FTP client must support passive mode. Microsoft DOS FTP command does not support passive mode.

Configuring SSL VPN Global Bookmark

The most frequently used clientless mode services like RDP, VNC, HTTP, HTTPS, Telnet, FTP, and SSH can be bookmarked in form of shortcut links in the SSLVPN portal. The administrator can configure bookmarks, which will be globally available to all users.

Required Steps:

1. Enter the configuration mode.
2. Enter the SSL VPN global bookmark mode.
3. Configure the required services for bookmarking.

Step-by-Step Configuration

Step	Command	Purpose
1	Router# configure terminal	Enter the terminal configuration mode.
2	Router/configure# ssl-vpn global-bookmark	Enter the SSL VPN global bookmark mode.
3	Router/configure/ssl-vpn/global-bookmark# desktop-bookmark-rdp [bookmark name] [ip address] [screen-size]	Configure the desktop RDP as a global bookmark.
4	Router/configure/ssl-vpn/global-bookmark# desktop-bookmark-vnc [bookmark name] [ip address]	Configure the desktop VNC as a global bookmark.
5	Router/configure/ssl-vpn/global-bookmark# service-bookmark [bookmark name] [ip address] [service-type]	Configure the services(ftp, http, https, ssh and telnet) as a service bookmark.

Command Examples

The following example shows the commands used to configure SSL VPN Global Bookmark.

```
Router# configure terminal
Router/configure/ssl-vpn/global-bookmark# desktop-bookmark-
rdp RDP 10.1.1.1 800x600
Router/configure/ssl-vpn/global-bookmark# desktop-bookmark-
vnc VNC 10.1.1.1
Router/configure/ssl-vpn/global-bookmark# service-bookmark
HTTP 10.1.1.1 http
```



CHAPTER 7. Management

Statistics

Ubigate iBG router statistics displays the numerical value of accumulation after booting up the system. The objects in the Ubigate iBG router statistics are as followings.

- Firewall packet statistics
- IPSec packet statistics

Firewall statistics.

It displays the statistics of firewall.

Firewall Statistics Command

Table 6.1 Firewall Statistics command

Command	Explanation
show firewall statistics	Displays statistics of firewall packet and dos-protect.

The following command shows the detailed firewall statistics:

```
Router# show firewall statistics
Global packet statistics
-----
Received                0
Transmitted             0
Local delivery          0
```

Global packet Statistics

```

-----
Possible land attack detected : 0
Spoofed packet : 0
Invalid TCP connection request : 0
Invalid ACK value (Cookie enabled) : 0
UDP echo response for uninitiated request : 0
ICMP echo Reply (echo uninitiated) : 0
General attack detected : 0
IP header length is less then the minimum length : 0
Packet without any data recieved : 0
Invalid TCP packet length : 0
Packet with short TCP Header length : 0
Invalid UDP packet length : 0
Packet with short UDP Header length : 0
Packet with short ICMP length : 0
Post connection SYN detected : 0
Data packet received after reset from same direction : 0
Blind spoofing attack detected : 0
Closing connection as WinNuke Attack detected, out of band
packet : 0
Invalid sequence number received with reset : 0
Connection unestablished, data arrives : 0
ICMP error message (uninitiated traffic) : 0
Invalid source Interface : 0
Memory Allocation failed : 0
Service access request successful : 0
Unable to find route for source : 0
Source address broadcast : 0
Unable to send SYN packet : 0
Send final ACK to target failed : 0
Max connection limit reached, new connections will not be
formed : 0
Attempt to release incorrect TCP NAT port : 0
Attempt to release incorrect UDP NAT port : 0
Attempt to release incorrect ICMP NAT port : 0
Unauthorized Admin login through HTTP : 0
Unable to free unknown protocol NAT port : 0
Unable to allocate NAT port, dropping packet : 0
Unable to free TCP NAT port : 0
Unable to free ICMP NAT port : 0
Unable to free UDP NAT port : 0
Unable to free GRE NAT port : 0
Memory allocation to register application failed : 0
VPN dropped the packet : 0
IIPS dropped the packet : 0
Traffic policies dropped the packet : 0

```



```

Access the policies already deleted : 0
Unable to determine route to destination : 0
Packet not allowed to self : 0
Statically allocated memory : 0
Dynamically allocated memory : 0
Destination address broadcast : 0
No inbound policy found : 0
No outbound policy found : 0
Invalid TCP packet, SYN+ACK expected : 0
Invalid TCP packet, no flags set : 0
Ceiling for number of connections reached, dropping packet : 0
Possible flooding : 0
Protocol is set to zero, dropping packet : 0
Dropping ICMP packet : 0
Checksum mismatch, dropping packet : 0
ICMP error message replay attack detected, dropping packet : 0
Invalid TCP packet recieved before 3-way Handshake is
complete : 0
Connection closed by RST before 3-way Handshake is complete : 0
Access policy not found, dropping packet : 0
Deny access policy matched, dropping packet : 0
Access policy referred on deny timerange, dropping packet : 0
Rate-Limiting: Maximum connection rate reached : 0
Rate-Limiting: Maximum connection limit reached : 0
Reset replay attack detected, dropping packet : 0
Connection closed by RST/FIN before any data transfer : 0
Zero bytes transferred for connection : 0
TCP timed out. 3-Way handShake incomplete, in SYN_RCVD1 state: 0
TCP timed out. 3-Way handShake incomplete, in SYN_RCVD2 state: 0
Connection closed : 0
Connection terminated : 0
Connection timed out : 0
Data connection not established from external network : 0
Traffic police module initialization function failed : 0
Traffic shaping module initialization function failed : 0
ICMP Type: Memory allocation failed, dropping packet : 0
ICMP Type: Received duplicate sequence number : 0
ICMP Type: Echo response with unknown sequence number,
dropping it : 0
Zero length IP option detected : 0
Source routing option set in IP packet : 0
Unaligned timestamp option set in IP packet : 0
Packet with sequence number out of range detected, dropping
it : 0
Invalid sequence number received with Reset, dropping packet : 0
Dropped packets : 0
Rate-Limiting: Maximum packet rate reached, dropping packet : 0

```

```

Rate-Limiting: Maximum bandwidth reached, dropping packet : 0
ICMP type packet received : 0
Memory allocation for connection failed, dropping packet : 0
Unable to allocate memory for NAT port map : 0
Attempt to de-register port map for unavailable NAT IP : 0
Something went wrong while deleting NAT port : 0
Unable to get port map for NAT : 0
Registering NAT ports:Invalid Start Port is more then end
port : 0
Registering NAT ports:Invalid Range : 0
Registering NAT ports:Trying to register twice : 0
Registering NAT ports:Some ports in the Range already
registered : 0
Registering NAT ports:Unable to allocate memory : 0
Default host: IP option modified from single to multiple IP
range : 0
Domain Name in IPDB record resolution failed : 0
Firewall configuration changed : 0
Maximum segment size has been modified : 0
Type of service has been modified : 0
Route entry not found for destination IP, dropping packet : 0
Packet with short GRE header length, dropping packet : 0
Packet with ACK number out of range detected : 0
RST packet with out of range ACK number detected : 0
RST packet with out of range SEQ number detected : 0
RST packet with invalid ACK number during 3-way TCP hand-
shake : 0
RST packet with invalid SEQ number during 3-way TCP hand-
shake : 0
TCP Pkt with invalid ACK number received during 3-way hand-
shake : 0
TCP Pkt with invalid SEQ number received during 3-way hand-
shake : 0
Resource Allocation by IPSEC for caching connection info
failed : 0
No security Policy but encrypted pkt received, dropping it : 0
Security Policy configured but plain pkt received, dropping
it : 0
TCP SYN Scan detected : 0
TCP Connect Scan detected : 0
TCP FIN Scan detected : 0
TCP NULL Scan detected : 0
XMAS Scan detected : 0
TCP Ack Scan detected : 0
Ping Scan detected : 0
UDP Scan Detected : 0

```

```

IP protocol scan detected : 0
Reject access policy matched, dropping the packet : 0
TCP Broadcast packet received, dropping Packet : 0
Connection dropped due to unavailable NAT IP address : 0
Ping of Death attack detected : 0
Jolt attack detected : 0
Zero data length IP fragment detected : 0
Overlapped IP fragment recieved : 0

```

Map-Name	To Internet	From Internet
-----	-----	-----
self	0	0
corp	0	0
dmz	0	0
Total	0	0

IPSec statistics.

It displays the statistics of IPSec packets.

IPSec Statistics Command

Table 6.2 IPSec Statistics command

Command	Explanation
show crypto statistics	Displays statistics of inbound and outbound IPSec packets.

IPSec Statistics Item

Table 6.3 IPSec Statistics Item - Inbound IPSec Packet Errors

Item	explanation
Encryption Failed	Number of encryption errors
Authentication Failed	Number of authentication errors
AH Header Validation Failed	Number of AH header validation errors
Sequence Number Failed	Number of sequence number errors
ESP Header Length Error	Number of ESP header length errors
AH Header Length Error	Number of AH header length errors
Too Many Header Error	Number of invalid header errors

Table 6.3 IPSec Statistics Item - Inbound IPSec Packet Errors (Continued)

Item	explanation
No SA Error	Number of SA availability errors
SA Bundle Verify Error	Number of SA bundle verification errors
Extract Selectors Error	Number of Selectors extraction errors
SA Lifetime Expired	Number of the SA lifetime expirations

Table 6.4 IPSec Statistics Item - Outbound IPSec Packet Errors

Item	explanation
Encrypt Failed Packets	Number of packet encryption errors
TTL Errors	Number of TTL errors
Apply SA Errors	Number of SA application errors
Construct Header Errors	Number of header construction errors
Sequence Over Flow Errors	Number of sequence number overflow errors
Padding Computation Errors	Number of padding computation errors
SA Lifetime Expired	Number of SA lifetime expirations

The following command shows the detailed IPSec statistics:

```
Router# show crypto statistics
Inbound IPSec Packet Errors:
  Encryption Failed           : 0
  Authentication Failed       : 0
  AH Header Validation Failed : 0
  Sequence Number Failed      : 0
  ESP Header Length Error     : 0
  AH Header Length Error      : 0
  Too Many Header Error      : 0
  No SA Error                  : 0
  SA Bundle Verify Error      : 0
  Extract Selectors Error     : 0
  SA Lifetime Expired         : 0

Outbound IPSec Packet Errors:
  Encrypt Failed Packets      : 0
  TTL Errors                   : 0
  Apply SA Errors              : 0
  Construct Header Errors     : 0
  Sequence Over Flow Errors   : 0
  Padding Computation Errors   : 0
  SA Lifetime Expired         : 0
```

Debug Management

This section describes commands that show Debug modes related to security. Following contents are displayed:

- Firewall Debug.
- IPSec Debug.

Firewall Debug Mode

This command displays debug messages for the firewall. It is helpful in troubleshooting firewall problems. Use the command 'show debug firewall' to check the debug mode status.

Table 6.5 Firewall Debug

Command	Purpose
debug firewall all	Enables or disables all firewall debug commands.
debug firewall dos-protect	Enables or disables dos-protect debug.
debug firewall ip-reassembly	Enables or disables IP-reassembly debug.
debug firewall packet	Enables or disables packet trace.
show debug firewall	Display the current firewall debug status.
show debug firewall packet	Displays the current firewall packet debug status.

To trace and debug the firewall packet the command described in Table 6.5 should be entered.

```
Router# debug firewall packet

FW in: self 40.1.1.1->40.1.1.101 proto = icmp len = 28
FW out: ethernet0/2 40.1.1.1->40.1.1.101 proto = icmp len = 28
FW in: ethernet0/2 40.1.1.101->40.1.1.1 proto = icmp len = 28
FW out: self 40.1.1.101->40.1.1.1 proto = icmp len = 28
FW in: ethernet0/2 40.1.1.10->50.1.1.10 proto = icmp len = 60
FW out: ethernet0/4 40.1.1.10->50.1.1.10 proto = icmp len = 60
```

```
Router# debug firewall packet protocol tcp destport 23 level
tcpdump
Router#
FW in: ethernet0/2 40.1.1.10:2035->50.1.1.10:23 proto = tcp
len = 41 DF = 1
IP (tos 0x0, ttl 128, id 4269, offset 0, flags [DF], length: 41)
TCP (40.1.1.10.2035 > 50.1.1.10.23 P [tcp sum ok]) 4:5(1) ack
1 win 65406
TELNET

FW out: ethernet0/4 40.1.1.10:2035->50.1.1.10:23 proto = tcp
len = 41 DF = 1
IP (tos 0x0, ttl 128, id 4269, offset 0, flags [DF], length: 41)
TCP (40.1.1.10.2035 > 50.1.1.10.23 P [tcp sum ok]) 4:5(1) ack
1 win 65406
TELNET

FW in: ethernet0/4 50.1.1.10:23->40.1.1.10:2035 proto = tcp
len = 40 DF = 1
IP (tos 0x0, ttl 128, id 45903, offset 0, flags [DF], length: 40)
TCP (50.1.1.10.23 > 40.1.1.10.2035 . [tcp sum ok]) ack 5 win
65430

FW out: ethernet0/2 50.1.1.10:23->40.1.1.10:2035 proto = tcp
len = 40 DF = 1
IP (tos 0x0, ttl 128, id 45903, offset 0, flags [DF], length: 40)
TCP (50.1.1.10.23 > 40.1.1.10.2035 . [tcp sum ok]) ack 5 win
65430
```

IPSec Debug Mode

This is the commands that displays debug messages for IKE, PKI and IPSec. It is helpful in troubleshooting IPSec problems. Use the command 'show debug crypto' to check the debug mode status.

Table 6.6 IPSec Debug

Command	Purpose
debug crypto all	Enables or disables all IPSec debug commands
debug crypto ca	Enables or disables PKI debug
debug crypto ike	Enables or disables IKE debug
debug crypto ipsec	Enables or disables IPSec debug
show debug crypto	Display the current IPSec debug status

The following examples show debug messages displayed on the terminals of both routers during the successful IPSec tunnel establishment.

```
Router-1# debug crypto all
Router-1# show debug crypto
Crypto debugging status:
  IKE debugging is on
  IPSEC debugging is on
  PKI debugging is on
Router-1#
Router-1#
*****
*****  IKE PHASE1 : 6  *****
*****
****  RECEIVED FIRST MESSAGE OF MAIN MODE  ****
<POLICY: vpn1> PAYLOADS: SA, PROP, TRANS, VID, VID, VID, VID
IkeSelectIsakmpProposal : Xauth is not Enabled
<POLICY: vpn1> PAYLOADS: SA, PROP, TRANS, VID, VID
****  SENT OUT SECOND MESSAGE OF MAIN MODE  ****
****  RECEIVED THIRD MESSAGE OF MAIN MODE  ****
<POLICY: vpn1> PAYLOADS: KE, NONCE, NATD, NATD
IkeInNatDProcess : Resetting
@@@ IPAddrList for NAT-D hash payload : 14010101
<POLICY: vpn1> PAYLOADS: KE, NONCE, NATD, NATD
****  SENT OUT FOURTH MESSAGE OF MAIN MODE  ****
****  RECEIVED FIFTH MESSAGE OF MAIN MODE  ****
<POLICY: vpn1> PAYLOADS: ID, HASH, NOTIFY
IKE Peer ID type = ID_IPV4_ADDR
```

```

IKE Peer ID = 20.1.1.2
IkeInNotifyProcess :: NOTIFY TYPE : 24578
RECEIVED NOTIFY message:
INITIAL_CONTACT
IkeInNotifyIDProcess :: Received Notify Type is not
supported
INITIAL_CONTACT
<POLICY: vpn1> PAYLOADS: ID,HASH,NOTIFY
**** MAIN MODE COMPLETED ****
**** RECEIVED FIRST MESSAGE OF QUICK MODE ****
<POLICY: vpn1> PAYLOADS: HASH,SA,PROP,TRANS,NONCE,ID,ID
SADFindSA : Packet values destipaddr 20.1.1.1, SecProto 50,
SPI 2743332238
SADFindSA : SA not found
<POLICY: vpn1> PAYLOADS: HASH,SA,PROP,TRANS,NONCE,ID,ID
**** SENT OUT SECOND MESSAGE OF QUICK MODE ****
**** RECEIVED THIRD MESSAGE OF QUICK MODE ****
<POLICY: vpn1> PAYLOADS: HASH
usAuthKeyLength:20      pIkeSAInfo->ucAuthAlgo:2
usAuthKeyLength:20      pIkeSAInfo->ucAuthAlgo:2
**** QUICK MODE COMPLETED ****
SPDMatchProposal : Matching Proposal Found
SADFindSA : Packet values destipaddr 20.1.1.1, SecProto 50,
SPI 2743332238
SADFindSA : SA found
*Jun 27,2007,09:23:09 #IPSEC-informational: 0.0.0.0 ->
20.1.1.1 esp INVpn1 SPI
= 0xa383ed8e, Seq. No = N/A :: InboSADFindSA : Packet values
destipaddr 20.1.1.2
, SecProto 50, SPI 4229753905
und SADFindSA : SA not found
SA Created
*Jun 27,2IpSecCreateSABundle:IGWVpnHAGetSACrtEventStruct()
Returned NULL..
007,09:23:09 #IPSEC-informational: 0.0.0.0 -> 20.1.1.2 esp
vpn1 SPI = 0xfc1cec31
, Seq. No = N/A :: Outbound SA Created
SADFindSA : Packet values destipaddr 20.1.1.1, SecProto 50,
SPI 2743332238
SADFindSA : SA found
*Jun 27,2007,09:23:13 #FIREWALL-informational: 222.2.2.20 -
> 201.1.1.9 icmp Ser
vice access request successful
*Jun 27,2007,09:23:13 #FIREWALL-informational: 222.2.2.20 -
> 201.1.1.9 icmp ICM
P Type: 8 Code: 0 Sequence number: 8448 received

```



```

*Jun 27,2007,09:23:13 #FIREWALL-informational: 201.1.1.9 ->
222.2.2.20 icmp ICM
P Type: 0 Code: 0 Sequence number: 8448 received
DISCARDING RETRANSMITTED PACKET...
IKEServer : Processing of data returned error -1
SADFindSA : Packet values destipaddr 20.1.1.1, SecProto 50,
SPI 2743332238
SADFindSA : SA found
*Jun 27,2007,09:23:14 #FIREWALL-informational: 222.2.2.20 -
> 201.1.1.9 icmp ICM
P Type: 8 Code: 0 Sequence number: 8704 received
*Jun 27,2007,09:23:14 #FIREWALL-informational: 201.1.1.9 ->
222.2.2.20 icmp ICM
P Type: 0 Code: 0 Sequence number: 8704 received
SADFindSA : Packet values destipaddr 20.1.1.1, SecProto 50,
SPI 2743332238
SADFindSA : SA found
*Jun 27,2007,09:23:15 #FIREWALL-informational: 222.2.2.20 -
> 201.1.1.9 icmp ICM
P Type: 8 Code: 0 Sequence number: 8960 received
*Jun 27,2007,09:23:15 #FIREWALL-informational: 201.1.1.9 ->
222.2.2.20 icmp ICM
P Type: 0 Code: 0 Sequence number: 8960 received
DISCARDING RETRANSMITTED PACKET...

```

```

Router-2# debug crypto all
Router-2# show debug crypto
Crypto debugging status:
IKE debugging is on
IPSEC debugging is on
PKI debugging is on
Router-2#
Router-2# SADFindSA : Packet values destipaddr 201.1.1.9,
SecProto 50, SPI 24153
09071
SADFindSA : SA not found
SADFindSA : Packet values destipaddr 201.1.1.9, SecProto 50,
SPI 2415309071
SADFindSA : SA found
IpIPSecOutProcess : Key mgmt type is AUTO
*Jun 27,2007,09:23:37 #FIREWALL-informational: 222.2.2.20 -
> 201.1.1.9 icmp Ser
vice access request successful
*Jun 27,2007,09:23:37 #FIREWALL-informational: 222.2.2.20 -
> 201.1.1.9 icmp ICM

```

```

P Type: 8 Code: 0 Sequence number: 8192 received
*Jun 27,2007,09:23:37 #FIREWALL-alert: 222.2.2.20 ->
222.2.2.2 icmp ICMP error
message replay attack detected, dropping packet

*****
***** IKE PHASE1 :      6 *****
*****
**** SENT OUT FIRST MESSAGE OF MAIN MODE ****
<POLICY: vpn1> PAYLOADS: SA,PROP,TRANS,VID,VID,VID,VID
**** RECEIVED SECOND MESSAGE OF MAIN MODE ****
<POLICY: vpn1> PAYLOADS: SA,PROP,TRANS,VID,VID
IkeInXformProcess: Gotcha !! Selected the IKE proposal
@@@ IPAddrList for NAT-D hash payload : 14010102
**** SENT OUT THIRD MESSAGE OF MAIN MODE ****
<POLICY: vpn1> PAYLOADS: KE,NONCE,NATD,NATD
**** RECEIVED FOURTH MESSAGE OF MAIN MODE ****
<POLICY: vpn1> PAYLOADS: KE,NONCE,NATD,NATD
IkeInNatDProcess : Resetting
INITIAL_CONTACT
<POLICY: vpn1> PAYLOADS: ID,HASH,NOTIFY
**** SENT OUT FIFTH MESSAGE OF MAIN MODE ****
**** RECEIVED SIXTH MESSAGE OF MAIN MODE ****
<POLICY: vpn1> PAYLOADS: ID,HASH,NOTIFY
IKE Peer ID type = ID_IPV4_ADDR
IKE Peer ID = 20.1.1.1
IkeInNotifyProcess :: NOTIFY TYPE : 24578
RECEIVED NOTIFY message:
INITIAL_CONTACT
IkeInNotifyIDProcess :: Received Notify Type is not
supported
**** MAIN MODE COMPLETED ****
SADFindSA : Packet values destipaddr 20.1.1.2, SecProto 50,
SPI 4229753905
SADFindSA : SA not found
<POLICY: vpn1> PAYLOADS: HASH,SA,PROP,TRANS,NONCE,ID,ID
**** SENT OUT FIRST MESSAGE OF QUICK MODE ****
**** RECEIVED SECOND MESSAGE OF QUICK MODE ****
<POLICY: vpn1> PAYLOADS: HASH,SA,PROP,TRANS,NONCE,ID,ID
IkeInXformProcess: Gotcha !! Selected the ESP proposal
<POLICY: vpn1> PAYLOADS: HASH
IkeQMInitSAWaitProcess: IKE_SA_MATURE
**** SENT OUT THIRD MESSAGE OF QUICK MODE ****
usAuthKeyLength:20      pIkeSAInfo->ucAuthAlgo:2

```

```

usAuthKeyLength:20      pIkeSAInfo->ucAuthAlgo:2
**** QUICK MODE COMPLETED ****
  SPDMatchProposal : Matching Proposal Found
SADFindSA : Packet values destipaddr 20.1.1.2, SecProto 50,
SPI 4229753905
SADFindSA : SA found
  *Jun 27,2SADFindSA : Packet values destipaddr 20.1.1.1,
SecProto 50, SPI 2743332238
007,SADFindSA : SA not found
09:23:38 #IPSEC-
infoIpSecCreateSABundle:IGWVpnHAGetsACrtEventStruct()
Returned NULL..
rmational: 0.0.0.0 -> 20.1.1.2 esp INvpn1 SPI = 0xfc1cec31,
Seq. No = N/A :: Inbound SA Created
  *Jun 27,2007,09:23:38 #IPSEC-informational: 0.0.0.0 ->
20.1.1.1 esp vpn1 SPI = 0xa383ed8e, Seq.
No = N/A :: Outbound SA Created
*Jun 27,2007,09:23:42 #FIREWALL-informational: 222.2.2.20 ->
201.1.1.9 icmp ICM
P Type: 8 Code: 0 Sequence number: 8448 received
SADFindSA : Packet values destipaddr 20.1.1.2, SecProto 50,
SPI 4229753905
SADFindSA : SA found
  *Jun 27,2007,09:23:42 #FIREWALL-informational: 201.1.1.9 ->
222.2.2.20 icmp ICM
P Type: 0 Code: 0 Sequence number: 8448 received
IkeRetryTimeOut: Retrying 2nd phase message..
  *Jun 27,2007,09:23:43 #FIREWALL-informational: 222.2.2.20 ->
201.1.1.9 icmp ICM
P Type: 8 Code: 0 Sequence number: 8704 received
SADFindSA : Packet values destipaddr 20.1.1.2, SecProto 50,
SPI 4229753905
SADFindSA : SA found
  *Jun 27,2007,09:23:43 #FIREWALL-informational: 201.1.1.9 ->
222.2.2.20 icmp ICM
P Type: 0 Code: 0 Sequence number: 8704 received
*Jun 27,2007,09:23:44 #FIREWALL-informational: 222.2.2.20 ->
201.1.1.9 icmp ICM
P Type: 8 Code: 0 Sequence number: 8960 received
SADFindSA : Packet values destipaddr 20.1.1.2, SecProto 50,
SPI 4229753905
SADFindSA : SA found
  *Jun 27,2007,09:23:44 #FIREWALL-informational: 201.1.1.9 ->
222.2.2.20 icmp ICM
P Type: 0 Code: 0 Sequence number: 8960 received

```



This page is intentionally left blank.

PART V. Voice



- CHAPTER 1. Voice Feature**
- CHAPTER 2. VoIP Gateway Management**
- CHAPTER 3. SIP Gateway Management**
- CHAPTER 4. H.323 Gateway Management**
- CHAPTER 5. Analog Voice Port**
- CHAPTER 6. Digital Voice Port**
- CHAPTER 7. ISDN**
- CHAPTER 8. Routing and Digit Manipulation**
- CHAPTER 9. Extended VoIP Services**
- CHAPTER 10. Call Admission Control**
- CHAPTER 11. Management**
- CHAPTER 12. Survivable Telephony**
- CHAPTER 13. Case Study**



CHAPTER 1. Voice Feature

Introduction of Voice Feature

Ubigate iBG router is a high performance enterprise access router, which provides a VoIP gateway feature. VoIP gateway, like Ubigate iBG router, provides real-time, two-way voice communications between packet networks and circuit networks. This system has two major functions. One is signaling the conversion function and the other is a media conversion function.

Network Architecture

The network architecture in view of Ubigate iBG router is shown in Figure 1.1.

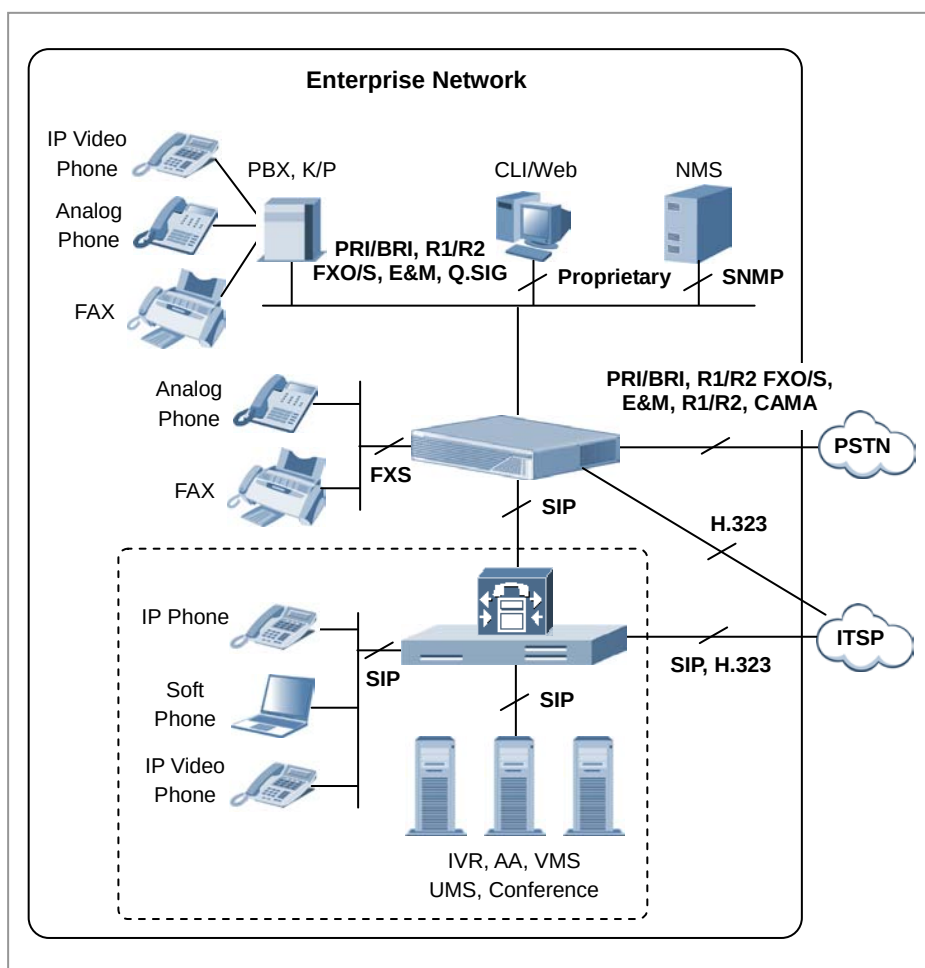


Figure 1.1 Ubigate iBG Network Diagram

The external entities which interwork with Ubigate iBG router over a network are as follows:

Ubigate iBG router

Ubigate iBG router acts as the interface between a traditional voice network and the IP network. Ubigate iBG router interfaces with traditional voice networks (PBX and PSTN) through digital trunk interfaces such as T1/E1, ISDN PRI/BRI, and Q.SIG and analog trunk interfaces such as FXS (DID), FXO, CAMA and E & M. Ubigate iBG router terminates the PSTN/ISDN and analog trunk signals. Ubigate iBG router acts as a VoIP gateway converting the TDM to packets and vice versa, and communicates with the Call Manager using standard protocols such as SIP.

IP PBX (Ubigate iPX)

IP PBX performs call processing functions and interfaces with Ubigate iBG router over the packet network using VoIP protocols such as SIP.

Ubigate iPX as an IP PBX provides basic VoIP call services and advanced supplementary features. It maintains one or more Ubigate iBG routers.

IP Phone/Soft Phone

IP phone provides a generic voice call service over the IP network.

IP phone, to support basic call and supplementary call services, interfaces with Ubigate iPX using standard RFC3261 based SIP Protocol with some other extensions.

Analog Phone/FAX

Analog phone is the terminal to provide a generic voice call via legacy analog lines. FAX is the terminal to provide a fax service via legacy analog lines.

PBX, KTS

PBX or Key Telephone System is voice equipments to connect the in-house extension calls or external calls in the legacy analog and digital trunks, instead of the IP Network.

CLI/Web

The OAM interface provided by the Ubigate iBG router, can control various OAM functions of Ubigate iBG router, after accessing a Ubigate iBG router via CLI or web from a desktop or laptop computer.

NMS

The Network Management System is used to manage Ubigate iBG router and Call Manager devices in the network.

IVR/AA/VMS/UMS/Conference Server

This is equipment to provide various services such as VMS, IVR, AA, Conference which are not provided by Ubigate iBG router and Call Manager.

Interface Between Network Entities

The interface specifications for interworking with network entities are as follows:

iBG router-iPX Interface

Ubigate iBG and iPX use Session Initiation Protocol (SIP) as call signaling. They use standard RFC3261 based SIP with extensions. Samsung proprietary headers are used for VoIP services.

For management, a TCP/IP protocol based proprietary protocol is used in-between to load subscriber's profiles, feature and access codes information, and additional information for survivability.

iBG router-PSTN Interface

This is the interface used for interworking between existing PSTN and voice calls.

E & M, PRI, BRI, FXO, FXS (DID), R1, R2, CAMA are used as a signaling method; and T1, E1, Analog Trunk and Analog Line are used as a physical layer.

- Analog I/F: FXO, FXS, DID, E & M
- Digital I/F: T1 CAS E & M/FXO/FXS, T1 R1, E1 R2 MFC/DTMF, ISDN - PRI/BRI (S/T, U)

iBG router-Analog Phone Interface

This is the interface used for iBG router to provide voice calls to generic analog phones. FXS is used.

iBG router-PBX Interface

This is the interface used for the iBG router to interwork with legacy PBX. PRI, BRI, R1, R2, FXO, E & M, Q.SIG, DID are used as signaling methods; and T1, E1, Analog Trunk and Analog Line are uses as a physical layer.

- Analog I/F: FXS, FXO, E & M
- Digital I/F: T1 CAS FXS/FXO/E & M, E1 R2 MFC/DTMF, ISDN - PRI/BRI (S/T, U), ISDN - Q.SIG

iBG router-CLI/Web Interface

This is the interface used to interwork with CLI and Web Client in order for iBG router to provide OAM functions. The TCP/IP protocol based proprietary interface defined by Samsung is used.

Operation Mode

When Ubigate iBG router runs as a SIP gateway, it can work in iPX Interworking mode, where it interworks with SIP network via Ubigate iPX; or in stand-alone Mode (or Toll Bypass Mode), where it directly interworks with other SIP gateways with/without a SIP server. When connectivity with Ubigate iPX fails, iBG automatically changes to Survivable Telephony Mode to provide basic calls and supplementary services without Ubigate iPX. The detailed operation mode is described below.

Call-server (Ubigate iPX) Interworking Mode

In iPX Interworking Mode, the Ubigate iBG router registers to Ubigate iPX and iPX manages multiple IP phones and Ubigate iBG routers. Generally, Ubigate iBG router delivers voice calls to iPX via SIP protocol when iPX would decide to route a call to other Ubigate iBG routers, IP Phones or other SIP/H.323 servers.

The generic network configuration in iPX Interworking Mode is shown in the Figure 1.1, Figure 1.2 shows that Ubigate iPX exists in headquarter office to control the corporate VoIP network, and multiple Ubigate iBG routers reside in individual branch offices. In addition, multiple IP phones reside in the headquarter office and each branches. Ubigate2016s and IP phones in the company are registered to iPX, and iPX controls the overall routing of internal and external calls.

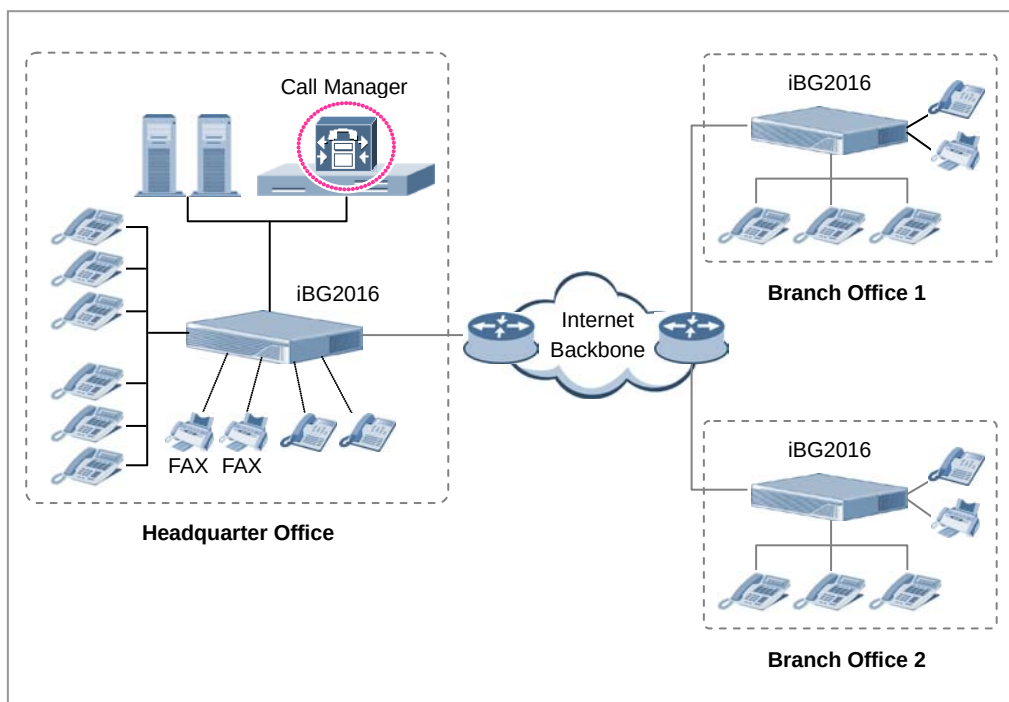


Figure 1.2 Example of Call Manager Interworking Mode Network Configuration

Survivable Telephony Mode

In Call-server (iPX) interworking mode, all voice calls over VoIP network are generally controlled by Ubigate iPX. No originating and terminating calls (IP Phone or Analog Phone) will be available if Ubigate iPX fails (e.g., link failure), or access to Ubigate iPX is not allowable. To overcome this failure, Ubigate iBG router continuously monitors connectivity with Ubigate iPX; When it detects iPX failure, it automatically changes to Survivable Telephony mode where Ubigate iBG router can provide voice services by itself. In Survivable Telephony mode, voice service features are limited from iPX interworking mode.

Stand-alone mode (or Toll Bypass mode)

In standalone mode, Ubigate iBG router provides SIP trunks with other SIP entities and can inter-work with standard-based SIP server such as Registrar, Proxy, and Redirect server.

In this mode, Ubigate iBG router makes a decision for all call processing and call routing.

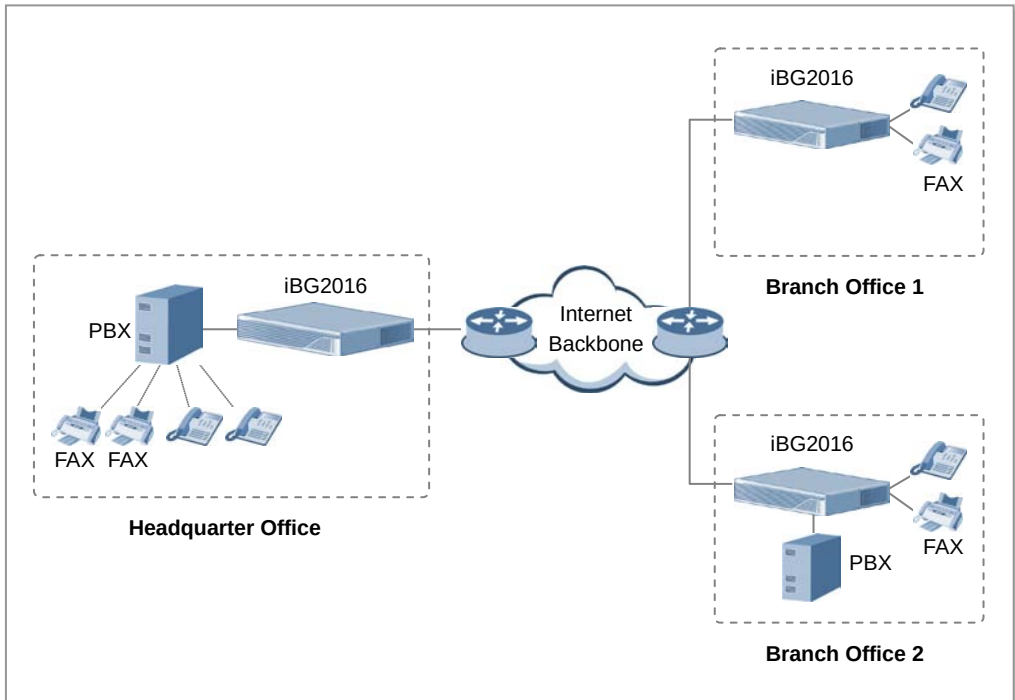


Figure 1.3 Example of Stand-alone mode network configuration

Figure 1.3 shows an example of standalone mode network configuration. In this network configuration, either Ubigate iPX or IP phones do not exist. Internal calls within HQ and branch office 2 are controlled by the PBXs residing on each network, and outgoing calls to other branches are carried out via VoIP network through Ubigate iBG routers.

Key Functions

VoIP Gateway

VoIP Gateway function is used to deliver voice calls between the PSTN and IP network. Ubigate iBG router acts as the interface between a traditional voice network and the IP network. Ubigate iBG router interfaces with the traditional voice networks (PBX and PSTN) through T1/E1/ISDN-PRI interfaces and analog trunk interfaces such as DID, E & M and FXO. Ubigate iBG router terminates the PSTN/ISDN and analog trunk signals. In addition, Ubigate iBG router interfaces with the IP network via interwork with SIP Proxy, SIP registrar, SIP Gateway, SIP terminal, H.323 Gatekeeper, H.323 Gateway, etc.

Support of SIP Signaling

Ubigate iBG router supports standard RFC3261-based SIP protocol and a number of extensions/drafts to provide SIP-based VoIP services.

Ubigate iBG router supports some different methods as follows.

Direct Connection

Direct connection enables call processing without a SIP server. It is used where there is no Ubigate iPX or proxy server directly connected to the network.

Ubigate should make SIP trunks among all other VoIP entities to route calls.

Indirect Connection via SIP Proxy Server

Indirect connection enables Ubigate iBG router to serve as a SIP gateway for Ubigate iPX or SIP proxy server.

In this indirect connection, Ubigate iBG router registers to Ubigate iPX or SIP registrar and outbound calls will route to the server.

Support of H.323 Signaling

Ubigate iBG router serves as an H.323 gateway and interworks with other H.323 network entities residing on the network in the following way.

H.323 Gateway Mode

In H.323 gateway mode, Ubigate iBG router serves as a gateway in a zone managed by the H.323 Gatekeeper.

When Ubigate iBG router runs in H.323 gateway mode, Ubigate iBG router performs general GK registration procedures using RRQ.

A gatekeeper identifies Ubigate iBG router as a gateway to be managed in a zone, and Ubigate iBG router provides the H.323 Gateway characteristics necessary for call signaling.

H.323 Direct Mode

Direct mode enables call processing without H.323 registration. It is used when signaling is performed directly among gateways without passing through a gatekeeper.

Support of PSTN Signaling

Ubigate iBG router acts as a VoIP Gateway to interconnect between legacy PSTN and VoIP network. To seamlessly interwork with PSTN, Ubigate iBG router supports various PSTN signalings that have been used for several decades.

- Ubigate iBG router supports the following PSTN signaling.
 - Analog FXS: loop-start, ground-start
 - Analog E & M: wink, immediate, delay
 - Analog FXO: loop-start, ground-start
 - Analog DID (Direct Inward Dial)
 - ISDN BRI Q.931: network side, user side
 - T1-CAS E & M: wink, immediate, delay
 - T1-CAS FXO: ground start, loop start
 - T1-CAS FXS: ground start, loop start
 - E1-CAS R2: MFC, DTMF
 - T1/E1 ISDN PRI Q.931: user side, network side
 - T1 R1

- Ubigate iBG router supports the following R2 Country variants.
 - Australia
 - Brazil
 - China
 - East Europe
 - Hong Kong
 - India
 - ITU, Korea
 - Thailand
 - Mexico
- Ubigate iBG router supports the following ISDN Country variants.
 - AT & T 4ESS (User Side-PRI, Network Side-PRI)
 - AT & T 5ESS (User Side-PRI/BRI, -Network Side-PRI/BRI)
 - ETSI (User & Network Side-PRI/BRI)
 - Australian Telecom (User Side-PRI/BRI and Network Side-PRI)
 - National ISDN-1 (User Side-BRI)
 - NTT (User & Network Side-PRI/BRI)
 - Northern Telecom DMS-100 (User Side & Network Side-PRI/BRI)
 - Northern Telecom DMS-250 (User Side & Network Side-PRI)
 - National ISDN-2 (User & Network Side-PRI)
 - Q.SIG (PRI)

Support of Voice Codec

Ubigate iBG router acts as a VoIP gateway converting TDM to packets and vice versa, and supports the following Voice Codecs:

- ITU-T G.711-Pulse code modulation (PCM) of voice frequencies
- ITU-T G.711 Appendix I-A high quality low-complexity algorithm for packet loss concealment with G.711
- ITU-T G.711 Appendix II-A comfort noise payload definition for ITU-T G.711 use in packet-based multimedia communication systems.
- ITU-T G.723.1-Dual rate speech coder for multimedia communications transmitting at 5.3 and 6.3 Kbit/s
- ITU-T G.723.1 Annex A-Speech coders: Silence compression scheme
- ITU-T G.726-40, 32, 24, 16 Kbit/s adaptive differential pulse code modulation (ADPCM)
- ITU-T G.729-Coding of speech at 8 Kbit/s using conjugate-structure algebraic-code-excited linear-prediction (CS-ACELP)

- ITU-T G.729 Annex A-Reduced complexity 8 Kbit/s CS-ACELP speech codec
- ITU-T G.729 Annex B-A silence compression scheme for G.729 optimized for terminals conforming to Recommendation V.70

Security

Ubigate iBG router provides such functions as S/MIME, TLS, sRTP and IPSec to ensure voice security.

S/MIME and TLS ensure security for SIP signaling, and sRTP ensures security for media. IPSec ensures security not only for signaling and media but also for all information between two devices connected via IPSec.

TLS

TLS can provide a Hop-by-Hop Security function for the SIP messages transceived from/to a network entity.

sRTP (Secure RTP)

sRTP is the function to encode and transceive the End-to-End RTP data over IP network to prevent the wiretapping of a conversation.

Call Routing and Digit Manipulation

Call Routing

The calls incoming to an Ubigate iBG router can be outbound to PSTN such as Port and Trunk Group, or to the VoIP network such as H.323 Session Target or SIP Session Target. Routing Control is the procedure to determine the route, out of various destinations, where a call will be outbound. The final routing route is determined depending on various settings such as Dial Plan, Preference, Hunting Scheme, etc.

Digit Manipulation

The Ubigate iBG router provides digit manipulation function in a dial string before it passes the dial string to the telephony device.

Digits Stripping and Prefixes

Digits stripping and prefixes function provides digits deletion or insertion before sending the outbound POTS peer.

For digits stripping, the Ubigate iBG router strips off the left-justified digits that explicitly match the destination pattern when the Ubigate iBG router matches a dial string to an outbound POTS dial peer.

For prefixes, the Ubigate iBG router may add specific digits to the front of the dialed string before it is forwarded to the telephony interface.

Forward Digits

The Ubigate iBG router defines the number of digits and then forwards it to the telephony interface. The Ubigate iBG router controls the number of digits that are stripped before the dialed string is passed to the telephony interface.

Digit Translation

Digit translation rules are used to manipulate the calling number (ANI) or called number (DNIS) digits for a voice call, or to change the numbering type of a call.

Translation rules are used to convert a telephone number into a different number before the call is matched to an inbound dial peer or before the call is forwarded by the outbound dial peer.

Call Block

The Ubigate iBG router provides a call-blocking function based on calling or called number.

Call Admission Control (CAC)

Voice CAC is one of techniques, which is used to maintain reasonable voice quality. For real-time delay-sensitive traffic such as voice, it is better to deny network access under congested conditions than to allow traffic onto the network to be dropped or delayed.

CAC is a deterministic and informed decision that is made before a voice call is established and is based on whether the required network resources are available to provide suitable QoS for the new call.

Local CAC

Local CAC mechanisms function on the outgoing Ubigate iBG router. The CAC decision is based on nodal information such as the state of the Max. Calls.

The Ubigate iBG router provides Call Admission Control based on Maximum Call Number per System Wide. The Call Admission Control Based on Max. Call feature permits the Ubigate iBG router to deny incoming calls exceeding a preconfigured threshold, permitting the selection of a system max. call value. This feature helps ensure the quality of service of existing calls and reliability of system processes by preventing system overload caused by excessive incoming calls. The feature rejects new calls, with minor disruption to system users. The administrator of the Ubigate iBG router sets a threshold at which denial of new calls occurs.

The Ubigate iBG router provides Call Admission Control based on Maximum Call Number per Dial-Peer.

The Ubigate iBG router provides Call Admission Control based on Physical DS0 Limitation.

Resource-based CAC

Resource based CAC mechanisms function on the outgoing Ubigate iBG router. The CAC decision is based on nodal information such as the state of the CPU, memory and DSP channels load level.

The Ubigate iBG router provides Call Admission Control based on CPU utilization. The Call Admission Control Based on the CPU Utilization feature permits the Ubigate iBG router to deny incoming calls exceeding a preconfigured threshold, permitting the selection of a system CPU load level value. This feature helps ensure the quality of service of existing calls and reliability of system processes by preventing system overload caused by excessive incoming calls. The feature rejects new calls, with minor disruption to system users. The administrator of the Ubigate iBG router sets a threshold at which denial of new calls occurs. This CPU load threshold may be set anywhere from 20 to 90%.

The Ubigate iBG router provides Call Admission Control based on memory utilization. The Call Admission Control Based on Memory Utilization feature permits the Ubigate iBG router to deny incoming calls exceeding a preconfigured threshold, permitting the selection of a system memory load level value. This feature helps ensure the quality of service of existing calls and reliability of system processes by preventing system overload caused by excessive incoming calls. The feature rejects new calls, with minor disruption to system users. The administrator of the Ubigate iBG router sets a threshold at which denial of new calls occurs.

This memory load threshold may be set anywhere from 20 to 90%.

The Ubigate iBG router provides Call Admission Control based on DSP utilization. The Call Admission Control Based on DSP channel Utilization feature permits the Ubigate iBG router to deny incoming calls exceeding a preconfigured threshold, permitting the selection of a system DSP channel load level value. This feature helps ensure the quality of service of existing calls and reliability of system processes by preventing system overload caused by excessive incoming calls. The feature rejects new calls, with minor disruption to system users. The administrator of the Ubigate iBG router sets a threshold at which denial of new calls occurs. This DSP load threshold may be set anywhere from 20 to 100%.

Voice Services

FAX

Ubigate iBG router supports FAX pass-through and SIP/H.323 T.38 FAX relay.

T.38

The Ubigate iBG router negotiates fax relay transmission by exchanging capability information in Session Description Protocol (SDP) messages and H.323 messages. T.38 Annex D procedures are used for the changeover from VoIP to fax mode during a call.

For SIP, initially a normal VoIP call is established using SIP INVITEs. The DSP of the Ubigate iBG router needs to be informed that it can support T.38 mode while it is put into voice mode. Then, during the call, when the DSP of the Ubigate iBG router detects fax flags, the Ubigate iBG router initiates a SIP INVITE mid-call to signal the desire to change the media stream.

FAX Pass-through

The Ubigate iBG router does not distinguish a fax call from a voice call.

Fax communication between the two fax machines is carried in its entirety in-band over a voice call.

Fax up-speed is similar to pass-through in the sense that the fax call is carried in-band over the voice call.

The difference is that when using up-speed, the Ubigate iBG router is to some extent aware of the fax call. Although relay mechanisms are not employed, with up-speed the gateways do recognize a CED fax tone and automatically change the voice codec to G.711 if necessary and turn off echo cancellation (EC) and voice activity detection (VAD) for the duration of the call.

DTMF Relay

The reliable DTMF relay feature provides reliable digit relay between Ubigate iBG routers or between Ubigate iBG router and Call Manager when a low-bandwidth codec is used.

RFC2833

The Ubigate iBG router support RFC 2833 for reliable DTMF relay. The Ubigate iBG router to relay DTMF tones provides a standardized means of transporting DTMF tones in Real-Time Transport Protocol (RTP) packets according to section 3 of RFC 2833.

DTMF events through SIP signaling

The Ubigate iBG router support the NOTIFY method for DTMF relay. The SIP event notification mechanism uses the NOTIFY method to signal when certain telephony events take place. In order to send DTMF signals through the NOTIFY method, the gateway notifies the subscriber when DTMF digits are signaled by the originator. The notification contains a message body with a SIP response status line.

Ad-hoc Conference

the Ad-hoc conferencing function provides the DSP conferencing resource contained in a Ubigate iBG router, to provide high voice quality for supplementary services such as 3-way conferencing or Call Manager.

For Ad-hoc conferencing, a Ubigate iBG router interworks with Call Manager using SIP, and the service is controlled by Call Manager.

Private Line Automatic Ringdown (PLAR)

The Ubigate iBG router provide PLAR (Private Line Automatic Ringdown) and OPX (Off premises extension).

PLAR

PLAR circuits have statically configured endpoints and do not require the user dialing to connect calls. The PLAR provides a mechanism to create a switched Voice over IP (VoIP) call without digit dialing.

PLAR OPX

OPX allows remote users on Foreign Exchange Station (FXS) ports to look to a central PBX-like physical extensions. The Ubigate iBG router offer toll-bypass VoIP services without having the Ubigate iBG router provide dial-tone or change their existing dial plan. OPX allows stations at remote sites to look like they are stations that are physically connected to a PBX.

LVBO (Local Voice Busy Out)

LVBO provides the Ubigate iBG router with the ability to monitor the state of various network interfaces, both LAN and WAN, and busy back the trunk to the PSTN interface if any of the monitored links should fail.

If an ISDN lines enters a LVBO state, a specific fail code is sent regarding it to the ISDN Inbound Call Attempt to notify a 'busyout' status.

For LVBO, the PSTN (FXS, FXO, E & M, T1/E1 CAS) signaling line runs in the following way:

- If a call comes into an analog FXS, a Fast-Busy Tone is sent to indicate that the relevant line is busy.
- In regard to the inbound call attempt such as FXO, E & M, T1-CAS FXS/FXO/E & M and T1-R1, a Ubigate iBG router runs in a way which enables a remote office to identify that the relevant line is in a 'Busyout' status.
- Since a block message exists for E1-R2, a block message is sent to a remote office to block the call attempt by a remote office; an Unblock Message is sent when LVBO status is released to return the line to idle status.

Supplementary Services

Ubigate iBG router provides the following supplementary services for each of iPX Interworking mode, Survivable Telephony Mode and Stand Alone Mode.

iPX Interworking Mode

When running in a iPX Interworking mode, Ubigate iBG router provides the supplementary services under iPX control.

- Calling Line Identification (CLID)
- Call Forward-All
- Call Forward-Busy
- Call Forward-NoAnswer
- Call Hold and Retrieve
- Call Park
- Call Pickup Group
- Call Pickup Direct
- Call Pickup Universal
- Call Restriction by User
- Call Waiting and Retrieve
- Call Transfer-Blind
- Call Transfer-Consultative
- Call Forwarding to VMS-All
- Call Forwarding to VMS-Busy
- Call Forwarding to VMS-NoAnswer
- Call Back Busy Subscriber
- Call Override
- Call Intrusion
- Privacy
- Wake-up Call
- Do Not Disturb (DND)
- Absentee Service (ABS)
- Conference calls
- Ad-hoc conference
- Group Call
- Distinctive Ring
- Music On Hold Service
- Malicious Call
- Follow Me

Survivable Telephony Mode

When running in a Survivable Telephony mode, a Ubigate iBG router provides the following supplementary services to the FXS and IP Phone subscribers which interwork with Call Manager via itself.

- Calling Line Identification (CLID)
- Call Forward-All
- Call Forward-Busy
- Call Forward-NoAnswer
- Call Hold and Retrieve
- Call Pickup Group
- Call Pickup Direct
- Call Pickup Universal
- Call Waiting and Retrieve
- Call Transfer-Blind
- Call Transfer-Consultative
- Distinctive Ring

Stand Alone Mode

When running in a Stand Alone mode, a Ubigate iBG router provides the following supplementary services to the FXS subscribers connected to it.

- Calling Line Identification (CLID)
- Call Hold and Retrieve
- Call Pickup Group
- Call Pickup Direct
- Call Pickup Universal
- Call Waiting and Retrieve
- Call Transfer-Blind
- Call Transfer-Consultative
- Distinctive Ring

E911 Support

Ubigate iBG router supports an E911 feature. E911 is an emergency telephone system capable of automatically displaying the callback number (and in some cases the location) of a person who dials emergency call numbers (911) to request emergency help from public safety agencies.

The North American emergency E911 phone system consists of a voice network that is built largely outside of the normal public switched telephone network (PSTN) on which common voice traffic rides. They are treated especially because they are routed differently within the PSTN than normal traffic. Calls to emergency services are routed based on the calling number, not the called number. The calling number is checked against a database of emergency service providers that cross-references the service providers for the caller's particular location. When this information is known, the call is then routed to the proper public service answering point (PSAP), which, in turn, dispatches those services for the caller's location.

High Availability of Voice Feature

As enterprises extend their IP telephony and high-value application deployments from central sites out to remote offices, one of the factors considered vital in deployment is the ability to cost-effectively provide backup redundancy functions at the remote branch office. However, the size and number of these small-office sites precludes most enterprises from deploying dedicated call-processing servers, unified messaging servers, or multiple WAN links to each site to achieve the high availability required.

Ubigate iBG router provides high availability voice solutions for the cases below:

Table 1.1 High Availability Cases

-	Local Call Server Through LAN	Remote Call Server Through WAN
WAN Link Fail (Call Server Alive)	PSTN Fallback - Analog call → PSTN - VoIP call → PSTN - Controlled by Call Server	Survivable Telephony - Analog call → PSTN - VoIP call → PSTN - Controlled by Ubigate iBG router (Call Server is down)

Table 1.1 High Availability Cases (Continued)

-	Local Call Server Through LAN	Remote Call Server Through WAN
Call Server Down (WAN Link Alive)	Survivable Telephony - Analog call → PSTN, IP N/W - VoIP call → PSTN, IP N/W - Controlled by Ubigate iBG router	Survivable Telephony - Analog call → PSTN, IP N/W - VoIP call → PSTN, IP N/W - Controlled by Ubigate iBG router

PSTN Fallback

Ubigate iBG router monitors the status of the IP network (WAN). When WAN failure is detected, the Ubigate iBG router redirects calls to the PSTN automatically. When the WAN link is restored, call routing reverts back to the IP Network.

This feature is called PSTN Fallback and enables an end-user to give a reasonable guarantee about call completion.

Survivable Telephony

Ubigate iBG router provides survivable telephony functionality that is very important for remote site branch offices that are connected over WAN links. When the WAN link fails and there is no other way to communicate with the Call Server (Ubigate iPX) then it is impossible to make a VoIP call setup.

In this scenario, Ubigate iBG router acts as a local PBX and SIP server to provide voice services for not only analog phones but IP phones.

While serving voice services, Ubigate iBG router keeps checking if the Call Server or WAN is back to service. When the Call Server is back to providing all voice services then Ubigate iBG stops acting as a local PBX and SIP server and returns to iPX interworking mode.

In survivable telephony mode, Ubigate iBG router could route outbound calls to PSTN or VoIP - SIP trunks if available.

When Ubigate iBG router changes to survivable telephony mode, active calls within the brace are not affected by WAN or Call Server failure. They will last for the duration of the calls.

In survivable telephony mode, Ubigate iBG router provides the services below:

- Local extension dialing IP Phone to/from IP Phone calls
- IP Phone to/from PSTN calls (VoIP trunks if available)
- IP Phone to/from analog device calls

It is recommended that all Ubigate iBG routers in remote offices maintain direct links to the PSTN for backup callout capability. This is particularly important for maintaining emergency calling capability.

Voice Deployment Scenario

In this Section, we describe various service scenarios that can be provided using the Ubigate iBG router VoIP system.

PSTN Toll Bypass

Ubigate iBG router provides voice and fax toll bypass capabilities as shown in Figure 1.4. In this scenario a telephonic device attached to a PBX or Key Phone System will be connected to Ubigate iBG router through an analog or digital trunk connection.

When Ubigate iBG router is in Call Manager Interworking mode, a call is established across the network by Ubigate iBG router and Call Manager. Call Manager communicates across the IP network using SIP or H.323. Packets are then routed over the IP network to the destination where the reverse operation is performed and thus the call is completed over the IP network, bypassing the traditional toll network, PSTN. When Ubigate iBG router is in Stand-alone mode, a call is established across the IP network between Ubigate iBG routers without Call Manager.

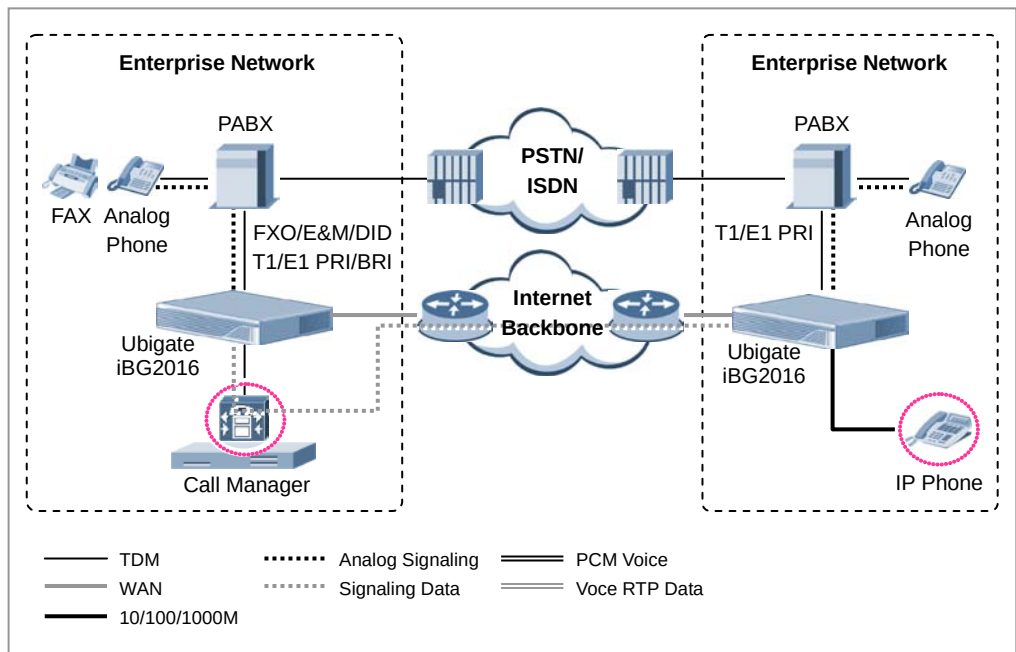


Figure 1.4 Toll Bypass for Voice and Fax services

IP Phones

The second scenario of an IP phone attached to Ubigate iBG router is shown in Figure 1.5. The SIP phone communicates directly with the Call Manager using SIP Protocol that is passed through Ubigate iBG router. The Call Managers communicate with each other across the IP network via SIP to establish and maintain the call. The packets are then routed across the IP network from IP phone to IP phone completing the connection. The second requirement, to support IP phones connected to Ubigate iBG router, is to connect Ubigate iBG router to the PBX or PSTN enabling the IP phones to make calls to traditional phones. In this case, the IP phones communicate with the Call Manager and in turn the Call Manager establishes the call to the PBX or PSTN through Ubigate iBG router. The packets from the IP phone are then routed through DSP and delivered to the PBX or PSTN via analog or digital trunk lines.

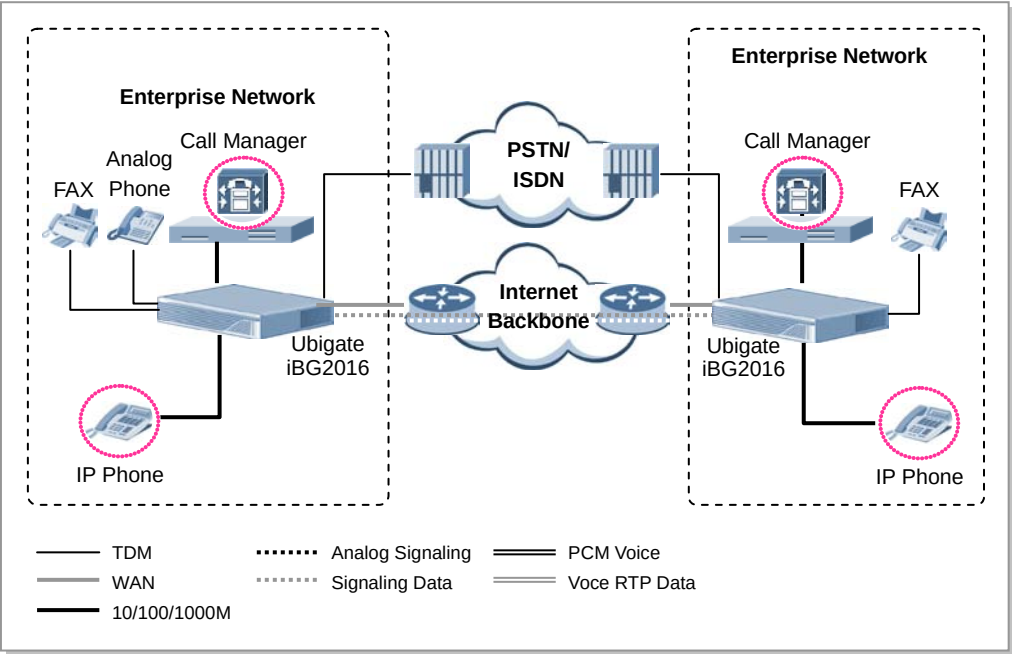


Figure 1.5 Connection to IP Phone, Analog Phone and FAX

Management System

Ubigate iBG routers are controlled via several Management System or a Command Line Interface (CLI) as shown in Figure 1.6. There is an integrated Graphical User Interface (GUI) that enables the user to configure Ubigate iBG routers. The CLI is a text line interface that allows the user to configure and retrieve the status of the individual system to which it is currently connected. The Network Management System uses Simple Network Management Protocol (SNMP) to communicate with Ubigate iBG routers. The SNMP 'get' and 'set' commands can be used to configure either system and retrieve current configuration and status information. These Management Systems can be located anywhere in the IP network.

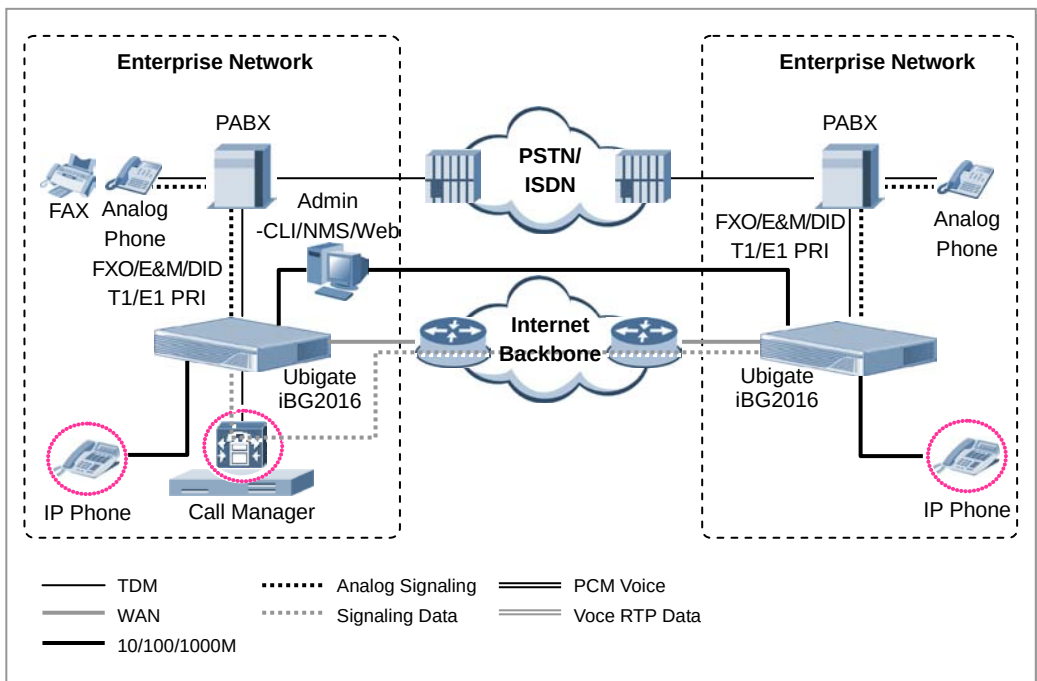


Figure 1.6 Management using CLI/GUI/NMS



CHAPTER 2. VoIP Gateway Management

Introduction to VoIP Gateway Features

VoIP Gateway function is used to deliver voice calls between PSTN and IP network. For interwork with PSTN over IP network, such call processing protocols as SIP, H.323, MGCP, etc. are used over IP network. Ubigate iBG router supports SIP and H.323 out of VoIP Call processing protocols. That is, it routes calls from PSTN to SIP or H.323 section, and terminates the calls incoming from SIP or H.323 network toward PSTN. In addition, a Ubigate iBG router provides a VoIP call service via interwork with SIP Proxy, SIP registrar, SIP Gateway, SIP terminal, H.323 Gatekeeper, H.323 Gateway, etc.

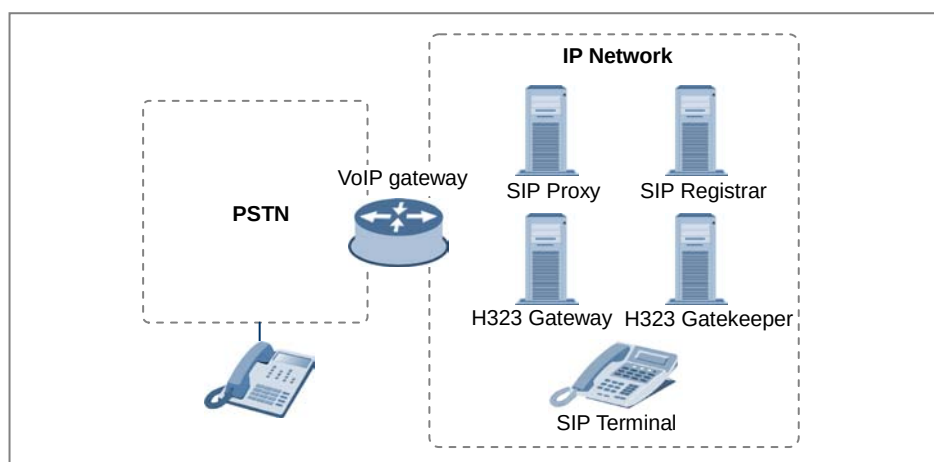


Figure 2.1 Architecture of VoIP Network

The common matters regarding VoIP Gateway will be discussed in this section, and the details of working as SIP and H.323 gateway will be described in the next section.

Configuring VoIP Gateway

Configuring VoIP source address

This section describes how to configure source IP address for VoIP gateway. With this feature, you can specify the source address of SIP and H323 signaling, and media stream - RTP/RTCP. You can assign an existing IP address on a specific interface by the 'bind' command or create a new IP address by the 'host ip-address' command.

Restrictions for VoIP source address

The interfaces which you can bind with as the source address of VoIP signaling and media stream are Ethernet, bundle, VLAN, and virtual-access interface. The 'host ip-address' command will create a new IP address.

Prerequisites for VoIP source address

VoIP gateway must be shut down before setting the VoIP source address. Interface bound with VoIP-gateway cannot be removed before VoIP-gateway unbinds the interface.

How to Configure VoIP source address

1. setting the IP Address of the interface to be bound
This procedure should be done first before using the bind command.
No need for the 'host ip-address' command.
 - Configuration Steps
 - configure terminal
 - interface
 - ip address
 - exit
 - Detailed Steps

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters global configuration mode.
2	Interface <i>type number</i> Example) /configure# interface Ethernet 0/0	Enters interface configuration mode to configure specific interface.
3	ip address <i>ip_address subnet_mask</i> Example) /configure/interface/ethernet(0/0)# ip address 90.90.90.90 255.255.255.0	Configure a IP Address for an interface.
4	exit Example) /configure/interface/ethernet(0/0)# exit	Exits the current mode

2. shutdown voip-gateway

voip-gateway must be shutdown before setting the voip-gateway IP address.

- Configuration Steps
 - configure terminal
 - voip-gateway
 - shutdown
 - exit
- Detailed Steps

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters global configuration mode.
2	voip-gateway Example) /configure# voip-gateway	Enters voip-gateway configuration mode.

(Continued)

Step	Command	Purpose
3	shutdown Example) /configure/voip-gateway# shutdown	Shuts down voip call services
4	exit Example) /configure/interface/ethernet(0/0)# exit	Exits the current mode

3. bind interface

To bind the interface for source address of VoIP signaling and media.

- Configuration Steps
 - configure terminal
 - voip-gateway
 - bind control
 - bind media
 - exit
- Detailed Steps

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters global configuration mode.
2	voip-gateway Example) /configure# voip-gateway	Enters voip-gateway configuration mode.
3	bind control interface <i>type num</i> Example) /configure/voip-gateway# bind control interface ethernet 0/0	Sets source interface for SIP and H.323.

(Continued)

Step	Command	Purpose
3	bind media interface <i>type num</i> Example) /configure/voip-gateway# bind control interface ethernet 0/0	Sets source interface for media - RTP/RTCP.
4	exit Example) /configure/voip-gateway# exit	Exits the current mode

4. host domain-name

VoIP gateway must have a domain name. 'samsung.com' or IP address form should be used.

- Configuration Steps
 - configure terminal
 - voip-gateway
 - host domain-name
 - exit
- Detailed Steps

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters global configuration mode.
2	voip-gateway Example) /configure# voip-gateway	Enters voip-gateway configuration mode.
3	host domain-name <i>DOMAIN.COM</i> Example) /configure/voip-gateway# host domain-name samsung.com	Sets domain name for Ubigate iBG
4	exit Example) /configure/voip-gateway# exit	Exits the current mode

5. host ip-address

Instead of binding an interface, you can directly create a new IP address for the source address for VoIP gateway.

- Configuration Steps
 - configure terminal
 - voip-gateway
 - host ip-address
 - exit
- Detailed Steps

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters global configuration mode.
2	voip-gateway Example) /configure# voip-gateway	Enters voip-gateway configuration mode.
3	host ip-address <i>ip-address</i> Example) /configure/voip-gateway# host ip-address ipv4:90.90.90.90	Sets source ip address for signaling and media streams.
4	exit Example) /configure/voip-gateway# exit	Exits the current mode

Enabling or Disabling VoIP Services

There are two ways of enabling or shutting down VoIP service. One uses a shutdown command in voip-gateway configuration mode, the other one uses a shutdown command in sip-ua configuration mode or h323-gateway configuration mode. The shutdown command in a sip-ua configuration mode enables or disables only the SIP service and the shutdown command in an h323-gateway configuration mode enables or disables only the H323 service; and the shutdown command in a voip-gateway configuration mode enables or disables not only SIP service, but also H323 service, that is, the entire VoIP call service. This section describes only the shutdown command in voip-gateway configuration mode.

How to Enable or Disable All VoIP call services

The procedure to enable or disable all VoIP call services including SIP service is as follows. If you want to terminate the current call together with stopping the service, use the forced parameter.

- Configuration Steps
 - configure terminal
 - voip-gateway
 - [no] shutdown
 - exit
- Detailed Steps

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters global configuration mode.
2	voip-gateway Example) /configure# voip-gateway	Enters voip-gateway configuration mode.
3	[no] shutdown Example) /configure/voip-gateway# no shutdown	Shuts down or enables voip call services
4	Exit Example) /configure/voip-gateway# exit	Exits the current mode

Configuring Call Server (Ubigate iPX)

This section describes how to configure iBG router to interwork with call-server (Ubigate iPX).

Before setting iBG, you must configure iPX in advance.

Here is the essential information to start configuration:

IP address, port number, and transport type of Ubigate iPX

Domain name

Ubigate iBG's gw-uri name and password for HTTP digest authentication

- gw-uri is a representative name of Ubigate iBG and iPX maintains iBG as an Endpoint.

FXS subscriber's number and password

Trunk access code number. Trunk URI name if it needs to register the trunk

Check if TCP 8088 port is being used for the management channel.

Timer values such as registration refresh timer and failure retry timer.

Other parameters such as type of DTMF relay, use of Session Timer, list of IP phones that are maintained by iBG when in survivable telephony mode.

Prerequisites for Call Server Configurations

You should shutdown voip-gateway before configuring call-server, and the VoIP gateway source address must be set in advance.

How to Configure Call Server

You can set the call server in the following ways:

- Configuration Steps
 - configure terminal
 - voip-gateway
 - call-server ip-address
 - call-server gw-uri
 - exit
- Detailed Steps

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters global configuration mode.
2	voip-gateway Example) /configure# voip-gateway	Enters voip-gateway configuration mode.
3	call-server ip-address <i>ip-addr</i> [udp tcp tls] [sip sips] [expires <i>expires</i>] [retry <i>retry</i>] Example) /configure/voip-gateway# call-server ip-address ipv4:90.90.90.100	Sets an Ubigate iPX IP Address. Expires and retry timer for FXS subscribers may be set. Use voice service SIP global configuration for transport type and uri.
4	call-server gw-uri <i>uri</i> [expires <i>expires</i>] [retry <i>retry</i>] Example) /configure/voip-gateway# call-server gw-uri iBG2016	Set gw-uri and Ubigate iBG will register to Ubigate iPX as an Endpoint. Expires and retry timer of GW-URI may be set.
5	exit Example) /configure/voip-gateway# exit	Exits the current mode.



CHAPTER 3. SIP Gateway Management

Introduction to SIP Gateway Features

Information about SIP

SIP is a simple and text-based protocol that uses requests and responses to establish communication among the various components in the network and to ultimately establish a conference between two or more endpoints.

SIP Capabilities

- Determines the location of the target endpoint
SIP supports address resolution, name mapping, and call redirection.
- Determines the media capabilities of the target endpoint
SIP determines the lowest level of common services between the endpoints through Session Description Protocol (SDP). Conferences are established using only the media capabilities that can be supported by all endpoints.
- Determines the availability of the target endpoint
If a call cannot be completed because the target endpoint is unavailable, SIP determines whether the called party is connected to a call already or did not answer in the allotted number of rings. SIP then returns a message indicating why the target endpoint was unavailable.
- Establishes a session between the originating and target endpoints
If the call can be completed, SIP establishes a session between the endpoints. SIP also supports mid-call changes, such as the addition of another endpoint to the conference or the changing of a media characteristic or codec.

- Handles the transfer and termination of calls
SIP supports the transfer of calls from one endpoint to another. During a call transfer, SIP simply establishes a session between the transferee and a new endpoint (specified by the transferring party) and terminates the session between the transferee and the transferring party. At the end of a call, SIP terminates the sessions among all parties.

SIP Components

SIP is a peer-to-peer protocol. The peers in a session are called user agents. A user agent can function in one of the following roles:

- User-agent client (UAC)
A UAC is capable of generating a request based on some external stimulus (the user clicking a button, or a signal on a PSTN line) and processing a response.
- User-agent server (UAS)
A UAS is capable of receiving a request and generating a response based on user input, external stimulus, the result of a program execution, or some other mechanism.

Typically, a SIP endpoint is capable of functioning as both a UAC and a UAS, but functions only as one or the other per transaction. Whether the endpoint functions as a UAC or a UAS depends on the user agent that initiated the request.

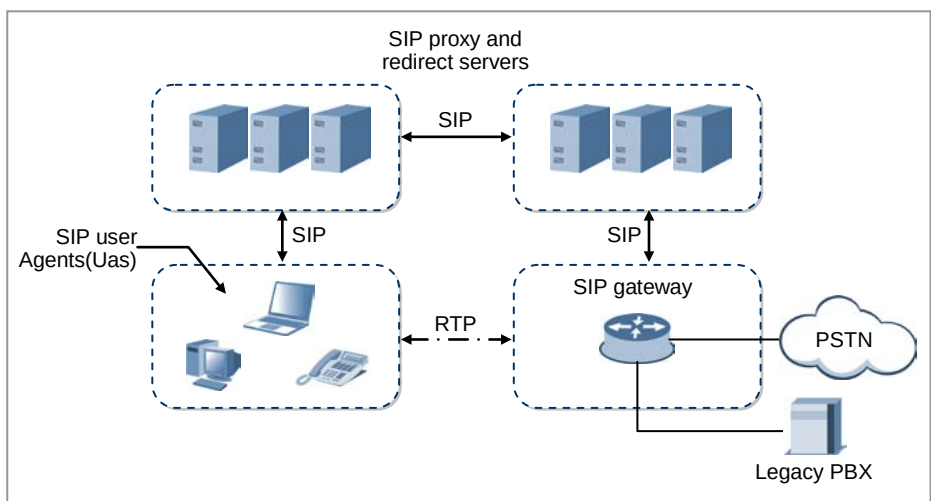


Figure 3.1 Architecture of SIP Network

From an architectural standpoint, the physical components of a SIP network can be grouped into two categories: clients (endpoints) and servers. Figure 3.1 illustrates the architecture of a SIP network.

1. SIP Client

- Phones
 - User agent which can attempt or receive a call voluntarily.
- Gateways
 - Intermediary entity which can perform a translation function between SIP conferencing endpoints and terminals of another type.
A gateway performs the translation between transmission formats and translation between communications procedures. In addition, the gateway translates between audio and video codecs and performs call setup and clearing on both the LAN side and the switched-circuit network side.

2. SIP Server

- Proxy server
 - An intermediary entity that acts as both a server and a client for the purpose of making requests on behalf of other clients. Proxy servers can provide functions such as authentication, authorization, network access control, routing, reliable request retransmission, and security.
- Redirect server
 - A user agent server that provides the client with information about the next hop or hops that a message should take and then the client contacts the next-hop server directly.
- Registrar server
 - A server that accepts REGISTER requests and places the information it receives in those requests into the location service for the domain it handles. Registrar servers are often co-located with a redirect or proxy server.

How SIP Works

On SIP network, SIP user has a unique SIP address. SIP address has a form similar to that of an e-mail address. The typical form of a SIP address is sip:userID@hostname. The userID can be a user name or E.164 address. The Hostname can be the IP address or domain address.

The SIP user registers his SIP address and current location information to a registrar server. The registrar server provides information to the SIP server (either a proxy or a redirect server), and the SIP server maps the SIP address of the request received from a user agent to the current location information.

This is called a location service.

When the SIP user attempts a call, it sends a SIP request to the SIP server. The SIP request header field includes the caller information, and the To header field includes the callee information. In the SIP server, a location service necessary for signaling routing is executed. After the request is sent to a proxy server, the proxy server proceeds with the call using the address resulting from the location service. Finally, the SIP request is delivered to a callee, to complete a call setup.

After a request is sent to a redirect server, the redirect server sends the location service result to a caller using the Contact header field of a response.

The redirect server does not participate in the call anymore. The caller sends a new SIP request to the address specified in the Contact header field.

How SIP Works with a Call Manager

If the Call Manager is used, a user agent sends a REGISTER request to the Call Manager. Here, the REGISTER request includes the SIP address and current location information of a caller. All the calls attempted by a user agent are made via the Call Manager. A caller sends a INVITE request to the Call Manager, and the Call Manager determines a path via a location service. The Call Manager delivers a request to a callee using the determined path. A callee sends a response to Call Manager, and the response is delivered to a caller. A caller sends ACK for the response. A session between a caller and callee is established, and session data is delivered to the caller and callee using Real-time Transfer Protocol (RTP).

How SIP Works with a Proxy Server

If a proxy server is used, the caller user agent sends an INVITE request to the proxy server, the proxy server determines the path, and then forwards the request to the called party. The called party responds to the proxy server, which in turn, forwards the response to the caller. The proxy server forwards the acknowledgments of both parties. A session is then established between the caller and called party. Real-time Transfer Protocol (RTP) is used for the communication between the caller and the called party. Figure 3.2, Figure 3.3 and Figure 3.4 illustrate how SIP works with a Proxy Server.

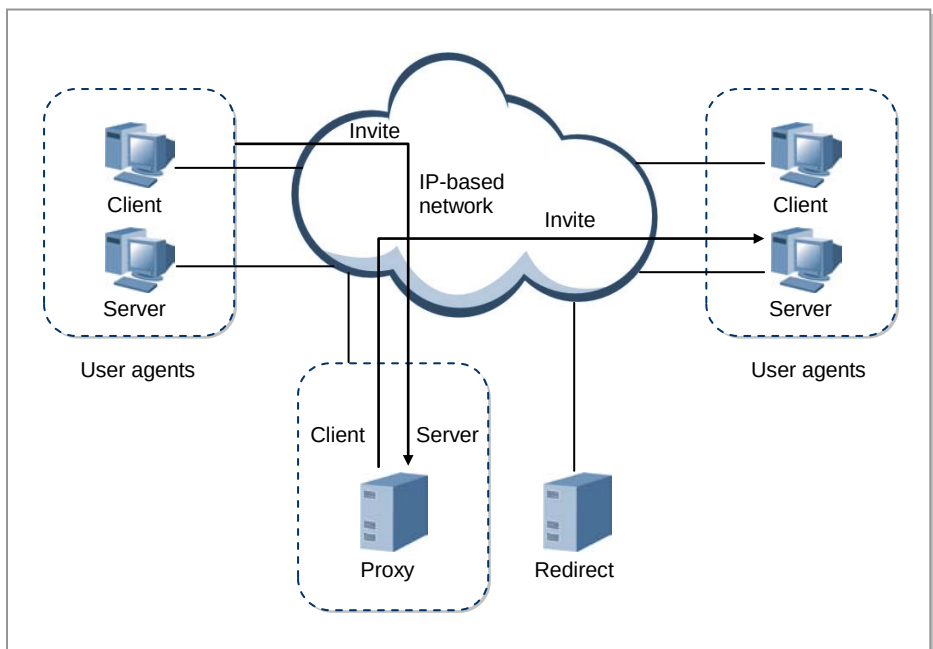


Figure 3.2 SIP Request Through a Proxy Server

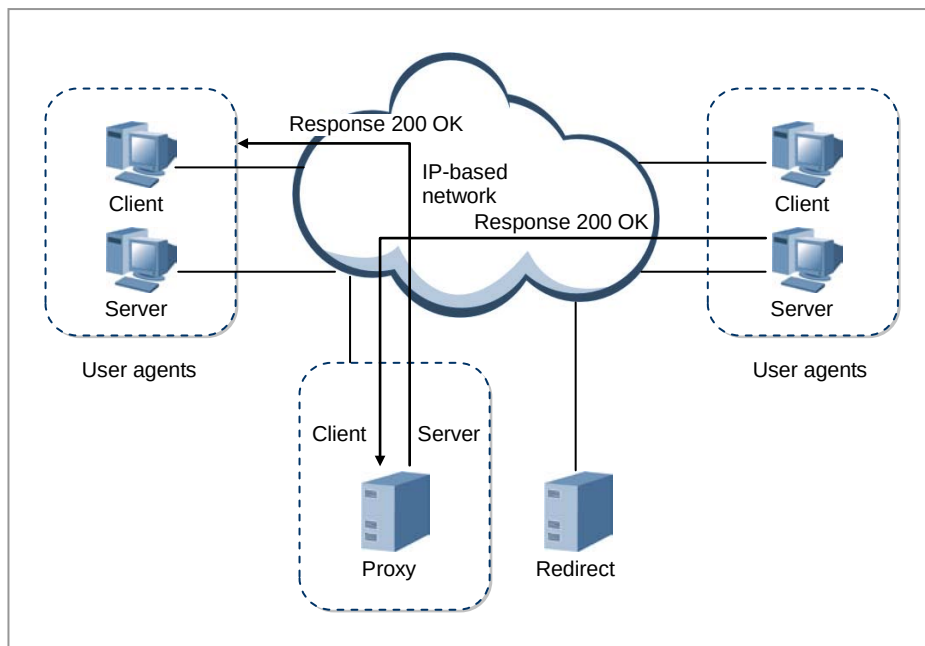


Figure 3.3 SIP Response Through a Proxy server

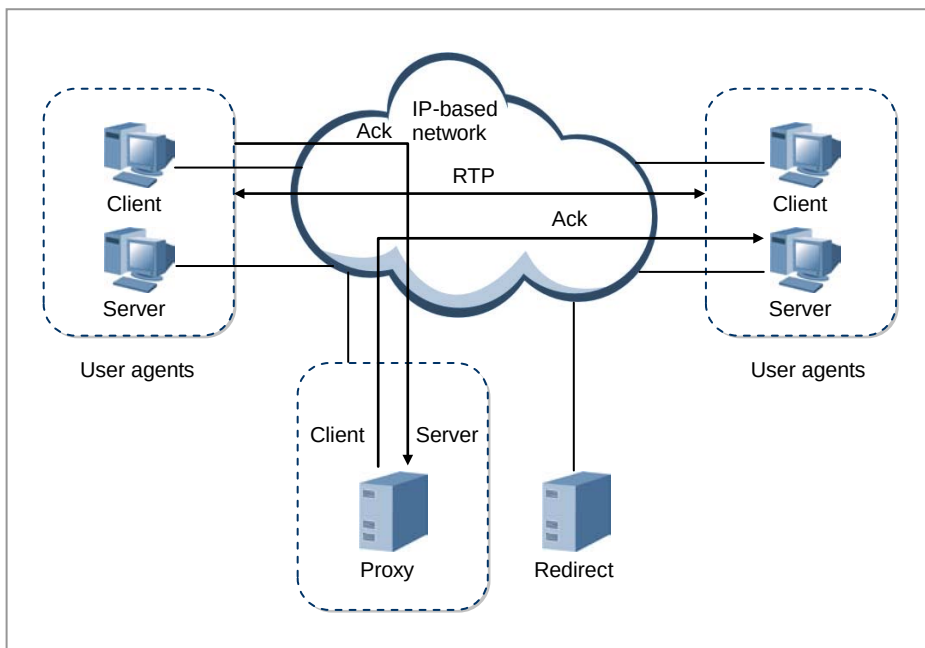


Figure 3.4 SIP Session Through a Proxy Server

How SIP Works with a Redirect Server

If a redirect server is used, the caller user agent sends an INVITE request to the redirect server, the redirect server contacts the location server to determine the path to the called party, and then the redirect server sends that information back to the caller. The caller then acknowledges receipt of the information. The caller then sends a request to the device indicated in the redirection information (which could be the callee or another server that forwards the request). Once the request reaches the called party, it sends back a response and the caller acknowledges the response. RTP is used for the communication between the caller and the callee. Figure 3.5 and Figure 3.6 illustrate how SIP works with a Redirect Server.

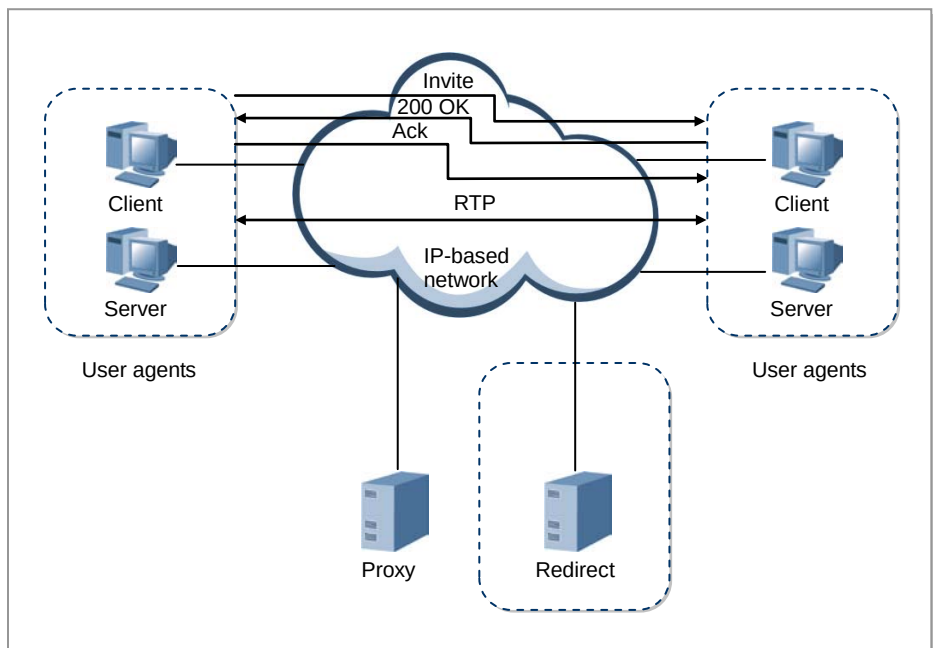


Figure 3.5 SIP Session Through a Redirect Server

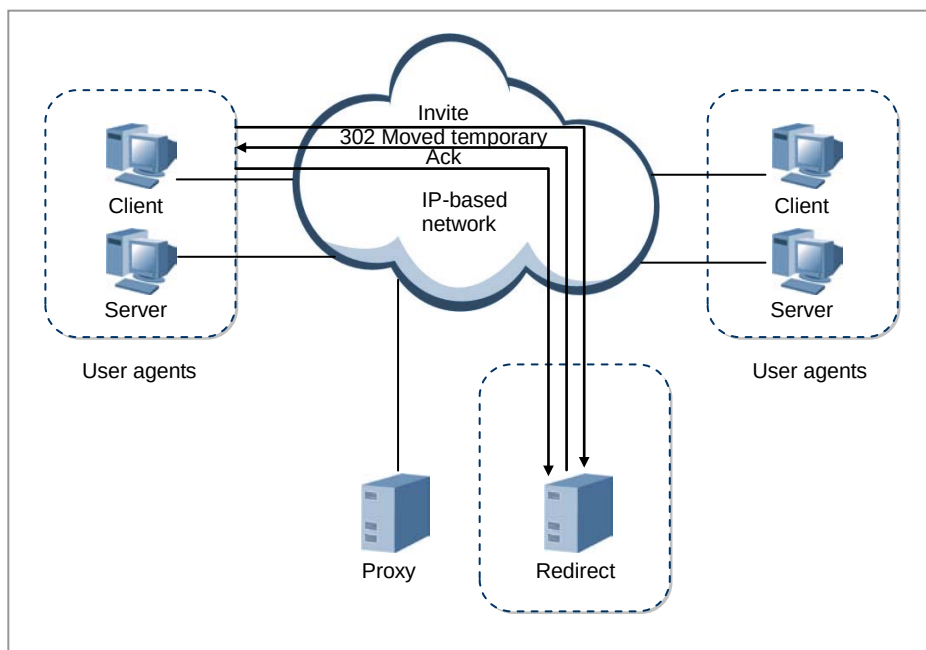


Figure 3.6 SIP Request Through a Redirect Server

SIP Call Flows

This section describes the basic SIP call flow in a SIP gateway.

SIP Gateway to SIP Gateway-Call Setup and Disconnect

Figure 3.7 shows a successful gateway-to-gateway call setup and disconnect. The two end users are User A and User B. User A is located at PBX A, which is connected to SIP gateway 1 via a T1/E1. User B is located at PBX B, which is connected to SIP gateway 2 via a T1/E1. Table 28.1 briefly describes the messages used in the call flow.

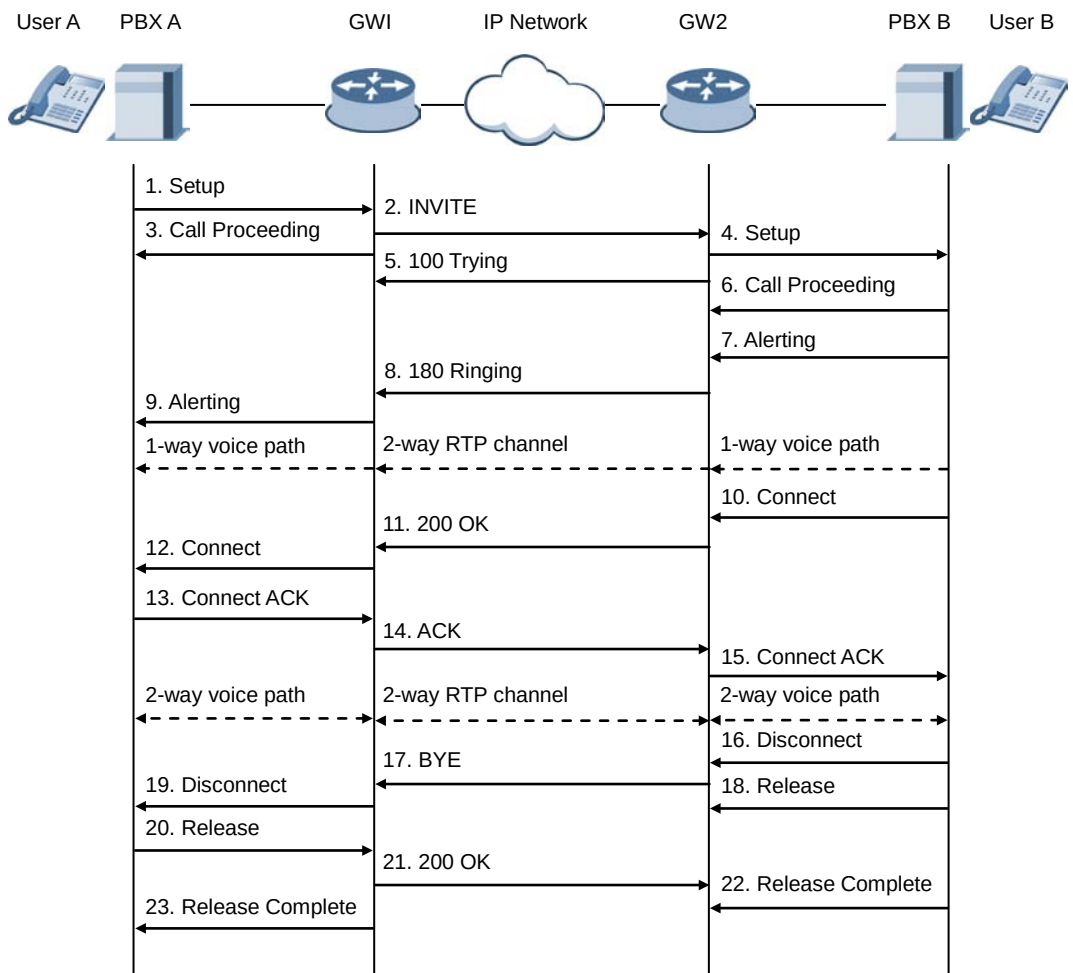


Figure 3.7 SIP Gateway-to-SIP Gateway-Call Setup and Disconnect

Table 3.1 Call Setup and Disconnect

No.	Message	Description
1	Setup	SIP Gateway 1 receives Setup from PBX A. Setup indicates the call attempt from User A to User B.
2	INVITE	SIP Gateway 1 sends INVITE request to SIP Gateway 2. INVITE request indicates the call attempt from User A to User B. INVITE includes the media capability of SIP Gateway 1.
3	Call Proceeding	SIP Gateway 1 sends Call Proceeding to PBX A. Call Proceeding indicates that SIP Gateway 1 received Setup and attempts SIP signaling call.
4	Setup	SIP Gateway 2, upon receiving INVITE, sends Setup to PBX B.
5	100 Trying	SIP Gateway 2 sends a response to INVITE request to SIP Gateway 1. 100 Trying response indicates that SIP Gateway 2 has received the INVITE request.
6	Call Proceeding	SIP Gateway 2 receives Call Proceeding from PBX B. Call Proceeding indicates that PBX B, after receiving Setup, proceeds with a call.
7	Alerting	SIP Gateway 2 receives Alerting from PBX B. Alerting indicates that User B is ringing.
8	180 Ringing	SIP Gateway 2 sends 180 Ringing to SIP Gateway 1. 180 Ringing indicates that a callee is located at SIP Gateway 2, and the User B is currently alerted.
9	Alerting	Upon receiving 180 Ringing, SIP Gateway 1 sends Alerting to PBX A.
10	Connect	If a called subscriber replies, SIP Gateway 2 receives Connect from PBX B. Connect indicates that a call was received from User B.
11	200 OK	SIP Gateway 2 sends 200 OK to SIP Gateway 1. 200 OK indicates that a session was formed normally between SIP Gateway 2 and SIP Gateway 1. 200 OK includes the media capability of SIP Gateway 2.
12	Connect	Upon receiving 200 OK, SIP Gateway 1 sends Connect to PBX A.
13	Connect ACK	SIP Gateway 1 receives Connect ACK from PBX A. Connect ACK indicates that Connect was received normally.
14	ACK	SIP Gateway 2 sends ACK request to SIP Gateway 2. ACK request indicates that SIP Gateway 1 received 200 OK response normally.

Table 3.1 Call Setup and Disconnect (Continued)

No.	Message	Description
15	Connect ACK	Upon receiving ACK, SIP Gateway 2 sends Connect ACK to PBX B.
16	Disconnect	If a subscriber hangs up the phone, SIP Gateway 2 receives Disconnect from PBX B. Disconnect indicates that User B requested a call release.
17	BYE	SIP Gateway 2 sends BYE request to SIP Gateway 1. BYE request indicates the end of a session.
18	Release	SIP Gateway 2 sends Release to PBX B. Release indicates the end of a call.
19	Disconnect	Upon receiving BYE, SIP Gateway 1 sends Disconnect to PBX A.
20	Release	SIP Gateway 1 receives Release from PBX A.
21	200 OK	SIP Gateway 1 sends 200 OK to SIP Gateway 2. 200 OK indicates that a session was terminated normally by BYE request.
22	Release Complete	SIP Gateway 2 receives Release Complete from PBX B. Release Complete indicates that the call was released normally.
23	Release Complete	Upon receiving Release, SIP Gateway 1 sends Release Complete to PBX A.

SIP Gateway to SIP Gateway-Call via Redirect Server

Figure 3.8 shows the SIP Gateway to SIP Gateway call using the SIP Redirect server. Table 28.2 briefly describes the messages used in the call flow.

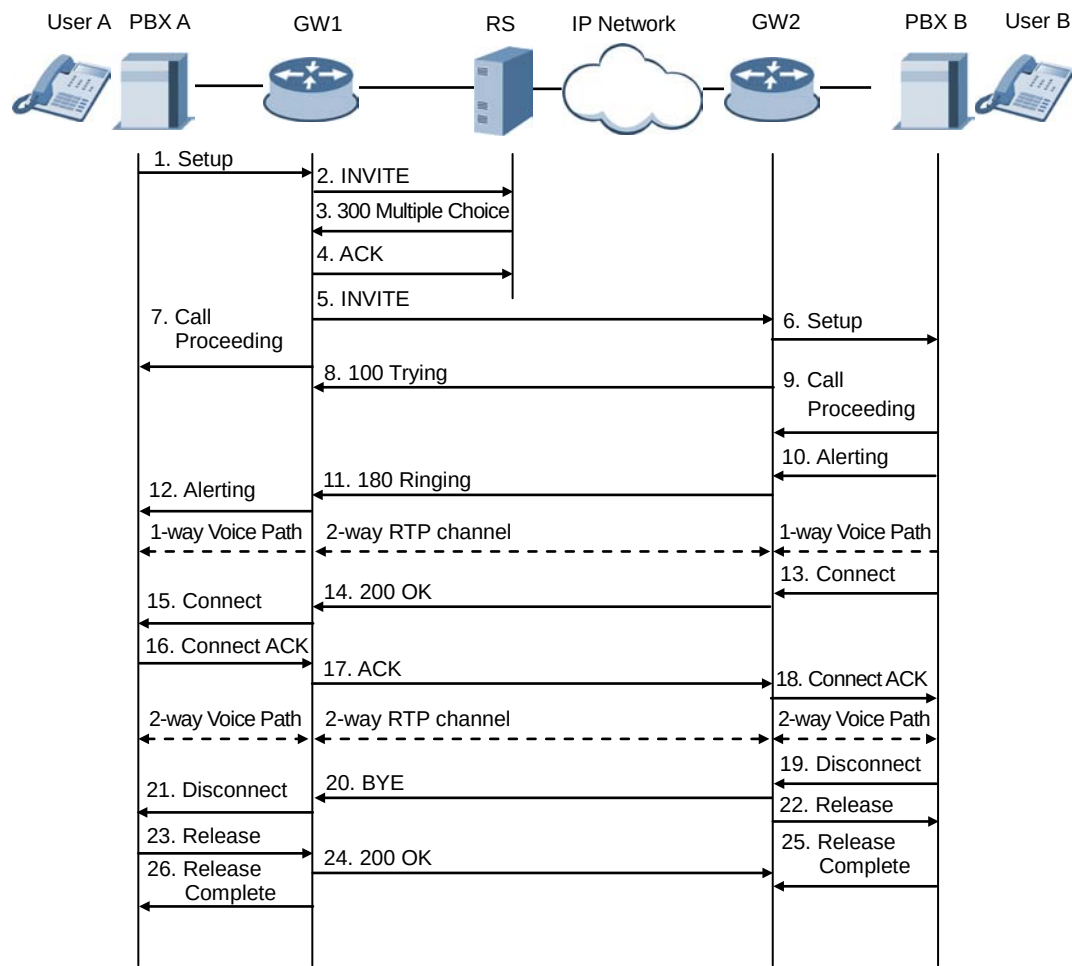


Figure 3.8 SIP Gateway-to-SIP Gateway-Call Via SIP Redirect Server

Table 3.2 Call via Redirect Server

No.	Message	Description
1	Setup	SIP Gateway 1 receives Setup from PBX A. Setup indicates the call attempt from User A to User B.
2	INVITE	SIP Gateway 1 sends INVITE request to a redirect server. INVITE request indicates the call attempt from User A to User B. INVITE includes the media capability of SIP Gateway 1.
3	300 Multiple Choice	Redirect server sends 300 Multiple choice to SIP Gateway 1. 300 Multiple choice response includes the information necessary for routing to User B which a redirect server knows.
4	ACK	SIP Gateway 1 sends ACK request to a redirect server. ACK request indicates that Gateway 1 received 300 Multiple choice response normally.
5	INVITE	SIP Gateway 1 sends INVITE request to SIP Gateway 2. SIP Gateway 1 gets SIP Gateway 2 information from 300 Multiple choice response. INVITE request indicates the call attempt from User A to User B. INVITE includes the media capability of SIP Gateway1.
6	Setup	SIP Gateway 2, upon receiving INVITE, sends Setup to PBX B.
7	Call Proceeding	SIP Gateway 1 sends Call Proceeding to PBX A. Call Proceeding indicates that SIP Gateway 1 received Setup and attempts SIP signaling call.
8	100 Trying	SIP Gateway 2 sends a response to INVITE request to SIP Gateway 1. 100 Trying response indicates that SIP Gateway 2 has received the INVITE request.
9	Call Proceeding	SIP Gateway 2 receives Call Proceeding from PBX B. Call Proceeding indicates that PBX B, after receiving Setup, proceeds with a call.
10	Alerting	SIP Gateway 2 receives Alerting from PBX B. Alerting indicates that User B is ringing.
11	180 Ringing	SIP Gateway 2 sends 180 Ringing to SIP Gateway 1. 180 Ringing indicates that a callee is located at SIP Gateway 2, and User B is currently alerted.
12	Alerting	Upon receiving 180 Ringing, SIP Gateway 1 sends Alerting to PBX A.
13	Connect	When a called party replies, SIP Gateway 2 receives Release Connect from PBX B.

Table 28.2 Call via Redirect Server (Continued)

No.	Message	Description
14	200 OK	SIP Gateway 2 sends 200 OK to SIP Gateway 1. 200 OK indicates that a session was formed normally between SIP Gateway 2 and SIP Gateway 1. 200 OK includes the media capability of SIP Gateway 2.
15	Connect	Upon receiving 200 OK, SIP Gateway 1 sends Connect to PBX A.
16	Connect ACK	SIP Gateway 1 receives Connect ACK from PBX A.
17	ACK	SIP Gateway 2 sends ACK request to SIP Gateway 2. ACK request indicates that SIP Gateway 1 received 200 OK response normally.
18	Connect ACK	SIP Gateway 2 sends Connect ACK from PBX B.
19	Disconnect	If a subscriber hangs up the phone, SIP Gateway 2 receives Disconnect from PBX B.
20	BYE	SIP Gateway 2 sends BYE request to SIP Gateway 1. BYE request indicates the end of a session.
21	Disconnect	Upon receiving BYE, SIP Gateway 2 sends Disconnect to PBX A.
22	Release	Sends a Release in regard to Disconnect.
23	Release	Receives a Release in regard to Disconnect.
24	200 OK	SIP Gateway 1 sends 200 OK to SIP Gateway 2. 200 OK indicates that a session was terminated normally by BYE request.
25	Release Complete	Receives Release Complete in regard to Release.
26	Release Complete	Sends Release Complete in regard to Release.

SIP Gateway to SIP Gateway-Call via Proxy Server

Figure 3.9 shows the call of SIP Gateway to SIP Gateway using SIP Proxy server. Table 28.3 briefly describes the messages used in the call flow.

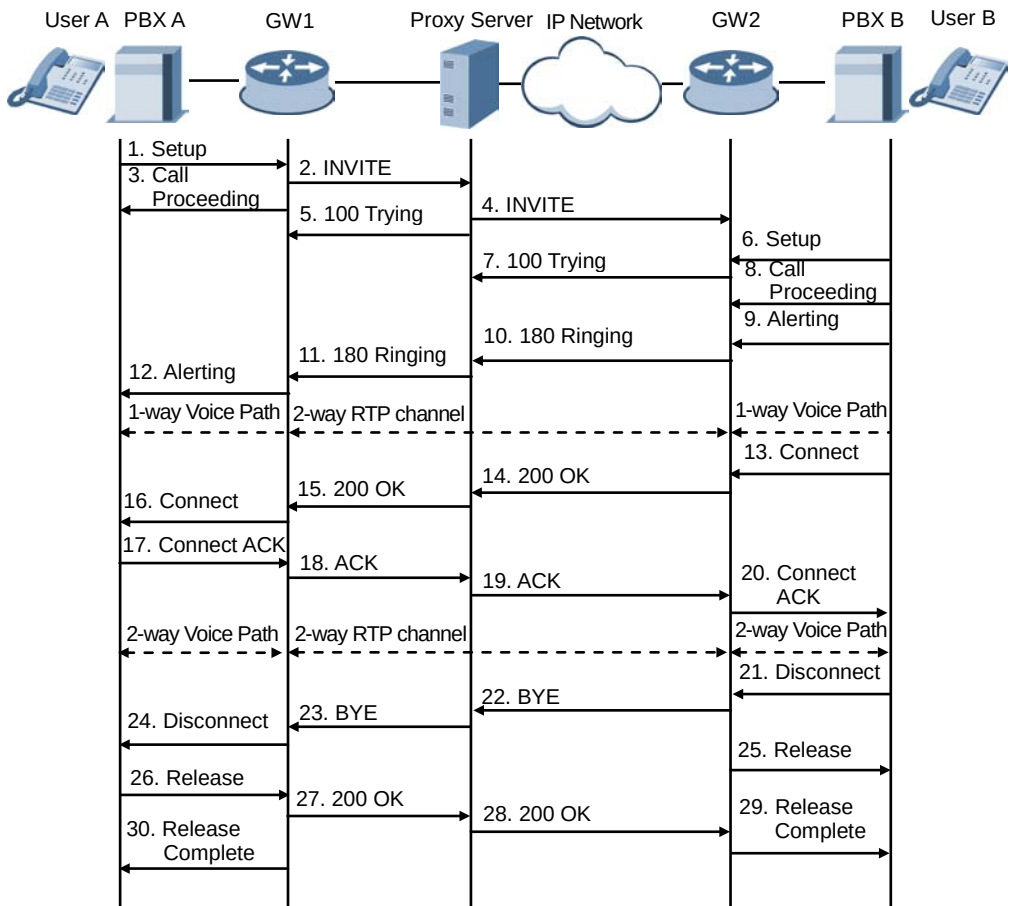


Figure 3.9 SIP Gateway-to-SIP Gateway-Call via SIP Proxy Server with Record Route Enabled

Table 3.3 Call via Proxy Server

No.	Message	Description
1	Setup	SIP Gateway 1 receives Setup from PBX A. Setup indicates the call attempt from User A to User B.
2	INVITE	SIP Gateway 1 sends INVITE request to a Proxy server. INVITE request indicates the call attempt from User A to User B. INVITE includes the media capability of SIP Gateway1.
3	Call Proceeding	SIP Gateway 1 sends Call Proceeding to PBX A. Call Proceeding indicates that SIP Gateway 1 received Setup and attempts SIP signaling call.
4	INVITE	Proxy Server searches a proper SIP gateway and delivers INVITE request.
5	100 Trying	Proxy Server sends 100 Trying to SIP Gateway 1. 100 Trying indicate that a proxy server is processing INVITE request.
6	Setup	Upon receiving INVITE from a proxy server, Gateway 2 sends Setup to PBX B.
7	100 Trying	Upon receiving INVITE from a proxy server, SIP Gateway 2 replies with 100 Trying.
8	Call Proceeding	SIP Gateway 2 receives Call Proceeding from PBX B.
9	Alerting	SIP Gateway 2 receives Alerting from PBX B.
10	180 Ringing	Upon receiving Ringing, SIP Gateway 2 sends 180 Ringing to a proxy server. 180 Ringing indicates that a callee is located at SIP Gateway 2, and the User B is currently alerted.
11	180 Ringing	Proxy Server transfers 180 Ringing to SIP Gateway 1.
12	Alerting	Upon receiving 180 Ringing, Gateway 1 sends Alerting to PBX A.
13	Connect	When a called party replies, SIP Gateway 2 receives Release Connect from PBX B.
14	200 OK	SIP Gateway 2 sends 200 OK to Proxy Server. 200 OK indicates the response of a called party. 200 OK includes the media capability of SIP Gateway 2.
15	200 OK	Proxy Server 2 sends 200 OK to SIP Gateway 1.
16	Connect	Upon receiving 200 OK, SIP Gateway 1 sends Connect to PBX A.
17	Connect ACK	SIP Gateway 1 receives Connect ACK from PBX A.

Table 28.3 Call via Proxy Server (Continued)

No.	Message	Description
18	ACK	SIP Gateway 1 sends ACK request to a Proxy server. ACK request indicates that SIP Gateway 1 received 200 OK response normally.
19	ACK	Proxy server sends ACK request to a SIP Gateway 2.
20	Connect ACK	SIP Gateway 2 sends Connect ACK from PBX B.
21	Disconnect	If a subscriber hangs up the phone, SIP Gateway 2 receives Disconnect from PBX B.
22	BYE	SIP Gateway 2 sends BYE request to a Proxy server. BYE request indicates the end of a session.
23	BYE	Proxy Server 2 sends Bye Request to SIP Gateway 1.
24	Disconnect	Upon receiving BYE, SIP Gateway 1 sends Disconnect to PBX A.
25	Release	Receives a Release in regard to Disconnect.
26	Release	Receives a Release in regard to Disconnect.
27	200 OK	SIP Gateway 1 sends 200 OK to Proxy Server. 200 OK indicates that a session was terminated normally by BYE request.
28	200 OK	Proxy Server 2 sends 200 OK to SIP Gateway 2.
29	Release Complete	Receives Release Complete in regard to Release.
30	Release Complete	Receives Release Complete in regard to Release.

Gateway Features

SIP Gateway provides the following features:

- Support early media session.
- Support out of band DTMF relay.
- Support for Reliability of provisional response in SIP.
- Ability to specify the maximum number of SIP redirects.
- Ability to specify SIP on a dial-peer basis.
- Configurable SIP transaction timers.
- Support for a variety of signaling protocols, including ISDN, PRI, and channel associated signaling (CAS).
- Support for a variety of interfaces, including
 - Analog interfaces: Foreign Exchange Station (FXS)/Foreign Exchange Office (FXO)/recEive and transMit (E & M) analog interfaces.
 - Digital interfaces: T1 CAS, T1 PRI, E1 CAS, E1 PRI, and E1 R2
- Support for SIP redirection messages and interaction with SIP proxies. The gateway can redirect an unanswered call to another SIP gateway or SIP-enabled IP phone. In addition, the gateway supports proxy-routed calls.
- Support for SIP over TCP and User Datagram Protocol (UDP).
- Support RTP/RTCP for media transport in VoIP networks.
- Support for the following codecs:
 - G711ulaw
 - G711alaw
 - G723
 - G726-32
 - G729
- Support for record-route headers.
- Support for IP quality of service (QoS) and IP precedence.
- Support S/MIME, SRTP, IP Security (IPSec) for secure SIP signaling.
- Authentication, authorization, and accounting (AAA) support. For accounting, the gateway device generates call data record (CDR) accounting records for export. For authentication, the SIP gateway sends validation requests to the AAA server. For authorization, the existing access lists are used.
- Support for configurable expiration time for SIP REGISTERS and maximum number of proxies or redirect servers that can forward a SIP request.

- Ability to hide the identity of the calling party by RFC 3325-Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks.
- Support for sips uri over TLS.
- capability to periodically refresh SIP sessions by sending repeated UPDATE requests.
- Support for QSig inter-working and QSig tunneling over SIP.
- Support for the following RFCs and Drafts

No.	Rec	Description
1	RFC2327	Session Description Protocol
2	RFC2543	Session Initiation Protocol
3	RFC2976	The SIP INFO Method
4	RFC3261	Session Initiation Protocol
5	RFC3262	Reliability of Provisional Responses in SIP
6	RFC3263	Locating SIP Servers
7	RFC3264	An Offer Answer Model with the SIP
8	RFC3265	SIP - Specific Event Notification
9	RFC3266	Support of IPv6 in SDP
10	RFC3311	The SIP UPDATE Method
11	RFC3323	A Privacy Mechanism for the SIP
12	RFC3325	Private Extensions to the SIP for Asserted Identity within Trusted Networks
13	RFC3326	The Reason Header Field for the SIP
14	RFC3420	Internet Media Type Message sipfrag
15	RFC3428	SIP Extension for Instant Messaging
16	RFC3515	The SIP Refer Method
17	RFC3578	Mapping of ISUP Overlap Signaling to the SIP
18	RFC3665	SIP Basic Call Flow Examples
19	RFC3666	SIP Public Switched Telephone Network (PSTN) Call Flows
20	RFC3725	Third Party Call Control in the SIP
21	RFC3824	Using E.164 numbers with the SIP
22	RFC3842	A Message Summary and MWI Event Package for the SIP
23	RFC3891	The SIP 'Replace' Header
24	RFC3892	The SIP Referred-By Mechanism

(Continued)

No.	Rec	Description
25	RFC3842	A Message Summary and Message Waiting Indication Event Package for the Session Initiation Protocol (SIP)
26	RFC4028	Session Timers in SIP
27	RFC4568	Security Descriptions for Media Stream
28	Draft-ietf-sipping-conference-package-10	A SIP Event Package for Conference State
29	Draft-ietf-sip-history-info-06	An Extension to the SIP Request History Information
30	Draft-ietf-sipping-service-examples-08	SIP Service Examples
31	Draft-ietf-sipping-cc-transfer-04	SIP Call Control - Transfer
32	Draft-ietf-sip-privacy-04	SIP Extensions for Network-Asserted Caller Identity and Privacy within Trusted Network

Configuring Basic SIP Gateway

Configuring SIP Server

This section describes how to set a SIP server in stand-alone mode.

Ubigate iBG can configure two different SIP servers, one is the SIP outbound proxy server and the other is the SIP Registrar.

Ubigate iBG registers to the SIP Registrar and route calls to the SIP outbound proxy server.

Restrictions for SIP Proxy Configuration

Standard RFC3261 based SIP server is supported with a number of extensions that iBG support. Use SIP server mode when iBG interoperates with commercial or free SIP server, but there could be interoperability issues. You must not set the SIP server for Ubigate iPX. iPX cannot provide its all voice features with SIP-server setting. 'Call-server' must be set for Ubigate iPX.

Survivable telephony cannot be supported with the SIP server.

How to Configure SIP Proxy

You can set the SIP Proxy in the following way.

- Configuration Steps
 - configure terminal
 - voip-gateway
 - sip-ua
 - sip-server
 - exit
 - exit
- Detailed Steps

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters global configuration mode.
2	voip-gateway Example) /configure# voip-gateway	Enters voip-gateway configuration mode.
3	sip-ua Example) /configure/ voip-gateway# sip-ua	Enters sip-ua configuration mode.
4	sip-server <i>ip-address</i> ip-addr [udp tcp tls] [sip sips] Example) /configure/voip-gateway/sip-ua# sip-server ip-address ipv4:90.90.90.100	Sets the SIP Signaling IP Address of SIP Proxy. And you can also configure transport type and uri type
5	exit Example) /configure/voip-gateway/sip-ua# exit	Exits the current mode
6	exit Example) /configure/voip-gateway# exit	Exits the current mode

How to Configure Dial-Peer for Call Routing

To route a call based on a specific dialed pattern, you can make one or more dial-peers to route calls to the sip-server. If you don't make a specific dial-peer for the SIP server, Ubigate iBG first searches all the patterns configured and if it fails to match any others then it routes calls to the SIP server.

- Configuration Steps
 - configure terminal
 - dial-peer
 - destination-pattern
 - session target
 - exit
- Detailed Steps

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters global configuration mode.
2	dial-peer voice {pots voip} <i>tag</i> Example) /configure# dial-peer voice voip 100	Enters VoIP dial-peer configuration mode.
3	destination-pattern <i>dest-pattern</i> Example) /configure/ dial-peer/voice/voip 100# destination-pattern .T	Sets a destination pattern. .T means any pattern
4	session target sip-server Example) /configure/ dial-peer/voice/voip 100# session target sip-server	Sets the session target as sip-server.
5	exit Example) /configure/dial-peer/voice/voip 100# exit	Exits the current mode

Configuring SIP Registrar

This section describes how to set a SIP server in stand-alone mode. Ubigate iBG registers its all FXS subscribers and POTS trunks that are configured with 'register e164 or uri' commands. NO VoIP trunks are registered to the SIP Registrar. Even though a general SIP server have both proxy and registrar function, you may configure different servers.

Restrictions for SIP Registrar

The Standard RFC3261 based SIP server is supported with a number of extensions that iBG support. Use the SIP server mode when iBG interoperates with commercial or free SIP server, but there could be interoperability issues. You must not set the SIP server for Ubigate iPX. iPX cannot provide its all voice features with the SIP server setting. 'Call-server' must be set for Ubigate iPX.

How to Configure SIP Registrar

You can set the SIP Registrar in the following way.

- Configuration Steps
 - configure terminal
 - voip-gateway
 - sip-ua
 - registrar
 - exit
- Detailed Steps

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters global configuration mode.
2	voip-gateway Example) /configure# voip-gateway	Enters voip-gateway configuration mode.
3	sip-ua Example) /configure/ voip-gateway# sip-ua	Enters sip-ua configuration mode.

(Continued)

Step	Command	Purpose
4	registrar <i>ip-address</i> ip-addr [udp tcp tls] [sip sips] [expires <i>expires</i>] [retry <i>retry</i>] Example) /configure/voip-gateway/sip-ua# registrar ip-address ipv4:90.90.90.100	Sets the SIP Signaling IP Address of SIP Registrar. And you can also configure transport type, uri type, registration expires and retry interval.
5	exit Example) /configure/voip-gateway/sip-ua# exit	Exits the current mode.
6	exit Example) /configure/voip-gateway# exit	Exits the current mode.

How to Configure Dial-Peer for Registration

The procedure of registration in SIP Registrar per dial-peer is as follows.

- Configuration Steps
 - configure terminal
 - dial-peer
 - destination-pattern
 - register {e164 | uri}
 - exit
- Detailed Steps

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters global configuration mode.
2	dial-peer voice {pots voip} <i>tag</i> Example) /configure# dial-peer voice pots 11	Enters POTS dial-peer configuration mode.

(Continued)

Step	Command	Purpose
3	destination-pattern <i>dest-pattern</i> Example) /configure/ dial-peer/voice/pots 11# dest-pattern 1234	Sets a destination pattern.
4	register { e164 uri } Example) /configure/ dial-peer/voice/pots 11# register e164 /configure/ dial-peer/voice/pots 11# register uri sip:ibg_01@samsung.com	Configure a dial-peer to register with full E.164 number by register e164 command. Configure a dial-peer to register with user specific URI string by register uri command.
5	Exit Example) /configure/dial-peer/voice/pots 11# exit	Exits the current mode.

Configuring SIP Redirect Processing

This section describes how to set the SIP Redirect processing. SIP Redirect processing refers to the incoming call redirection or processing of 3xx class of response. In a Call Manager Inter-working mode, all SIP incoming calls of Ubigate iBG router is redirected to Call Manager. This means that all calls are controlled by Call Manager.

The redirect response processing is controlled by a command. It can be enabled or disabled using redirection command in a voice service SIP configuration mode. If the redirect response processing command is enabled, a new INVITE is attempted based on the contact header of a response message.

Otherwise, the call processing fails. In addition, the number of redirect response processing times can be limited using the max-redirects command in a dial-peer configuration mode.

How to Configure SIP Redirect Processing

You can enable or disable the SIP redirect response processing in the following way. The default setting is 'disable'.

- Configuration Steps
 - configure terminal
 - voice service sip
 - [no] redirection
 - exit
- Detailed Steps

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters global configuration mode.
2	voice service sip Example) /configure# voice service sip	Enters SIP Service configuration mode.
3	[no] redirection Example) /configure/ voice/service/sip# redirection	Enables or Disables Redirect Response handling.
4	Exit Example) /configure/voice/service/sip# exit	Exits the current mode

How to Configure Dial-Peer for SIP Redirect Processing

You can limit the Redirect processing count per dial-peer in the following way.

- Configuration Steps
 - configure terminal
 - dial-peer
 - max-redirects
 - exit
- Detailed Steps

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters global configuration mode.
2	dial-peer voice {pots voip} <i>tag</i> Example) /configure# dial-peer voice voip 100	Enters VoIP dial-peer configuration mode.
3	max-redirects <i>count</i> Example) /configure/ dial-peer/voice/voip 100# max-redirects 3	Sets the maximum count for SIP redirect response handling.
4	exit Example) /configure/dial-peer/voice/voip 100# exit	Exits the current mode

Configuring SIP Server using SIPconnect

This section describes how to configure Ubigate iBG for the SIP server using SIPconnect.

SIPconnect is a standards-based method of interconnection between IP PBXs and VoIP service provider networks. It specifies a reference architecture, required protocols and features, and implementation rules necessary for seamless peering between IP PBXs and VoIP service providers. Refer to ‘www.sipforum.org’ for details.

Restrictions for SIP Proxy Configuration

Registrar and sip-server should be configured for using SIPconnect.

Survivable telephony cannot be supported with SIP server.

Only public-identity will register to the SIP server, dial-peer for an analog phone -i.e. dial-peer voice pots - should not register to the SIP server. This means that ‘register e164’ should not be used at the dial-peer for an analog phone.

How to Configure SIP Proxy

You can set the SIP Server in the following way:

- Configuration Steps
 - configure terminal
 - voip-gateway
 - sip-ua
 - registrar
 - sip-server
 - sip-connect
 - exit
- Detailed Steps

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters global configuration mode.
2	voip-gateway Example) /configure# voip-gateway	Enters voip-gateway configuration mode.

(Continued)

Step	Command	Purpose
3	sip-ua Example) /configure/ voip-gateway# sip-ua	Enters sip-ua configuration mode.
4	registrar <i>ip-address</i> ip-addr Example) /configure/voip-gateway/sip-ua# registrar ip-address ipv4:90.90.90.100	Sets IP Address of SIP Server.
5	sip-server <i>ip-address</i> ip-addr Example) /configure/voip-gateway/sip-ua# sip-server ip-address ipv4:90.90.90.100	Sets IP Address of SIP Server.. Same to Registrar.
6	sip-connect <i>public-identity</i> E.164-public-number Example) /configure/voip-gateway/sip-ua# sip-connect public-identity 07070151000	Public identity number for SIPconnect. Public identity number should be given from the SIP server.
7	peer-monitor <i>expires</i> time <i>retry</i> time Example) /configure/voip-gateway/sip-ua# peer-monitor expires 60	[OPTIONAL] Enable SIPconnect monitoring by OPTIONS request.
8	exit Example) /configure/voip-gateway/sip-ua# exit	Exits the current mode
9	exit Example) /configure/voip-gateway# exit	Exits the current mode

How to Configure Dial-Peer for Call Routing

To route a call based on a specific dialed pattern, you can make one or more dial-peers to route calls to the SIP server. If you don't make a specific dial-peer for SIP server, Ubigate iBG first searches all the patterns configured and it fails to match any others then it routes calls to the SIP server.

- Configuration Steps
 - configure terminal
 - dial-peer
 - destination-pattern
 - session target
 - exit
- Detailed Steps

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters global configuration mode.
2	dial-peer voice {pots voip} <i>tag</i> Example) /configure# dial-peer voice voip 100	Enters VoIP dial-peer configuration mode.
3	destination-pattern <i>dest-pattern</i> Example) /configure/ dial-peer/voice/voip 100# destination-pattern .T	Sets a destination pattern. .T means any pattern
4	session target sip-server Example) /configure/ dial-peer/voice/voip 100# session target sip-server	Sets the session target as sip-server.
5	exit Example) /configure/dial-peer/voice/voip 100# exit	Exits the current mode

Configuring Enhanced SIP Gateway Features

Configuring PSTN Cause Code Mapping

This section describes the method of mapping between SIP status code and PSTN Cause code. For calls to be established between a SIP network and a PSTN network, the two networks must be able to interoperate. One aspect of their interoperability is the mapping of PSTN cause codes, which indicate reasons for PSTN call failure or completion, to SIP status codes or events. The opposite is also true: SIP status codes or events are mapped to PSTN cause codes.

Ubigate iBG router provides a SIP- PSTN default mapping table.

The method for an operator to change the mapping is also provided. You can change the mapping using set the pstn-cause command and set sip-status command. You can check the current mapping table settings using the show sip-ua maps command.

Restrictions for PSTN Cause Code Mapping

Using the command described above, you can change the existing inter-code mapping, but not create a new code.

Default Mapping

- Default PSTN Cause Code to SIP Status Code Mapping

Table 3.4 Table Default PSTN cause code to SIP status code mapping

PSTN Cause Code	Description	SIP Event
1	Unallocated number	404 Not found
2	No route to specified transit network	404 Not found
3	No route	404 Not found
17	User busy	486 Busy here
18	No user response	480 Temporarily unavailable
19	No answer from the user	480 Temporarily unavailable
20	Subscriber absent	480 Temporarily unavailable
21	Call rejected	403 Forbidden

Table 28.4 Table Default PSTN cause code to SIP status code mapping (Continued)

PSTN Cause Code	Description	SIP Event
22	Number changed	410 Gone
26	Non-selected user clearing	404 Not found
27	Destination out of order	404 Not found
28	Address incomplete	484 Address incomplete
29	Facility rejected	501 Not implemented
31	Normal, unspecified	404 Not found
34	No circuit available	503 Service unavailable
38	Network out of order	503 Service unavailable
41	Temporary failure	503 Service unavailable
42	Switching equipment congestion	503 Service unavailable
47	Resource unavailable	503 Service unavailable
55	Incoming class barred within Closed User Group (CUG)	403 Forbidden
57	Bearer capability not authorized	403 Forbidden
58	Bearer capability not presently available	501 Not implemented
65	Bearer capability not implemented	501 Not implemented
79	Service or option not implemented	501 Not implemented
87	User not member of Closed User Group (CUG)	503 Service Unavailable
88	Incompatible destination	400 Bad request
95	Invalid message	400 Bad request
102	Recover on Expires timeout	408 Request timeout
111	Protocol error	400 Bad request
Any code other than those listed above		500 Internal server

- Default SIP Status Code to PSTN Cause Code Mapping

Table 3.5 Default SIP Event to PSTN cause code mapping

SIP Event	PSTN Cause code	Description
400 Bad request	127	Interworking, unspecified
401 Unauthorized	57	Bearer capability not authorized
402 Payment required	21	Call rejected
403 Forbidden	57	Bearer capability not authorized
404 Not found	1	Unallocated number
405 Method not allowed	127	Interworking, unspecified
406 Not acceptable	127	Interworking, unspecified
407 Proxy authentication required	21	Call rejected
408 Request timeout	102	Recover on Expires timeout
409 Conflict	41	Temporary failure
410 Gone	1	Unallocated number
411 Length required	127	Interworking, unspecified
413 Request entity too long	127	Interworking, unspecified
414 Request URI (URL) too long	127	Interworking, unspecified
415 Unsupported media type	79	Service or option not implemented
420 Bad extension	127	Interworking, unspecified
480 Temporarily unavailable	18	No user response
481 Call leg does not exist	127	Interworking, unspecified
482 Loop detected	127	Interworking, unspecified
483 Too many hops	127	Interworking, unspecified
484 Address incomplete	28	Address incomplete
485 Address ambiguous	1	Unallocated number
486 Busy here	17	User busy
487 Request cancelled	127	Interworking, unspecified
488 Not acceptable here	127	Interworking, unspecified
500 Internal server error	41	Temporary failure

Table 28.5 Default SIP Event to PSTN cause code mapping (Continued)

SIP Event	PSTN Cause code	Description
501 Not implemented	79	Service or option not implemented
502 Bad gateway	38	Network out of order
503 Service unavailable	63	Service or option unavailable
504 Gateway timeout	102	Recover on Expires timeout
505 Version not implemented	127	Interworking, unspecified
580 Precondition Failed	47	Resource unavailable, unspecified
600 Busy everywhere	17	User busy
603 Decline	21	Call rejected
604 Does not exist anywhere	1	Unallocated number
606 Not acceptable	58	Bearer capability not presently available

How to Configure PSTN Cause Code to SIP Status Code Mapping

You can change the PSTN Cause code to SIP Status code mapping in the following way.

- Configuration Steps
 - configure terminal
 - voip-gateway
 - sip-ua
 - set pstn-cause
 - exit
 - exit
 - show sip-ua maps pstn-sip
- Detailed Steps

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters global configuration mode.
2	voip-gateway Example) /configure# voip-gateway	Enters voip-gateway configuration mode.
3	sip-ua Example) /configure/ voip-gateway# sip-ua	Enters sip-ua configuration mode.
4	set pstn-cause <i>cause</i> sip-status <i>code</i> Example) /configure/voip-gateway/sip-ua# set pstn-cause 1 sip-status 404	Changes pstn cause code to sip status code mapping.
5	exit Example) /configure/ voip-gateway/sip-ua# exit	Exits the current mode
6	exit Example) /configure/voip-gateway# exit	Exits the current mode
7	show sip-ua maps pstn-sip Example) # show sip-ua maps pstn-sip	Display current pstn cause code to sip status code mapping table.

How to Configure SIP Status Code to PSTN Cause Code Mapping

You can change the SIP Status code to PSTN Cause code mapping in the following way.

- Configuration Steps
 - configure terminal
 - voip-gateway
 - sip-ua
 - set sip-status
 - exit
 - exit
 - show sip-ua maps sip-pstn
- Detailed Steps

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters global configuration mode.
2	voip-gateway Example) /configure# voip-gateway	Enters voip-gateway configuration mode.
3	sip-ua Example) /configure/ voip-gateway# sip-ua	Enters sip-ua configuration mode.
4	set sip-status <i>code</i> pstn-cause <i>cause</i> Example) /configure/voip-gateway/sip-ua# set sip-status 404 pstn-cause 1	Changes sip status code to pstn cause code mapping.
5	exit Example) /configure/ voip-gateway/sip-ua# exit	Exits the current mode
6	exit Example) /configure/voip-gateway# exit	Exits the current mode
7	show sip-ua maps sip-pstn Example) # show sip-ua maps pstn-sip	Display current sip status code to pstn cause code mapping table.

Configuring Early Media Session

This section describes the method of handling 18x provisional response. Ubigate iBG router can receive the Answer SDP for Offer SDP delivered being included in INVITE, via 180 or 183 provisional response message. If this SDP is processed, a media path is opened prior to Answer status. Using the disable-early-media command in a SIP-UA configuration mode, you can control the method for Ubigate iBG router to handle the SDP delivered via 180 response.

On the contrary, it is possible to control whether, when Ubigate iBG router sends an 18x provisional response including SDP, to send 180 or 183 response, or send it together with SDP, by using the alert-cut-through command.

How to Configure 180 Provisional Response Handling

You can set the method of handling the 180 provisional response where SDP is included, in the following way.

- Configuration Steps
 - configure terminal
 - voip-gateway
 - sip-ua
 - [no] disable-early-media 180
 - exit
 - exit
- Detailed Steps

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters global configuration mode.
2	voip-gateway Example) /configure# voip-gateway	Enters voip-gateway configuration mode.
3	sip-ua Example) /configure/ voip-gateway# sip-ua	Enters sip-ua configuration mode.

(Continued)

Step	Command	Purpose
4	[no] disable-early-media 180 Example) /configure/voip-gateway/sip-ua# disable-early-media 180	Disables or re-enables early media processing for 180 provisional response. Default is enable.
5	exit Example) /configure/ voip-gateway/sip-ua# exit	Exits the current mode
6	exit Example) /configure/voip-gateway# exit	Exits the current mode

How to Configure Early Media Cut-through

You can set the Early media cut-through method in the following way.

- Configuration Steps
 - configure terminal
 - voip-gateway
 - sip-ua
 - alert-cut-through
 - exit
 - exit
- Detailed Steps

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters global configuration mode.
2	voip-gateway Example) /configure# voip-gateway	Enters voip-gateway configuration mode.

(Continued)

Step	Command	Purpose
3	sip-ua Example) /configure/ voip-gateway# sip-ua	Enters sip-ua configuration mode.
4	[no] alert-cut-through {180 183} Example) /configure/voip-gateway/sip-ua# alert-cut-through 180	no alert-cut-through: 18x response does not include SDP. alert-cut-through 180: 180 response includes SDP for sending. alert-cut-through 183: 183 response includes SDP for sending. it is default.
5	exit Example) /configure/ voip-gateway/sip-ua# exit	Exits the current mode
6	exit Example) /configure/voip-gateway# exit	Exits the current mode

Configuring Session Timer

This section describes how to enable the SIP Session Timer feature. For the established session, SIP Session Timer feature periodically updates the session via re-INVITE or UPDATE method. If no reply is received in response to re-INVITE or UPDATE for session updating, or an error response is received, the session is closed by sending BYE method. A session is also closed when the session is not updated within the mutually negotiated interval. Two SIP headers were added to support SIP Session Timer feature. One is Session-Expires which is a Session Update cycle. The other one is Min-SE, which is used to limit the minimum value of the session update cycle.

Restrictions for Session Timer

Ubigate iBG router uses an UPDATE method as the method of session update. Even though Session update is not done using INVITE, when INVITE for session update is received, it is processed normally.

How to Configure Session Timer Feature

To enable the Session Timer Feature, you can set Min-Se in the following way.

- Configuration Steps
 - configure terminal
 - voice service sip
 - min-se
 - exit
- Detailed Steps

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters global configuration mode.
2	voice service sip Example) /configure# voice service sip	Enters SIP Service configuration mode.
3	[no] min-se <i>duration</i> Example) /configure/ voice/service/sip# min-se 300	Sets the minimum session expires. (default value 90 seconds) no mean disabling this feature
4	Exit Example) /configure/voice/service/sip# exit	Exits the current mode

Configuring Reason header support

This section describes how to set the use of the Reason header in SIP message. To deliver the Q.850 Cause of PSTN via SIP message in SIP-PSTN interworking, a reason header is added to SIP message. Ubigate iBG router loads the Q.850 Cause received from PSTN to the SIP message reason header, and if it receives the SIP message including a reason header, it delivers it to PSTN.

How to Configure Reason Header Support

You can enable the reason header function as follows. The default setting does not support a reason header.

- Configuration Steps
 - configure terminal
 - voip-gateway
 - sip-ua
 - reason-header override
 - exit
 - exit
- Detailed Steps

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters global configuration mode.
2	voip-gateway Example) /configure# voip-gateway	Enters voip-gateway configuration mode.
3	sip-ua Example) /configure/ voip-gateway# sip-ua	Enters sip-ua configuration mode.
4	[no] reason-header override Example) /configure/voip-gateway/sip-ua# reason-header override	Enables or disables reason header feature.

(Continued)

Step	Command	Purpose
5	exit Example) /configure/ voip-gateway/sip-ua# exit	Exits the current mode
6	exit Example) /configure/voip-gateway# exit	Exits the current mode

Configuring Reliable Provisional Responses

This section describes how to enable the Reliable Provisional Response feature. When the SIP message is delivered via UDP, the reliability of 1xx response cannot be guaranteed. That is, the originating side may not receive 180 or 183 responses sent from a destination side. In this case, the originating side cannot hear the Ring back tone. Furthermore, if the early media path is established to the response, the originating side cannot hear the announcement. To complement this, an additional method called PRACK is used to ensure the reliability of the Provisional response. Ubigate iBG router supports this function by default, or it can disable or force the function.

Restrictions for Reliable Provisional Response

Reliable Provisional Response feature is available only when both originating side and destination side support this function. If either side cannot support this function, this function does not work. If either side has the setting to support the function forcibly, and the other side does not support it, the call between them fails.

How to Configure Reliable Provisional Response

You can enable or disable the Reliable Provisional Response Feature in the following way.

- Configuration Steps
 - configure terminal
 - voice service sip
 - rel1xx
 - exit
- Detailed Steps

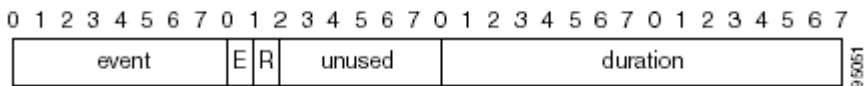
Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters global configuration mode.
2	voice service sip Example) /configure# voice service sip	Enters SIP Service configuration mode.
3	rel1xx [supported require disable] Example) /configure/ voice/service/sip# rel1xx supported	Enables or Disables reliable provisional response feature.
4	Exit Example) /configure/voice/service/sip# exit	Exits the current mode

Configuring SIP DTMF Relay

This section describes how to set the method of delivering DTMF tone via SIP signaling. To relay DTMF tone, Ubigate iBG router supports the 4 methods as follows.

- inband
- rtp-nte
- sip-notify
- sip-info

The inband method delivers DTMF to a voice path without separate processing. In this case, a distortion may occur due to loss of RTP packets. The rtp-nte method delivers DTMF tone via RTP according to RFC 2833, RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals. The SIP NOTIFY method delivers DTMF tone using the SIP NOTIFY method. The sip-info method delivers DTMF tone using SIP INFO method. SIP NOTIFY based out-of-band DTMF relay format is similar to the DTMF message format described in RFC2833.



Field	Description
event	The DTMF event that is between 0-9, A, B, C, D, #, * and flash.
E	E signifies the end bit. If E is set to a value of 1, the NOTIFY message contains the end of the DTMF event. Thus, the duration parameter in this final NOTIFY message measures the complete duration of the event.
R	Reserved
unused	In RFC2833, unused corresponds to the volume field, but is not used in the NOTIFY-based out-of-band DTMF relay.
duration	Duration of the DTMF event, in milliseconds.

With SIP INFO method, use the ‘application/dtmf-relay’ content-type header, containing the signal and duration attribute field.

signal= *dtmf event value*

How to Configure SIP DTMF Relay

The DTMF Relay method can be set for all SIP calls, or be set differently for each dial-peer. To set it for all SIP calls, follow the procedure below.

- Configuration Steps
 - configure terminal
 - voip-gateway
 - sip-ua
 - dtmf-relay
 - exit
 - exit
- Detailed Steps

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters global configuration mode.
2	voip-gateway Example) /configure# voip-gateway	Enters voip-gateway configuration mode.
3	sip-ua Example) /configure/ voip-gateway# sip-ua	Enters sip-ua configuration mode.
4	dtmf-relay [inband rtp-nte sip-info sip-notify] Example) /configure/voip-gateway/sip-ua# dtmf-relay sip-info	Specifies how to relay DTMF tone between telephony interface and SIP network.
5	exit Example) /configure/ voip-gateway/sip-ua# exit	Exits the current mode
6	exit Example) /configure/voip-gateway# exit	Exits the current mode

To set the DTMF Relay method for each dial-peer, follow the procedure below.

- Configuration Steps
 - configure terminal
 - dial-peer
 - dtmf-relay
 - exit
- Detailed Steps

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters global configuration mode.
2	dial-peer voice {pots voip} tag Example) /configure# dial-peer voice voip 100	Enters VoIP dial-peer configuration mode.
3	[no] dtmf-relay [inband rtp-nte h245- alphanumeric sip-info sip-notify] Example) /configure/ dial-peer/voice/voip 100# dtmf-relay sip-info	Specifies how to relay DTMF tone between telephony interface and IP network.
4	Exit Example) /configure/dial-peer/voice/voip 100# exit	Exits the current mode

Configuring ISDN Suspend/Resume Support

This section describes how to set the function, in SIP and ISDN interworking, to map the ISDN Suspend/Resume message to SIP Hold/Retrieve. Upon receiving a Suspend message from ISDN, it sends re-INVITE for SIP Hold; and upon receiving the Resume message, it sends re-INVITE for SIP Retrieve.

How to Configure ISDN Suspend/Resume Support

You can enable the ISDN Suspend/Resume to SIP Hold/Retrieve mapping function in the following way.

- Configuration Steps
 - configure terminal
 - voip-gateway
 - sip-ua
 - [no] suspend-resume
 - exit
 - exit
- Detailed Steps

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters global configuration mode.
2	voip-gateway Example) /configure# voip-gateway	Enters voip-gateway configuration mode.
3	sip-ua Example) /configure/ voip-gateway# sip-ua	Enters sip-ua configuration mode.
4	[no] suspend-resume Example) /configure/voip-gateway/sip-ua# suspend-resume	Enables or Disables ISDN Suspend/Resume support.
5	exit Example) /configure/ voip-gateway/sip-ua# exit	Exits the current mode
6	exit Example) /configure/voip-gateway# exit	Exits the current mode

Configuring QSIG tunneling over SIP

This section describes how to make the necessary settings to deliver QSIG message via SIP signaling. Ubigate iBG router provides the function to load QSIG message in SIP message. Its purpose is to deliver the QSIG message transparently to the SIP section, when a different QSIG network is connected to the SIP. To do so, it is necessary to enable the QSIG Tunneling function to the SIP type VoIP Dial-Peer.

How to Configure QSIG Tunneling

You can enable the QSIG Tunneling function in SIP type VoIP Dial-Peer in the following way.

- Configuration Steps
 - configure terminal
 - dial-peer
 - sip-class qsig tunneling
 - exit
- Detailed Steps

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters global configuration mode.
2	dial-peer voice {pots voip} tag Example) /configure# dial-peer voice voip 100	Enters VoIP dial-peer configuration mode.
3	[no] sip-class qsig tunneling Example) /configure/ dial-peer/voice/voip 100# sip-class qsig tunneling	Enables or Disables QSIG Tunneling feature.
4	Exit Example) /configure/dial-peer/voice/voip 100# exit	Exits the current mode

Configuring Calling-Info for SIP Calls

This section describes how to set the calling information for SIP Calls forcibly. Ubigate iBG router ignores the calling name and number received from the Calling party and changes them to what is configured. To change the calling information for PSTN-to-SIP call forcibly, you can make a setting using a calling-info pstn-to-sip command and to change the calling information for SIP-to-PSTN call forcibly, you can make a setting using the calling-info sip-to-pstn command.

Restrictions for Calling-Info Feature

This configuration affects all SIP inbound and outbound calls. So, be careful how you use this feature.

How to Configure Calling-info for PSTN-to-SIP calls

You can set the calling information for PSTN-to-SIP calls in the following way.

- Configuration Steps
 - configure terminal
 - voip-gateway
 - sip-ua
 - calling-info pstn-to-sip
 - exit
 - exit
- Detailed Steps

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters global configuration mode.
2	voip-gateway Example) /configure# voip-gateway	Enters voip-gateway configuration mode.
3	sip-ua Example) /configure/ voip-gateway# sip-ua	Enters sip-ua configuration mode.

(Continued)

Step	Command	Purpose
4	[no] calling-info pstn-to-sip { unscreened discard name <name string> number <number> } Example) /configure/voip-gateway/sip-ua# calling-info pstn-to-sip number 7778888	Sets the calling-info for pstn-to-sip call.
5	exit Example) /configure/ voip-gateway/sip-ua# exit	Exits the current mode
6	exit Example) /configure/voip-gateway# exit	Exits the current mode

How to Configure Calling-info for SIP-to-PSTN calls

You can set the calling information for SIP-to-PSTN calls in the following way.

- Configuration Steps
 - configure terminal
 - voip-gateway
 - sip-ua
 - calling-info sip-to-pstn
 - exit
 - exit
- Detailed Steps

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters global configuration mode.
2	voip-gateway Example) /configure# voip-gateway	Enters voip-gateway configuration mode.

(Continued)

Step	Command	Purpose
3	sip-ua Example) /configure/ voip-gateway# sip-ua	Enters sip-ua configuration mode.
4	[no] calling-info sip-to-pstn { unscreened discard name <name string> number <number> } Example) /configure/voip-gateway/sip-ua# calling-info sip-to-pstn number 7778888	Sets the calling-info for sip-to-pstn call.
5	exit Example) /configure/ voip-gateway/sip-ua# exit	Exits the current mode
6	exit Example) /configure/voip-gateway# exit	Exits the current mode

Configuring SIP Entity Monitoring Features

This section describes how to enable SIP Entity Monitoring Features. Ubigate iBG router sends an OPTIONS message to monitor SIP remote entities. If no response is received, that entity is considered as in not operating status and the new call is not routed to that entity. After the configured duration, iBG sends the OPTIONS message again. And if it gets a response, the status is changed to normal. To set the duration and retry interval, use the peer-monitor command.

Restrictions for SIP Entity Monitoring Feature

This feature is available only when the SIP remote entity can generate a response, which is positive or negative, to the OPTIONS request. If the SIP entity ignores the OPTIONS request and makes no response, its status is always abnormal and it never receives a call from iBG.

How to Configure SIP Entity Monitoring Feature

You can enable or disable the SIP entity monitoring feature in the following way:

- Configuration Steps
 - configure terminal
 - voip-gateway
 - sip-ua
 - peer-monitor
 - exit
 - exit
- Detailed Steps

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters global configuration mode.
2	voip-gateway Example) /configure# voip-gateway	Enters voip-gateway configuration mode.
3	sip-ua Example) /configure/ voip-gateway# sip-ua	Enters sip-ua configuration mode.
4	[no] peer-monitor expires <expire seconds> retry <retry seconds> Example) /configure/voip-gateway/sip-ua# peer-monitor expires 200 retry 30	Enables or Disables SIP entity monitoring feature.
5	exit Example) /configure/ voip-gateway/sip-ua# exit	Exits the current mode
6	exit Example) /configure/voip-gateway# exit	Exits the current mode

Configuring Miscellaneous Features

This section describes the miscellaneous SIP settings not discussed in the previous section. These commands are available in the SIP UA Configuration mode and SIP Service Configuration mode. For information on how to use the commands, see the Command Reference.

Command	Mode	Purpose
offer call-hold	SIP-UA	specifies globally how the Session Initiation Protocol (SIP) gateway should initiate call-hold requests.
max-forwards	SIP-Service	Specifies the Max-Forwards Header value to used in the request message.
no-answer-timer	SIP-Service	Specifies the timer value to specify the interval from the receipt of 1xx response to 2xx response message.
registrar local-service expires	SIP-Service	Specifies the allowable expires header value of a REGISTER message when it runs as a register in a Survivable telephony mode.
timers	SIP-Service	Specifies the timer value used in Session Initiation Protocol (SIP) stack.
transport-switch udp-to-tcp	SIP-Service	Enables switching between UDP and TCP transport mechanisms globally for large Session Initiation Protocol (SIP) messages.
url	SIP-Service	Configures URLs to either the Session Initiation Protocol (SIP) or telephone (TEL) format for your VoIP SIP calls.
Transport	SIP-Service	Specifies default transport type to be used in the Session Initiation Protocol (SIP).
Port	SIP-Service	Specifies default port numbers of transport types to be used in the Session Initiation Protocol (SIP).

Configuring SIP Security Features

Configuring HTTP Authentication Digest

This section describes the configuration for the HTTP Authentication Digest function. The HTTP Authentication Digest is a protocol based on UserName/Password. Using this function, the SIP server authenticates SIP clients. To make this function available, UserName/Password should be shared with the SIP server in advance.

The SIP server requesting authentication of the SIP client response to the request sent from Ubigate iBG router with 401 response. Using the information contained in 401 response and UserName/Password, Ubigate iBG router adds the Authorization Token to a request.

Upon receiving the request where the Authorization Token is added, SIP server verifies the authorization token using the shared information. Via this verification procedure, SIP server authenticates SIP clients.

Restrictions for HTTP Authentication Digest

The HTTP Authentication Digest follows the Digest procedure of RFC 2617 'HTTP authentication Basic and Digest Access Authentication'.

Prerequisites for HTTP Authentication Digest

To set the HTTP Authentication, the dial-peer voice pots should be created already. The UserName/Password setting should be agreed upon by the SIP server in advance.

How to Configure UserName and Password for a POTS dial-peer

You can specify the UserName and Password per Dial-peer voice pot in the following way.

- Configuration Steps
 - configure terminal
 - dial-peer voice pots
 - authentication
 - exit
- Detailed Steps

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters global configuration mode.
2	dial-peer voice {pots voip} <i>tag</i> Example) /configure# dial-peer voice pots 11	Enters POTS dial-peer configuration mode
3	authentication username <i>username</i> password <i>password</i> Example) configure/ dial-peer/voice/pots 11#authentication username 1001 password 12345678	Configures a user name and password for a POTS dial-peer
4	exit Example) configure/ dial-peer/voice/pots 11# exit	Exits the current mode

How to Configure System Default Digest

This is the method of setting the system default digest parameter. You can set the realm information of the SIP server where the UserName/Password are agreed upon.

- The system default digest parameter will be used. The default dial peer has no digest parameter configuration. Configuration Steps:
 - configure terminal
 - voip-gateway
 - sip-ua
 - authentication
 - exit
- Detailed Steps

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters global configuration mode.
2	voip-gateway Example) /configure# voip-gateway	Enters voip-gateway configuration mode.
3	sip-ua Example) /configure/ voip-gateway# sip-ua	Enters sip-ua configuration mode.
4	authentication username <i>username</i> password <i>password</i> [realm <i>realm</i>] Example) /configure/voip-gateway/sip-ua#authentication username Ubigate iBG2016 password 12345678 realm proxy.com	Configures a user name, password and realm for system default
5	exit Example) /configure/voip-gateway/sip-ua# exit	Exits the current mode
6	exit Example) /configure/voip-gateway# exit	Exits the current mode

Configuring SIPS URI with TLS transport

This section describes how to set SIP signaling via TLS connection. To do this, set the URI type to SIPS, and change the transport type to TLS. You can change the URI type and transport type in two ways. That is, you can make a setting which applies to the entire SIP signaling, or individual SIP type dial-peers.

How to Configure SIP URI with TLS transport for All SIP Calls

You can perform a system global configuration for SIP URI with the TLS transport in the following way:

- Configuration Steps
 - configure terminal
 - voice service sip
 - uri
 - transport
 - exit
- Detailed Steps

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters global configuration mode.
2	voice service sip Example) /configure# voice service sip	Enters SIP Service configuration mode.
3	uri [sip sips] Example) /configure/ voice/service/sip# uri sips	Specifies SIP URI type. sip or sips is available.
4	transport [udp tcp tls] Example) /configure/ voice/service/sip# transport tls	Specifies SIP transport type. udp, tcp or tls is available.
5	Exit Example) /configure/voice/service/sip# exit	Exits the current mode

How to Configure Dial-Peer for SIPS URI with TLS transport

You can configure a specific dial-peer for SIPS URI with TLS transport in the following way.

- Configuration Steps
 - configure terminal
 - dial-peer
 - sip-class uri
 - session transport
 - exit
- Detailed Steps

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters global configuration mode.
2	dial-peer voice {pots voip} <i>tag</i> Example) /configure# dial-peer voice voip 100	Enters VoIP dial-peer configuration mode.
3	sip-class uri [sip sips] Example) /configure/ dial-peer/voice/voip 100# sip-class uri sips	Specifies SIP URI type.
4	session transport [udp tcp tls] Example) /configure/ dial-peer/voice/voip 100# session transport tls	Specifies SIP transport type.
5	Exit Example) /configure/dial-peer/voice/voip 100# exit	Exits the current mode

Configuring SRTP support

This section describes the SRTP function to encode and deliver a media packet. SRTP encodes and sends the media packet using the key exchanged via SIP signaling, and the receiving party decodes the encrypted media packet to support media level security. To use this SRTP, it is necessary to specify crypto suite to a dial-peer where SRTP will be used.

How to Configure SRTP transport for All SIP Calls

You can perform a system global configuration for SRTP support in the following way:

- Configuration Steps
 - configure terminal
 - voice service sip
 - srtp crypto
 - exit
- Detailed Steps

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters global configuration mode.
2	voice service sip Example) /configure# voice service sip	Enters SIP Service configuration mode.
3	srtp crypto [AES_CM_128_HMAC_SHA1_32 AES_CM_128_HMAC_SHA1_80] Example) /configure/ voice/service/sip# srtp crypto AES_CM_128_HMAC_SHA1_80	Specifies SRTP crypto suite. You can specify either AES_CM_128_HMAC_SHA1_32 or AES_CM_128_HMAC_SHA1_80, or both of them. Recommend to use AES_CM_128_HMAC_SHA1_80
5	Exit Example) /configure/voice/service/sip# exit	Exits the current mode

How to Configure Dial-Peer for SRTP support

- Configuration Steps
 - configure terminal
 - dial-peer
 - srtp crypto
 - exit
- Detailed Steps

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters global configuration mode.
2	dial-peer voice {pots voip} tag Example) /configure# dial-peer voice voip 100	Enters VoIP dial-peer configuration mode.
3	srtp crypto [AES_CM_128_HMAC_SHA1_32 AES_CM_128_HMAC_SHA1_80] Example) /configure/ dial-peer/voice/voip 100# srtp crypto AES_CM_128_HMAC_SHA1_80	Specifies SRTP crypto suite. You can specify either AES_CM_128_HMAC_SHA1_32 or AES_CM_128_HMAC_SHA1_80, or both of them. Recommend to use AES_CM_128_HMAC_SHA1_80
4	Exit Example) /configure/dial-peer/voice/voip 100# exit	Exits the current mode

Verifying and Troubleshooting SIP Features

This section describes how to use the show command and debug command to verify and troubleshoot the SIP feature of Ubigate iBG router.

Using show commands

You can use the show commands as follows to confirm or see the current status of the SIP feature settings.

show sip-ua service

Shows the SIP service status. The service status is 'up' or 'down'.

Example)

```
# show sip-ua service
SIP Service is up
```

show sip-ua operation-mode

Shows the operation mode. The operation mode is a Call Manager interworking mode, Survivable Telephony mode, and Stand-alone mode.

Example)

```
# show sip-ua operation-mode
Call Manager interworking mode.
```

show sip-ua registrar

Shows the SIP Registrar settings.

Example)

```
# show sip-ua registrar
registrar type is SCM
host ip is ipv4:172.19.30.230
transport is system
port is used system configuration
expires is 3600
uri type is system
username is 07070154420
password is 07070154420
realm is not configured
```

show sip-ua sip-server

Shows the SIP Proxy settings.

Example)

```
# show sip-ua sip-server
proxy type is SCM
host ip is ipv4:172.19.30.230
transport is system
port is used system configuration
uri type is system
expires is 3600
retry time is 60
```

show sip-ua registration

Shows the registration status of Ubigate iBG router and each dial-peer.

If Ubigate iBG cannot register to the SIP Registrar - e.g. Ubigate iPX or SIP server, refer to 'SIP-UA cannot register to the SIP server' and 'SIP-UA cannot register to Ubigate iPX' for details.

Example)

```
# show sip-ua registration
Call-Server(GW-URI): Expires=60 Registered
sip:ibg14@vgw10.com
```

ID	USERINFO	EXPIRES		STATUS	PORT	AUTHENTICATION
1400	1400	0	0	no	0/0/0	1400[****]
1401	1401	0	0	no	0/0/1	1401[****]
7701	7701	3600	3600	yes	0/0/0	7701[****]
7702	7702	3600	3600	yes	0/0/0	7702[****]

```
Number of 4/total(4) is registered
```

show sip-ua parameters

Shows other SIP settings.

Example)

```
# show sip-ua parameters
SIP-UA : up
  Operation mode : Call-server mode
  Authentication : username[4420], password[4420]
  SIP-UA is use call-server
  SIP-UA use ip address for call-server : ipv4:172.19.30.230
  SIP-UA expires time for REGISTER : 3600
  SIP-UA retry time for REGISTER : 60
  SIP-UA use transport : system
  SIP-UA use uri type : system
  SIP-UA URI : sip:ibg14@vgw10.com
  SIP-UA use duration : 60
  SIP-UA use retry : 10
  registrar is not configured
  mwi server is not configured
```

```
SIP UA Timers
SIP timer T1 : 500
SIP timer T2 : 4000
SIP timer T4 : 5000
peer monitoring (OPTIONS) is disabled
Session Timer Expires : 1800
Session Timer Min-SE : 90
SIP UA Parameters
SIP-UA default dtmf relay : Inband
SIP-UA default transport : tls
SIP-UA default uri type : sip
SIP-UA default UDP port : 5060
SIP-UA default TCP port : 5060
SIP-UA default TLS port : 5061
SIP-UA default max forwards : 70
SIP rel1xx is supported
SIP Redirect ip to ip : no
SIP Inband alerting : no
SIP Redirection : no
SIP Send SDP in 183
SIP Suspend Resume : no
SIP offer hold : direction attribute sendonly (RFC 3264)
PSTN code for SIP Request CANCEL : 16
SIP Early media at 180 : Enabled
SIP Reason-header Override : no
use tel url : no
SRTP not use sha1 32
SRTP use sha1 80
Registrar local service expires min : 60
Registrar local service expires max : 86400
max udp msg length to switch to tcp : not switch
SIP no answer timer value for sip outbound call 120
SIP calling-info PSTN-to-SIP unscreened discard : no
SIP calling-info SIP-to-PSTN unscreened discard : no
voip gateway profiles are synchronized to call-server
VoIP fallback configuration
voip fallback normal system message : "Normal Mode"
voip fallback survivable system message : "Survivable
Mode"
Local Registrar configuration
Local Registrar is configured
Min Expires timer : 60s
Max Expires timer : 86400s
```


show sip-ua calls

Shows the status of SIP calls in progress.

If Ubigate iBG cannot make outbound calls through the SIP protocol, refer to 'Outbound SIP Calls fail because of CODEC mismatch', 'Outbound SIP Calls fail because of Restriction', 'SIP phone Registration to Ubigate fails' for details.

Example)

```
# show sip-ua calls
-----
SIP-CALL CTXID : 1
-----
-SIP-CALLID : AAFfkD4bDhsAAAAAAAAAAAA@10.254.167.249
-CALL-STATES : PIC_T_Active
-FROM : <sip:2301@samsung.com>;tag=7267517
-TO : <sip:2302@samsung.com>;tag=7267170
-SOURCE ADDRESS : udp 10.254.167.249:0
-DESTINATION ADDRESS : udp 10.254.167.244:0
-MEDIA INFO
  -PAYLOAD ID(CODEC) : g711u
  -RTP LOCAL ADDRESS : 10.10.10.10:16388
  -RTP REMOTE ADDRESS : 10.10.10.10:16388
  -DTMF PAYLOAD TYPE : 101
-----
SIP-CALL CTXID : 2
-----
-SIP-CALLID : AAFfkD4bDhsAAAAAAAAAAAA@10.254.167.249
-CALL-STATES : PIC_O_Active
-FROM :
<sip:2301@samsung.com>;tag=7267517
-TO : <sip:2302@samsung.com>;tag=7267170
-SOURCE ADDRESS : udp 10.254.167.249:0
-DESTINATION ADDRESS : udp 10.254.167.244:0
-MEDIA INFO
  -PAYLOAD ID(CODEC) : g711u
  -RTP LOCAL ADDRESS : 10.10.10.10:16388
  -RTP REMOTE ADDRESS : 10.10.10.10:16388
  -DTMF PAYLOAD TYPE : 101
-----
TOTALA NUMBER: 2
```

show sip-ua connections

Shows the SIP connection status. It shows the connection status per the transport type of UDP, TCP and TLS.

If Ubigate iBG has some problems to communicate with SIP server - e.g. Ubigate iPX, refer to 'Each SIP message uses different transport protocol' for details.

```
# show sip-ua connections udp
UDP CONNECTION INFO
-----
No.   Local Address      Remote Address      Status
-----
0.    10.254.167.249:5060 -                    Listen
1.    10.254.167.249:5060 10.254.167.244:5060 Established
-----
TOTAL NUMBER: 2
```

Using debug commands

You can use the following debug commands to view the debugging messages of an application, or the SIP message sent or received.

debug sip log

Command to view the SIP message. You can display messages by filtering them by calling number or called number.

debug sip vcc

Displays the SIP call processing task debugging messages.

debug sip stack

Displays the SIP Stack level debugging messages.

debug sip dump req

Displays SIP message's request and response line.

debug sip dump msg

Displays SIP messages.



CHAPTER 4. H.323 Gateway Management

Introduction to H.323 Gateway Features

This section describes how the H.323 gateway works in regard to the features stated below.

- Call Setup Procedure
- RAS Signaling
- Codec Negotiation
- Support for Supplementary Services
- Call Statistics

Conformance

H.323 gateway basically follows the recommendations below.

Table 4.1 Standards

Standards	Title
ITU-T H.323 Version4	Packet-based multimedia communications systems
ITU-T H.225	Call signaling protocols and media stream packetization for packet-based multimedia communication systems
ITU-T H.245	Control protocol for multimedia communication
ITU-T E.164	Overall network operation, telephone service, service operation and human factors
RFC 2833	RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals

Call Setup Procedure

Call Signaling basically follows the ITU-T Rec.H.323 recommendation; and the call setup procedure can be generally divided into the case where Ubigate iBG router is registered in the gatekeeper, and where it is registered. If the H.323 gateway is registered in a gatekeeper, it can be divided into Direct Call Signaling and Gatekeeper Routed Call Signaling depending on the call model supported by a gatekeeper.

This section will discuss how Ubigate iBG router performs a call setup procedure in dial-peer depending on the registered information (session target).

The H.225.0 SETUP message from the H.323 Endpoint registered as a session target on dial-peer follows the call procedure illustrated in Figure 4.1.

In this case, call setup is done regardless of the existence of the gatekeeper to interwork over the H.323 network.

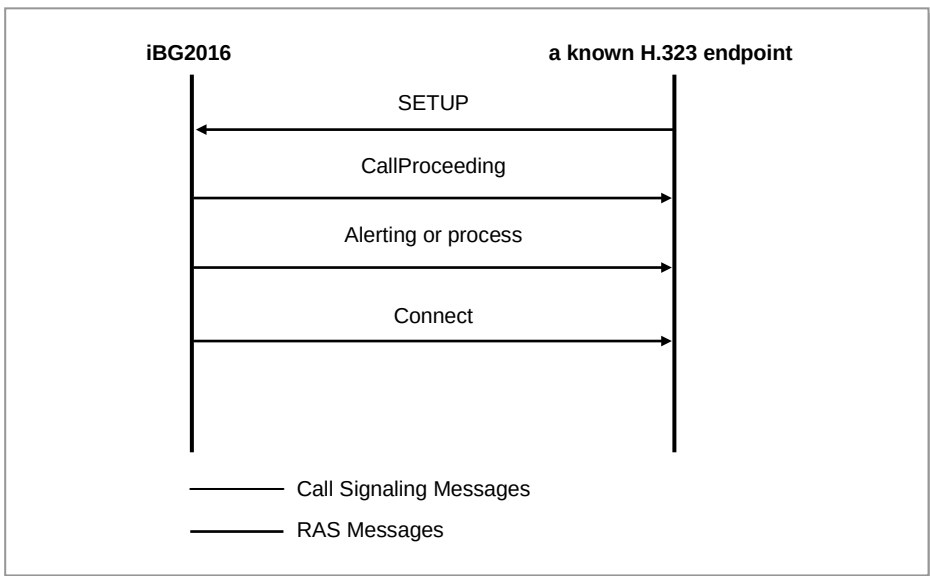


Figure 4.1 Call Setup from a known H.323 Endpoint

If the H.323 gateway is not registered in a gatekeeper, the H.225.0 SETUP message from the H.323 Endpoint is not registered as a session target on dial-peer reject calls as in Figure 4.2.

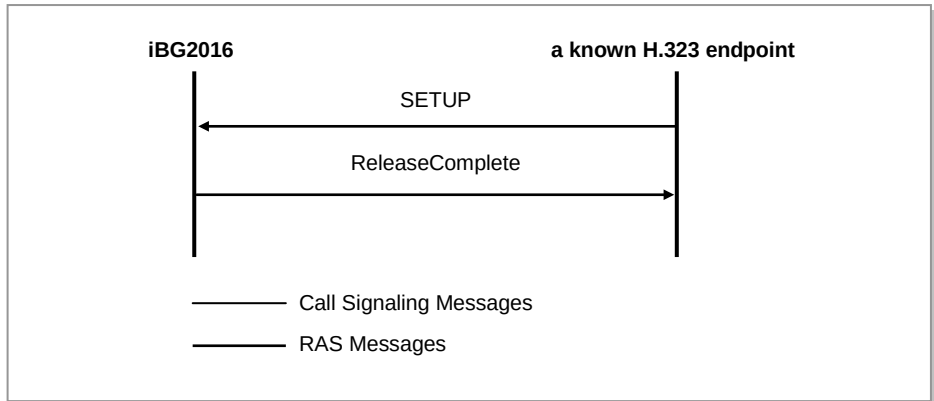


Figure 4.2 Call Setup from a unknown H.323 Endpoint, no Gatekeepers

If the H.323 gateway is registered in a gatekeeper, the H.225.0 SETUP message from the H.323 Endpoint is not registered as a session target on dial-peer following the call procedure illustrated in Figure 4.3. Figure 4.3 shows the case where a gatekeeper uses a Direct Call Signaling method.

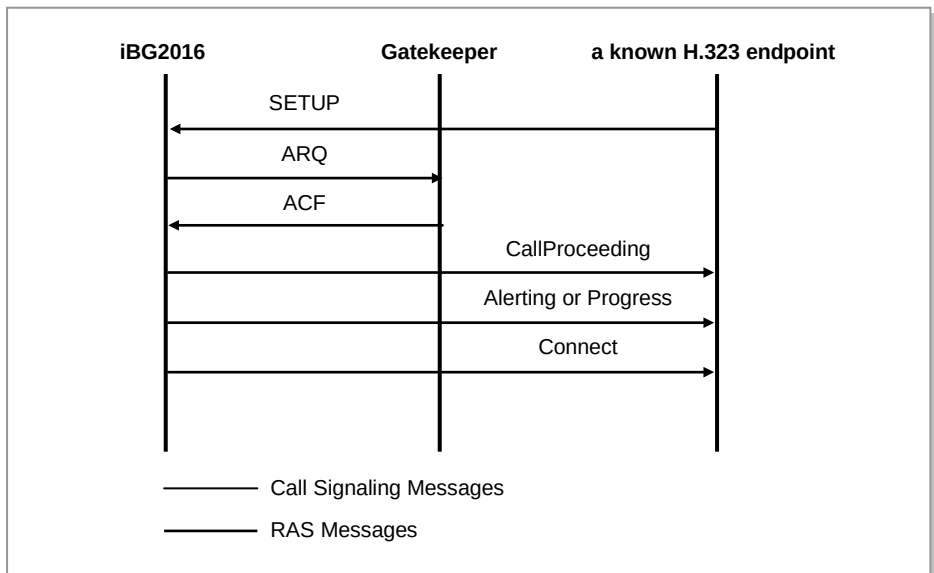


Figure 4.3 Call Setup from a unknown H.323 Endpoint, with Gatekeeper

When the H.323 gateway is registered in a gatekeeper, the H.225.0 SETUP message from the gatekeeper follows the call procedure illustrated in Figure 4.4. Figure 4.4 shows the case where a gatekeeper usually uses Gatekeeper Routed Call Signaling.

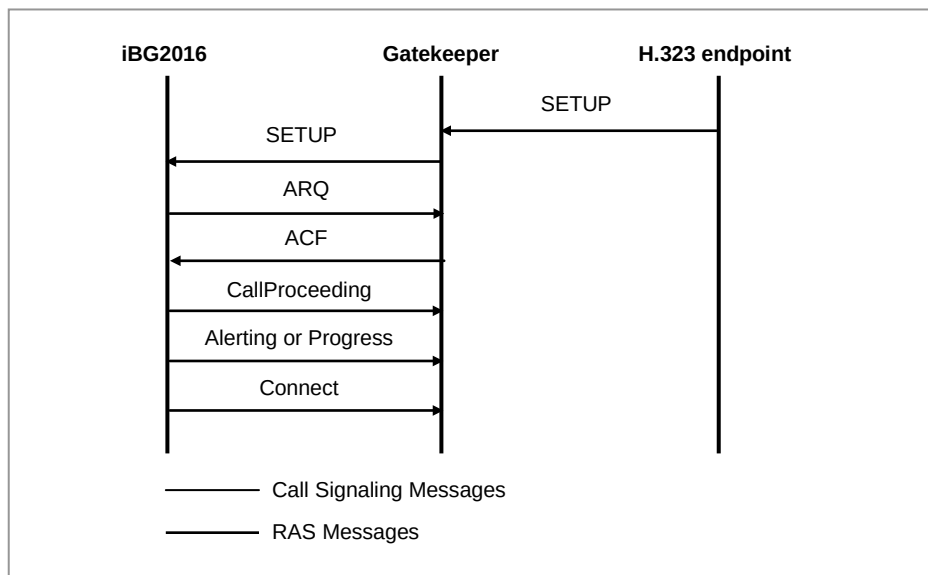


Figure 4.4 Call Setup from Gatekeeper

When a specific IP address is designated as a session target and the H.225.0 SETUP message from the H.323 Endpoint, the H.225.0 SETUP message sent from the H.323 Gateway follows the call procedure illustrated in Figure 4.5. In this case, call setup is done regardless of the existence of the gatekeeper to interwork over the H.323 network.

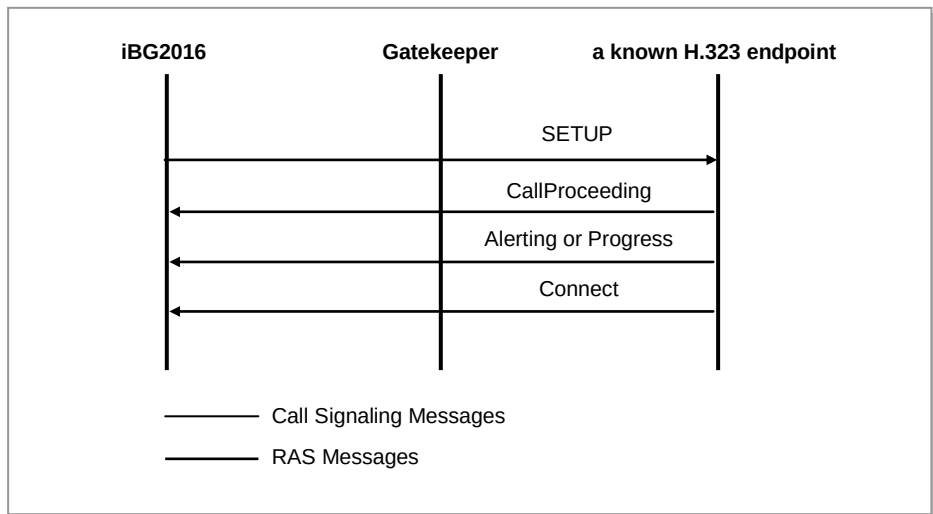


Figure 4.5 Call Setup to a known H.323 Endpoint

When a ‘gatekeeper’ is designated as a session target, the H.225.0 SETUP message sent from H.323 gateway follows the call procedure illustrated in Figure 4.6. Figure 4.6 shows the case where a gatekeeper usually uses Gatekeeper Routed Call Signaling.

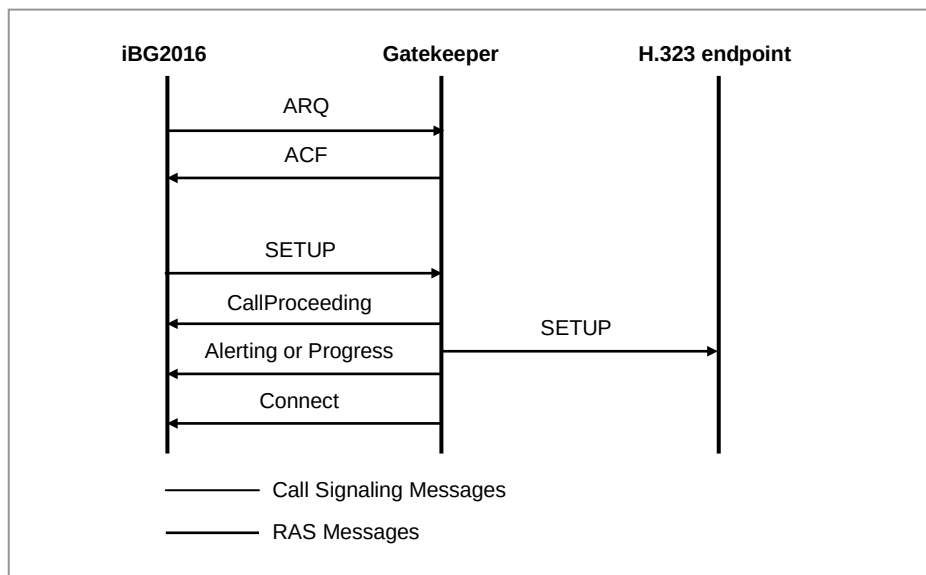


Figure 4.6 Call Setup to a Gatekeeper

RAS Signaling

RAS Signaling basically follows ITU-T Rec.H.323 recommendation; and this section describes the procedure of registering the H.323 gateway as a gatekeeper, and an Alternative Gatekeeper procedure.

Registration & UnRegistration

An operator can designate a maximum of 2 (Primary, Second) gatekeepers, and the first registration is attempted with the primary gatekeeper.

The time points when H.323 gateway attempts registration in a gatekeeper are as follows:

Table 4.2 RAS Registration Trial

Registration Attempt Time Point	Related CLI	Remarks
Time when primary gatekeeper information is set.	gatekeeper gatekeeper name	When H.323 Service is already running
When H.323 Service becomes 'up'.	no shutdown (h323-gateway configuration mode)	When primary gatekeeper information is already set.

The time points when H.323 gateway attempts unregistration from a gatekeeper are as follows:

Table 4.3 RAS UnRegistration Trial

UnRegistration Attempt Time	Related CLI	Remarks
When gatekeeper info is deleted	no gatekeeper no gatekeeper-name	Both primary and secondary gatekeeper info are deleted.
When H.323 Service is turned 'Down'	shutdown (forced) (h323-gateway configuration mode)	When registration was made.
When URQ is explicitly received from a gatekeeper.	-	When registration was made.

H.323 gateway, using the primary and secondary Gatekeeper information, performs registration as shown in Figure 4.7. (However, the Alternative Gatekeeper Procedure is omitted from the flowchart.)

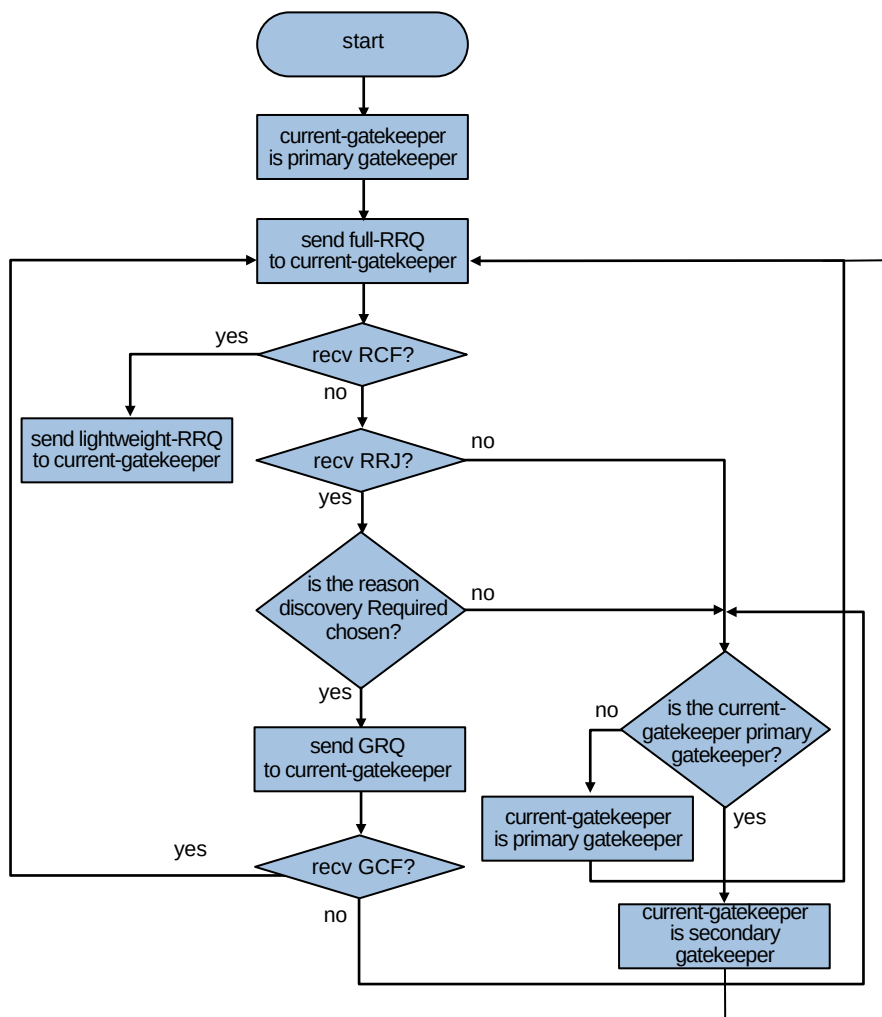


Figure 4.7 RAS Registration Procedure

Alternative Gatekeeper Procedure

H.323 gateway processes the alternate gatekeeper field (altGKList, altGKList) in the GatekeeperConfirm (GCF), GatekeeperRejection (GRJ), RegistrationConfirm (RCF) and RegistrationRejection (RRJ) Messages; and the H.323 gateway enables interworking with other gatekeepers at the GRQ and RRQ stage. This function provides redundancy when the gatekeeper interworking over the H.323 network fails and system availability, redundancy and scalability should be implemented at the gatekeeper level.

- AltGKList in GCF Messages

The alternative gatekeeper list currently managed by the H.323 gateway is replaced by the list in this field. In case of an empty AltGKList, the alternative gatekeeper list managed by the H.323 gateway is kept.

- AltGKList in RCF Messages

The alternative gatekeeper list currently managed by H.323 gateway is replaced by the list in this field. In case of an empty AltGKList, the alternative gatekeeper list managed by the H.323 gateway is cleared.

- AltGKInfo in GRJ Messages

The alternative gatekeeper list currently managed by the H.323 gateway is replaced by the list in this field. The H.323 gateway selects a gatekeeper with high priority out of the list to perform the RAS registration procedure. If no response is received from the selected gatekeeper, it selects the gatekeeper with the next highest priority to perform the RAS registration procedure. After the entire alternative gatekeeper list is selected, the RAS registration procedure is performed with the secondary gatekeeper or original gatekeeper according to the Figure 29.7.

- AltGKInfo in RRJ Messages

The alternative gatekeeper list currently managed by H.323 gateway is replaced by the list in this field. H.323 gateway selects a gatekeeper with the highest priority out of the list to perform the RAS Registration procedure. If no response is received from the selected gatekeeper, it selects the gatekeeper with the next highest priority to perform the RAS registration procedure. After the entire alternative gatekeeper list is selected, the RAS registration procedure is performed with the secondary gatekeeper or original gatekeeper according to the Figure 29.7.

Codec Negotiation

Codec Negotiation reports multiple codecs, which the H.323 gateway can support in the H.245 capability exchange stage, to a remote H.323 endpoint, so that a single codec can be selected ultimately in a call establishment stage. Multiple codecs supplied in the H.245 capability exchange stage increases the possibility of call establishment. A single dial-peer can have a single codec, or a codec list with priority. When a H.323 call occurs from a Ubigate iBG router, the codec list (or a single codec) related to the selected dial-peer is delivered to a remote H.323 endpoint via H.245 Terminal Capability Set message. When a call is received from the H.323 endpoint, the codec list (or a single codec) related to the selected dial-peer is also delivered to a remote H.323 endpoint via H.245 Terminal Capability Set message.

If a dial-peer containing an unexpected codec list is matched, using ‘incoming called-number’ on a dial-peer to match can perform dial-peer matching forcibly.

The followings are the codecs supported in H.323 gateway.

- G.711 a-law
- G.711 u-law
- G.723 series
- G.729 series (G.729, G.729 Annex A)

Support for Supplementary Services

H.323 gateway supports the supplementary services as follows for analog FXS subscribers, and no configuration is required for H.323. However, it is necessary to set the supplementary services available for analog FXS subscribers in the POTS dial-peer configuration mode.

Each service has the restrictions as described in Table 4.4.

Table 4.4 Supported Supplementary Services in H.323 Gateway

Service Name	Description	Restriction
Call Transfer (blind/consultative)	While A and B are busy, blind: A presses a hook flash, and attempts a call to C → A does hook-on → C does hook-off → Call between B and C is made. consultative: A presses a hook flash, and attempts a call to C → C does hook-off → A and C are connected (B in Hold status) → A does hook-on → Call between B and C is made	H.323 party cannot be other party (A, C) than B-party. No configuration is needed.
Call Hold & Retrieve	While A and B are busy, If A presses a hook flash, B turns to a hold status; and if A presses a hook flash again, B is retrieved.	H.323 party cannot be other party (A) than B-party. No configuration is needed.
Call Waiting	While A and B are busy, C attempts a call to A. At this time, A can hear a Call Waiting tone; and when A presses a hook flash, the call between A and C is made. (B is in a Hold status.)	H.323 party cannot be other party (A, B) than C-party. 'call-waiting' command should be set in a POTS dial-peer configuration mode.
Call Pickup	While A attempts a call to B, if C presses a specific feature code after hook-off, C can converse with A, instead of B.	H.323 party cannot be other party (B, C) than A-party. 'call-pickup-group' command should be set in a POTS dial-peer configuration mode.

Call Statistics & Debug

H.323 gateway provide the statistical information as follows:

- H.225.0 CS Message statistics (sent/received)
- H.225.0 RAS Message statistics (sent/received)
- H.245 Message statistics (sent/received)
- Call Disconnect Cause statistics (sent/received)
- Current H.323 Call List
- RAS Registration statistics

To view the statistical information as above, you must enter the command described in Table 4.5 in a privileged EXEC mode.

Table 4.5 H.323 Call Statistics Command

Command	Description
show h323-gateway h225	Accumulated data per H.225.0 CS message transceived by H.323 gateway after Ubigate iBG router is booted.
show h323-gateway h245	Accumulated data per H.245 message transceived by H.323 gateway after Ubigate iBG router is booted.
show h323-gateway ras	Accumulated data per H.225.0 RAS message transceived by H.323 gateway after Ubigate iBG router is booted.
show h323-gateway release-cause	Accumulated data per cause of H.225.0 Release Complete message transceived by H.323 gateway after Ubigate iBG router is booted.

To trace and debug the H.323 call in progress, the command described in Table 4.6 should be entered in a privileged EXEC mode.

Table 4.6 H.323 Call Tracing & Debug Command

Command	Description
debug h323 stack [h225 h245 ras all]	Shows the ASN.1 information and the encoded messages of the following messages in hexadecimal number. - h225: H.225.0 Call Signaling Message - h245: H.245 Message - ras: H.225.0 RAS Message
debug h323 vcc [in out all] [deb0 deb1 deb2 info all]	For the H.323 calls in progress, the following information is displayed. - deb0: H.323 Message sent and received - deb1: Internal Call Control Message and Call State transition information - deb2: detailed message processing information - info: not used

Configuring a H.323 Gateway

This section describes how to configure the items below.

- Prerequisites for Configuring H.323 gateways
- Configuring H.323 Bind
- Shutting Down and Enabling H.323 Services
- Configuring Basic H.323 Services
- Configuring Gateway RAS
- Configuring Multiple Codecs
- Configuring Enhanced H.323 Services

Prerequisites for Configuring H.323 Gateways

Before configuring the H.323 gateway, the following should be done first:

- IP network environment for operation
- voice network module and voice-interface card installation
- Configuration of H.323 Endpoint (Gateways, Gatekeepers, Proxies) to interwork with
- Establishing a network plan for the requirements and features of VoIP network where H.323 gateway belongs.
- Establishing a Call Routing Plan on H.323 Network

Configuring H.323 Bind

This section describes the H.323 bind feature. With this feature, you can specify the source address for H.323 signaling, and the source address for media stream as well. You can specify the interface by the Bind command or specify the IP address directly by the host ip-address command.

Restrictions for H.323 Bind

The interfaces which you can specify as the source address of H.323 signaling and media stream via Bind command are Ethernet, bundle and loopback.

Prerequisites for H.323 Bind

You must shut down the VoIP service before executing Bind command or host ip-address command. To execute the Bind command, it is necessary to first set the IP address to the interface to bind.

How to Configure H.323 Bind

1. Setting the IP Address of the interface to be bound

This procedure should be executed first before executing the bind command.

- Configuration Steps
 - configure terminal
 - interface
 - ip address
 - exit
- Detailed Steps

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters global configuration mode.
2	Interface <i>type number</i> Example) /configure# interface ethernet 0/0	Enters interface configuration mode to configure specific interface.
3	{ ip ipv6 } address <i>ip_address subnet_mask</i> Example) /configure/interface/ethernet(0/0)# ip address 90.90.90.90 255.255.255.0	Configures an IP Address for an interface.
4	exit Example) /configure/interface/ethernet(0/0)# exit	Exits the current mode

2. Shutdown voip-gateway

This procedure should be executed first before executing the bind command or host ip-address command.

- Configuration Steps
 - configure terminal
 - voip-gateway
 - shutdown
 - exit
- Detailed Steps

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters global configuration mode.
2	voip-gateway Example) /configure# voip-gateway	Enters voip-gateway configuration mode.
3	shutdown [forced] Example) /configure/voip-gateway# shutdown forced	Shut downs voip call services
4	exit Example) /configure/interface/ethernet(0/0)# exit	Exits the current mode

3. Bind control

To specify the source address of H.323 signaling, you have to do the followings.

- Configuration Steps
 - configure terminal
 - voip-gateway
 - bind control
 - exit
- Detailed Steps

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters global configuration mode.
2	voip-gateway Example) /configure# voip-gateway	Enters voip-gateway configuration mode.
3	bind control interface <i>type num</i> Example) /configure/voip-gateway# bind control interface ethernet 0/0	Sets source interface for signaling.
4	exit Example) /configure/voip-gateway# exit	Exits the current mode

4. Bind media

To specify the media stream source address, you have to do the followings.

- Configuration Steps
 - configure terminal
 - voip-gateway
 - bind media
 - exit
- Detailed Steps

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters global configuration mode.
2	voip-gateway Example) /configure# voip-gateway	Enters voip-gateway configuration mode.
3	bind media interface <i>type num</i> Example) /configure/voip-gateway# bind media interface ethernet 0/0	Sets source interface for media streams.
4	exit Example) /configure/voip-gateway# exit	Exits the current mode

5. Host ip-address

Instead of specifying the signaling and media stream source address via the bind command, you can directly specify the IP address in the following way:

- Configuration Steps
 - configure terminal
 - voip-gateway
 - host ip-address
 - exit
- Detailed Steps

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters global configuration mode.
2	voip-gateway Example) /configure# voip-gateway	Enters voip-gateway configuration mode.
3	host ip-address <i>ip-address</i> Example) /configure/voip-gateway# host ip-address ipv4:90.90.90.90	Sets source ip address for signaling and media streams.
4	exit Example) /configure/voip-gateway# exit	Exits the current mode

Shutting Down and Enabling H.323 Services

This section describes the basic configuration necessary for H.323 gateway functions. Since it is essential for H.323 call signaling, it should be done before other settings. This section also describes how to enable or disable H.323 service.

Prerequisites for Enabling H.323 Services

Before enabling H.323 service, a source IP address should be set using the Bind command or the host ip-address command.

How to Enable or Shutdown H.323 service

There are two ways of enabling or shutting down H.323 service. One way uses a shutdown command in voip-gateway configuration mode, the other uses a shutdown command in h323-gateway configuration mode. The shutdown command in h323-gateway configuration mode enables or disables only the h.323 service; the shutdown command in a voip-gateway configuration mode enables or disables not only H.323 service, but also SIP service, that is, the entire VoIP call service.

When H.323 service is actually enabled or shut down, Table 4.7 below applies.

Table 4.7 combination to enable or shutdown H.323 Service

voip-gateway	h323-gateway	H.323 Service Status
shutdown	shutdown	disabled
no shutdown	shutdown	disabled
shutdown	no shutdown	disabled
no shutdown	no shutdown	enabled

1. Shutdown in voip-gateway configuration mode
The procedure to enable or disable all VoIP call services including H.323 service is as follows:

- Configuration Steps
 - configure terminal
 - voip-gateway
 - [no] shutdown
 - exit
- Detailed Steps

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters global configuration mode.
2	voip-gateway Example) /configure# voip-gateway	Enters voip-gateway configuration mode.
3	[no] shutdown [forced] Example) /configure/voip-gateway# no shutdown	Shuts down or enables voip call services
4	Exit Example) /configure/voip-gateway# exit	Exits the current mode

2. Shutdown in h323-gateway configuration mode

The procedure to enable or disable H.323 service is as follows:

- Configuration Steps
 - configure terminal
 - voip-gateway
 - h323-gateway
 - [no] shutdown
 - exit
 - exit
- Detailed Steps

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters global configuration mode.
2	voip-gateway Example) /configure# voip-gateway	Enters voip-gateway configuration mode.
3	h323-gateway Example) /configure/voip-gateway# h323-gateway	Enters h323-gateway configuration mode.
4	[no] shutdown [forced] Example) /configure/voip-gateway/h323-gateway# no shutdown	Shuts down or enables H.323 services
5	exit Example) /configure/voip-gateway/h323-gateway# exit	Exits the current mode
6	exit Example) /configure/voip-gateway# exit	Exits the current mode

Configuring Basic H.323 Services

This section describes how to do a configuration to enable the H.323 gateway to perform a basic call processing.

Prerequisites for Basic H.323 Services

The following should be done before setting the configuration to enable the H.323 gateway to perform a basic call processing.

- H.323 services should be already enabled.
- A routing plan for POTS/VoIP call should already be established.
- The POTS side configuration of the H.323 gateway should be set normally.
- Indirect Connection where the H.323 gateway is managed by a gatekeeper.

How to Configure Basic H.323 Services

To set a configuration enabling the H.323 gateway to perform a basic call processing, use the 'dial-peer voice voip' configuration mode, in the following way.

- Configuration Steps
 - configure terminal
 - dial-peer voice voip
 - destination-pattern
 - session protocol
 - session target
 - codec or voice-class codec
 - voice-class h323
 - exit
- Detailed Steps

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters global configuration mode.
2	dial-peer voice voip <i>tag</i> Example) /configure# dial-peer voice voip 100	Enters dial-peer configuration mode for the VoIP peer designated by tag.

(Continued)

Step	Command	Purpose
3	destination-pattern <i>number</i> Example) /configure/dial-peer/voice/voip 100#destination-pattern 02.T	Specifies the telephone number associated with the dial peer. Matches dialed digits to a telephony device. The string argument is a series of digits that specifies the E.164 or private dialing plan telephone number. Valid entries are the numbers 0 through 9 and the letters A through D. You can also enter the following special characters: - The asterisk(*) or pound sign(#) on standard touch-tone dial pads can be used anywhere in the pattern. - The period(.) acts as a wildcard character. When the timer(T) character is included at the end of the destination-pattern, the router collects dialed digits until the interdigit timer expires (5 seconds, by default) or until you dial the termination character (the default is #). The timer character must be a capital T.
4	session protocol {h323 sip} Example) /configure/dial-peer/voice/voip 100#session protocol h323	A session protocol for calls between local and remote routers using the packet network.
5	session target { ip-address {ipv4:ip-address[:port] ipv6:ip-address[:port] dns:userid@hostname[:port] } sip-server gatekeeper name voip-peer-name } Example) /configure/dial-peer/voice 100#session target ip-address ipv4:192.168.10.100:1720	Specifies 'gatekeeper' as session target if you want to run an indirect connection to be managed by the gatekeeper. Specifies the IP address as the session target if you want to run a direct connection to the H.323 endpoint.

(Continued)

Step	Command	Purpose
6	codec {g711alaw g711ulaw g723r53 g723r63 g729} [<i>interval-time</i>] or voice-class codec <i>tag</i> Example) /configure/dial-peer/voice 100#codec g711alaw or /configure/dial-peer/voice 100#voice-class codec 1000	Specifies the information of a codec for a multimedia communication or Specifies the tag value of the voice class created using the 'voice class codec' command.
7	voice-class h323 <i>tag</i> Example) /configure/dial-peer/voice 100#voice-class h323 100	Tag value of the voice class created using the 'voice class h323' command.
8	exit Example) /configure/dial-peer/voice 100#exit	Exits the current mode.

Configuring RAS

This section describes the configuration necessary for the H.323 gateway to perform RAS Signaling with a gatekeeper. Since this configuration is essential in the Indirect Connection mode where the H.323 gateway is managed by a gatekeeper, it should precede the basic call processing of the H.323 gateway.

This section includes the followings.

- How to register or unregister with Gatekeeper
- How to configure RAS Retries and Timers
- How to configure RRQ TimeToLive Value

Prerequisites for Configuring RAS

The followings should be done before the H.323 gateway performs RAS signaling.

- H.323 services should be already enabled.
- The information of the H.323 gateway should be previously set on the gatekeeper to interwork.

How to register or unregister with Gatekeeper

There are 2 types of commands used for the H.323 gateway to be registered in a gatekeeper. One is the 'gatekeeper ip-address' command where you must enter the information of the gatekeeper to interwork directly; and the other one is the 'gatekeeper name' command, where you enter the gatekeeper information named by the 'voip-peer' command.

You can register or unregister the H.323 gateway in/from a gatekeeper in the following way.

1. RAS registration or unregistration using the 'gatekeeper ip-address' command.
 - Configuration Steps
 - configure terminal
 - voip-gateway
 - h323-gateway
 - h323-id
 - gatekeeper id
 - [no] gatekeeper ip-address
 - exit
 - exit
 - Detailed Steps

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters global configuration mode.
2	voip-gateway Example) /configure# voip-gateway	Enters voip-gateway configuration mode.

(Continued)

Step	Command	Purpose
3	h323-gateway Example) /configure/voip-gateway#h323-gateway	Enters h323-gateway configuration mode.
4	h323-id <i>h323-id</i> Example) /configure/voip-gateway/h323-gateway#h323-id gw.samsung.com	Defines H.323 name of this H.323 gateway.
5	[no] gatekeeper id { <i>gatekeeper-ID</i> } [primary secondary] Example) /configure/voip-gateway/h323-gateway#gatekeeper id gk1.samsung.com	Defines H.323 identification of the gatekeeper that H.323 gateway will be registered with.
6	[no] gatekeeper ip-address { <i>ipv4:ip-address</i> <i>ipv6:ip-address</i> } <i>port</i> [primary secondary] Example) /configure/voip-gateway/h323-gateway# gatekeeper ip-address ipv4:192.168.10.200 1719 primary	Defines the location of the gatekeeper if 'no' flag is not used, this command causes RAS registration. If 'no' flag is used and H323 gateway is registered with a gatekeeper, this command causes RAS unregistration.
7	exit Example) /configure/voip-gateway/h323-gateway# exit	Exits the current mode
8	exit Example) /configure/voip-gateway#exit	Exits the current mode

2. RAS registration or unregistration using the ‘gatekeeper-name’ command.

- Configuration Steps
 - configure terminal
 - voip-peer
 - ip-address
 - exit
 - voip-gateway
 - h323-gateway
 - h323-id
 - [no] gatekeeper id
 - [no] gatekeeper name
 - exit
 - exit
- Detailed Steps

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters global configuration mode.
2	voip-peer <i>peer-name</i> {h323 sip} Example) /configure#voip-peer pri-gatekeeper h323	Enters voip-peer configuration mode
3	ip-address {ipv4: <i>ip-address</i> [: <i>port</i>] ipv6: <i>ip-address</i> [: <i>port</i>] dns: <i>hostname</i> [: <i>port</i>] } Example) /configure/voip-peer pri-gatekeeper h323#ip-address ipv4:10.254.10.200:1719	specifies ip address and port
4	exit Example) /configure/voip-peer pri-gatekeeper h323#exit	Exits the current mode

(Continued)

Step	Command	Purpose
5	voip-gateway Example) /configure# voip-gateway	Enters voip-gateway configuration mode.
6	h323-gateway Example) /configure/voip-gateway#h323-gateway	Enters h323-gateway configuration mode.
7	h323-id <i>h323-id</i> Example) /configure/voip-gateway/h323-gateway#h323-id gw.samsung.com	Defines H.323 name for this H.323 gateway.
8	[no] gatekeeper id { <i>gatekeeper-ID</i> } [primary secondary] Example) /configure/voip-gateway/h323-gateway#gatekeeper id gk1.samsung.com	Defines H.323 identification for the gatekeeper that the H.323 gateway will be register with.
9	[no] gatekeeper name <i>peer-name</i> [primary secondary] Example) /configure/voip-gateway/h323-gateway#gatekeeper name pri-gatekeeper primary	Specifies peer name registered using 'voip-peer' command. if 'no' flag is not used, this command causes RAS registration. if 'no' flag is used and H323 gateway is registered with a gatekeeper, this command causes RAS unregistration.
10	exit Example) /configure/voip-gateway/h323-gateway#exit	Exits the current mode.
11	exit Example) /configure/voip-gateway#exit	Exits the current mode

How to configure RAS Retries and Timers

The 'ras timeout' command sets the time (in seconds) for the H.323 gateway to wait before resending a RAS message to the gatekeeper. The 'ras retry' command specifies the number of retransmissions of the RAS message when the specified timeout value is exceeded. The default value for timeout and retry counter value is suitable for most networks. These commands are recommended to be used when the RAS message transmission between the H.323 gateway and its interworking gatekeeper has a problem due to network environment.

The procedure of setting the timeout and retry count values for each RAS message is as follows:

- Configuration Steps
 - configure terminal
 - voice service h323
 - ras timeout
 - ras retry
 - exit
- Detailed Steps

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters global configuration mode.
2	voice service h323 Example) /configure # voice service h323	Enters 'voice service h323' configuration mode.
3	ras timeout {all arq drq grq rai rrq urq} <i>seconds</i> Example) /configure/voice/service/h323# ras timeout rrq 3	Sets RAS timeout conditions. Keywords and argument are as follows: - all: All RAS message counters that do not have explicit values configured individually. If no RAS timeout all is entered, all values set to the default except the individual values that were configured separately. - arq: Admission Request (ARQ) message counter - drq: Disengage Request (DRQ) message counter

(Continued)

Step	Command	Purpose
3	ras timeout {all arq drq grq rai rrq urq} <i>seconds</i> Example) /configure/voice/service/h323# ras timeout rrq 3	- grq: Gatekeeper Request (GRQ) message counter - rai: Resource Availability Indication (RAI) message counter - rrq: Registration Request (RRQ) message counter - urq: Unregistration Request (URQ) message counter - value: How long the gateway waits for a message from the gatekeeper before timing out, in seconds. Range: 1 to 30
4	ras retry {all arq drq grq rai rrq urq} <i>value</i> Example) /configure/voice/service/h323# ras retry rrq 5	Sets RAS retry conditions. Keywords are as above. The argument is as follows: - value: Number of times that the gateway resends messages to the gatekeeper after timeout. Range: 1 to 10.
5	Exit Example) /configure/voice/service/h323 # exit	Exits the current mode

How to configure RRQ TimeToLive

The ‘ras rrq-ttl’ command specifies the time which should be considered as the time that H.323 gateway is running after a gatekeeper receives the lightweight RRQ for the last time. The H.323 gateway sets this value (TimeToLive value) within a RRQ message and sends it to a gatekeeper. If the lightweight RRQ is not sent out from H.323 gateway within the specified time, a gatekeeper determines that the H.323 gateway has a problem, and changes the status to a unregistration status.

You can set the TimeToLive value to RRQ message in the following way:

- Configuration Steps
 - configure terminal
 - voice service h323
 - ras rrq-ttl
 - exit
- Detailed Steps

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters global configuration mode.
2	voice service h323 Example) /configure# voice service h323	Enters 'voice service h323' configuration mode.
3	ras rrq-ttl <i>time-to-live</i> Example) /configure/voice/service/h323# ras rrq-ttl 60	Sets time-to-live parameter. Argument is as follows: - time-to-live:How long, in seconds, the gatekeeper considers the gateway active. Range: 15 to 300
5	exit Example) /configure/voice/service/h323# exit	Exits the current mode

Configuring Multiple Codecs

When a single dial-peer is set, only a single codec can be specified.

This, however, decreases the possibility of call establishment. Therefore, this section describes how to set a list of codecs having priority to increase the call establishment possibility between H.323 endpoints in an H.245 capability exchange stage.

You can set multiple codecs in a single dial-peer in the following way.

- Configuration Steps
 - configure terminal
 - voice class codec
 - codec-preference
 - exit
 - dial-peer voice voip
 - voice-class codec
 - exit
- Detailed Steps

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters global configuration mode.
2	voice class codec <i>tag</i> Example) /configure# voice class codec 100	Enters voice-class configuration mode and assigns an identification tag number for a codec voice class. The tag argument is the unique number assigned to the voice class. Range: 1 to 10000.
3	codec-preference <i>value</i> {g711alaw g711ulaw g723r53 g723r63 g729} [<i>interval-time</i>] Example) /configure/voice/class/codec 100#codec-preference 1 g711alaw 20	Adds codecs to the prioritized list of codecs. Keyword and arguments are as follows: - value: Order of preference, with 1 being the most preferred and 5 being the least preferred. - codec-type: Type of codec referred. - interval-time: 10/20/30/40/50/60 (ms) Repeat this command to specify the preferred selection order for additional codecs, if required.

(Continued)

Step	Command	Purpose
4	exit Example) /configure/voice/class/codec 100# exit	Exits the current mode
5	dial-peer voice voip <i>tag</i> Example) /configure#dial-peer voice voip 1000	Enters dial-peer configuration mode for the VoIP peer designated by tag.
6	voice-class codec <i>tag</i> Example) /configure/dial-peer/voice/voip 1000#voice-class codec 100	Assigns a previously configured codec selection preference list (codec voice class) to the VoIP dial peer designated by tag. Range: 1 to 10000. Maps to the tag number created using the 'voice class codec' command.
7	exit Example) /configure/dial-peer/voice/voip 1000#exit	Exits the current mode

Configuring DTMF Relay

This section describes how to set the method of delivering DTMF tones via H.323 signaling. To relay DTMF tones, H.323 gateway supports the 4 methods as follows.

- inband
- rtp-nte
- h245-alphanumeric
- queued-digits

The inband method delivers DTMF to a voice path without separate processing. In this case, a distortion may occur due to loss of RTP packets. The rtp-nte method delivers DTMF tone via RTP according to RFC 2833, RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals. The h245-alphanumeric method delivers DTMF tones via the H.245 UserInputIndication message. The queued-digits method delivers DTMF tones as RTP packets according to RFC 2833, and Queued Digits are supported for analog-FXS subscribers.

How to Configure H.323 DTMF Relay

The DTMF Relay method can be set for all H.323 calls, or differently for each dial-peer. To set it for all H.323 calls, follow the procedure below:

- Configuration Steps
 - configure terminal
 - voice service h323
 - dtmf-relay
 - exit
- Detailed Steps

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters global configuration mode.
2	voice service h323 Example) /configure# voice service h323	Enters 'voice service h323' configuration mode.
3	dtmf-relay {inband rtp-nte h245- alphanumeric queued-digits} Example) /configure/voice/service/h323# dtmf- relay h245-alphanumeric	Specifies how to relay DTMF tone between telephony interface and H.323 network. - inband: DTMF is sent together with general voice stream. - rtp-nte: DTMF is sent using the voice stream, according to the RFC2833 recommendation - h245-alphanumeric: DTMF is sent using H.245 UserInputIndication (alphanumeric) message. - queued-digits: DTMF is sent using the voice stream according to the RFC2833 recommendation; and additionally, Queued Digits are supported for analog-FXS subscribers.
4	exit Example) /configure/voice/service/h323# exit	Exits the current mode

To set the DTMF Relay method for each dial-peer, follow the procedure below.

- Configuration Steps
 - configure terminal
 - dial-peer
 - dtmf-relay
 - exit
- Detailed Steps

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters global configuration mode.
2	dial-peer voice {pots voip} <i>tag</i> Example) /configure# dial-peer voice voip 100	Enters VoIP dial-peer configuration mode.
3	[no] dtmf-relay {inband rtp-nte h245-alphanumeric queued-digits} Example) /configure/ dial-peer/voice/voip 100# dtmf-relay h245-alphanumeric	Specifies how to relay DTMF tone between telephony interface and IP network. - inband: DTMF is sent together with general voice stream. - rtp-nte: DTMF is sent using the voice stream, according to the RFC2833 recommendation - h245-alphanumeric: DTMF is sent using H.245 UserInputIndication (alphanumeric) message. - queued-digits: DTMF is sent using the voice stream according to the RFC2833 recommendation; and additionally, Queued Digits are supported for analog-FXS subscribers.
4	Exit Example) /configure/dial-peer/voice/voip 100# exit	Exits the current mode

Configuring Enhanced H.323 Services

The additional control of the H.323 gateway call processing can be done in a ‘voice service h323’ configuration mode or ‘voice class h323’ configuration mode. The ‘voice service h323’ configuration is applied to all H.323 calls, while ‘voice class h323’ configuration is applied only at a dial-peer level. If a specific dial-peer specifies an already-created voice class using the ‘voice-class h323’ command, the specified ‘voice class h323’ configuration has a priority over the ‘voice service h323’ configuration. The commands in the Table 4.8 below are those available in each configuration mode.

Table 4.8 commands of ‘voice service h323’ configuration and ‘voice class h323’ configuration

command	Description	voice service h323	voice class h323
h225 call-start	Specifies the H.323 call setup method.	O	O
h225 early-h245	Specifies whether to perform the normal H.245 procedure before or after CONNECT message.	O	O
h225 h245-tunnel	Specifies the H.245 Tunneling support.	O	O
h225 T301	Maximum time to wait for CONNECT or RELCOMP message, after receiving ALERT message.	O	O
h225 T303	Maximum time to wait for CALLPROCEEDING or ALERTING or PROGRESS or RELCOMP message, after sending SETUP message.	O	O
h225 call-response	Specifies, as a response to SETUP message, what H.225.0 CS message to send after call proceeding.	O	X
dtmf-relay	Specifies the method of delivering DTMF for H.323 call.	O	X

Let’s discuss how to use commands in the ‘voice service h323’ configuration mode. The commands are used in the same way even in a ‘voice class h323’ configuration mode. But, there is a keyword ‘system’ for each command in a ‘voice class h323’ configuration mode. This means that the same command settings are used in a ‘voice service h323’ configuration mode.

1. h225 call-start

You can perform H.323 call setup in the following way:

- Configuration Steps
 - configure terminal
 - voice service h323
 - h225 call-start
 - exit
- Detailed Steps

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters global configuration mode.
2	voice service h323 Example) /configure# voice service h323	Enters 'voice service h323' configuration mode.
3	h225 call-start {fast slow} Example) /configure/voice/service/h323#h225 call-start fast	Specifies how to setup H323 call
4	exit Example) /configure/voice/service/h323#exit	Exits the current mode

2. h225 early-h245

The settings to execute the Early H245 Procedure during H.323 Call Signaling are as follows:

- Configuration Steps
 - configure terminal
 - voice service h323
 - h225 early-h245
 - exit
- Detailed Steps

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters global configuration mode.
2	voice service h323 Example) /configure# voice service h323	Enters 'voice service h323' configuration mode.
3	h225 early-h245 {on off} Example) /configure/voice/service/h323#h225 early-h245 on	Specifies whether early H245 procedure should be implemented during call signaling
4	exit Example) /configure/voice/service/h323#exit	Exits the current mode

3. h225 h245-tunnel

The settings to support H.245 Tunneling during H.323 Call Signaling are as follows:

- Configuration Steps
 - configure terminal
 - voice service h323
 - h225 h245-tunnel
 - exit
- Detailed Steps

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters global configuration mode.
2	voice service h323 Example) /configure# voice service h323	Enters 'voice service h323' configuration mode.
3	h225 h245-tunnel {on off} Example) /configure/voice/service/h323#h225 h245-tunnel on	Specifies whether h245 tunneling method will be supported during call-signaling
4	exit Example) /configure/voice/service/h323#exit	Exits the current mode

4. h225 call-response

You can determine which H.225.0 message to send as a response to the H.225.0 Setup message.

- Configuration Steps
 - configure terminal
 - voice service h323
 - h225 call-response
 - exit
- Detailed Steps

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters global configuration mode.
2	voice service h323 Example) /configure# voice service h323	Enters 'voice service h323' configuration mode.
3	h225 call-response {alert progress} Example) /configure/voice/service/h323#h225 call-response progress	Specifies which message to be send in response to H.225.0 SETUP message
4	exit Example) /configure/voice/service/h323#exit	Exits the current mode

Verifying and Troubleshooting H.323 Features

This section describes how to use the show command and debug command to verify and troubleshoot the H.323 feature of Ubigate iBG router.

Using show commands

You can use show commands as follows to confirm or see the current status of the H.323 feature settings.

show h323-gateway service

Shows the H.323 service status. The service status is 'up' or 'down'.

Example)

```
# show h323-gateway service
H.323 service is up
```

show h323-gateway status

This command shows the information of a server port of the H.323 gateway.

Example)

```
# show h323-gateway status
=====
          H.323 Server Port Configuration
=====
H.225.0 Call Signalling Port: 1720
H.225.0 RAS Signalling Port: 1719
H.245 Server Port Range: 32768 - 33023
```

```
=====
          H.323 Server Port Status
=====
H.225.0 Call Signalling Port: TCP Opened(IP
Address[10.254.139.45] Port[1720])
H.225.0 RAS Signalling Port: UDP Opened(IP
Address[10.254.139.45] Port[1719])
```

show h323-gateway detailed

This command shows all the setting values of 'voice class h323'.

Example)

```
# show h323-gateway detailed
=====
VOICE SERVICE H323
=====
dtmf-relay: [rtp-nte]
tech-prefix: []
h225
    call-start      : fast
    h245-tunnel     : on
    early-h245      : off
    call-response   : alert
    t301            : 180
    t303            : 15
ras
    rrq-ttl         : 60
    msg retry timeout
    all      2      3
    arq      2      5
    drq      2      3
    grq      2      5
    rrq      2      3
    rai      2      3
    urq      1      3
```

show h323-gateway registration

This command shows the gatekeeper registration of H.323 gateway.

Example)

```
# show h323-gateway registration
H323-ID ibg.samsung.com
Primary gatekeeper information is configured as below.
Gatekeeper ID: GK1
IP address : 10.254.139.50
RAS port : 1719
Secondary gatekeeper information is not configured.
```

This gateway is registered with a gatekeeper.

Gatekeeper ID: GK1

IP address : 10.254.139.50

RAS port : 1719

Alternative Gatekeeper List from Gatekeeper:

1. GK-ID[GK2] IPAddr[10.254.149.50] Port[1719] Priority[0]
NeedToReg[True]

2. GK-ID[GK3] IPAddr[10.254.159.50] Port[1719] Priority[1]
NeedToReg[True]

show h323-gateway calls

Shows the status of H.323 calls in progress.

Example)

```
# show h323-gateway calls
=====
Current H323 Calls                               Current
Time: 2005/11/29 06:09:55.280   Total:   2 calls
=====
=====
CRV   CallState          SrcIpAddr  SrcPort  DstIpAddr
DstPort StartTime
-----
-----
13    CallDelivered      10.254.167.239  1111
10.254.167.235  1720  2005/11/29 06:09:40.370
14    Active             10.254.167.239  1113
10.254.167.235  1720  2005/11/29 06:09:50.720
```

Using debug commands

You can use the following debug commands to view the debugging messages of an application, or the H.323 message sent or received.

debug h323 log

Command to view the H.323 message. You can display messages by filtering them by calling number or called number.

debug h323 vcc

Displays the debugging messages of the H.323 call processing task.

debug h323 stack

Displays the debugging messages of the H.323 stack level.



CHAPTER 5. Analog Voice Port

Introduction to Analog Voice Port Features

This chapter describes Analog Voice Port Features. Analog Voice Port plays a role in transmitting voice and call signals between a packet-based network and the existing telephony network. The configuration of the Analog Voice Port is automatically perceived while booting up the system, and can basically work as a default Configuration.

- Analog FXS and FXO Interface
- Analog E & M Interface

Analog FXS and FXO Interface

FXS - Foreign eXchange Subscriber interface

FXS (the plug on the wall) delivers POTS service from the local phone company's Central Office (CO) and must be connected to subscriber equipment (telephones, modems, and fax machines). In other words an FXS interface points to the subscriber.

FXO - Foreign eXchange Office interface

FXO (the plug on the phone) receives POTS Service, typically from a Central Office of the Public Switched Telephone Network (PSTN). In other words an FXO interface points to the Telco office. A standard RJ-11 modular telephone cable connects the FXO voice interface card to the PSTN or PBX through a telephone wall outlet.

FXO and FXS interfaces indicate on-hook or off-hook status and the seizure of telephone lines by one of two access signaling methods: loop start or ground start.

Loop Start Signaling

Loop-start is generally used in Analog FXS/FXO instead of Ground-start. Hooking off handset makes a circuit close, and off-hook status is detected, while Ubigate iBG sends dial tone. Also it sends an on/off pattern ring to receive dial tone.

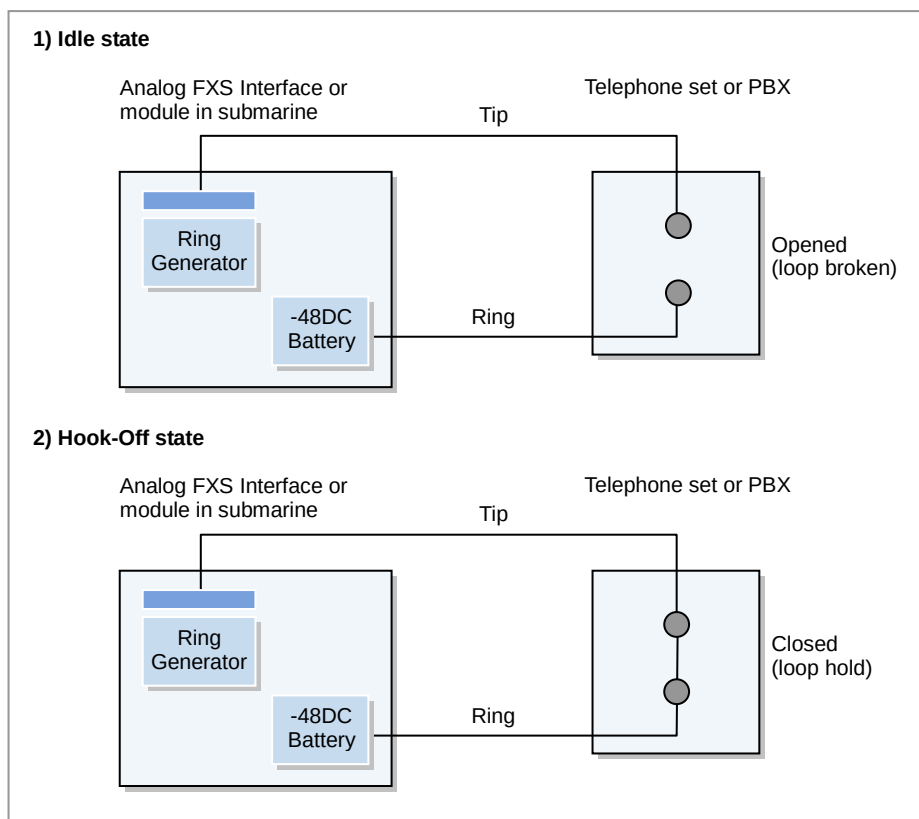


Figure 5.1 Loop Start Signaling

Ground Start Signaling

It works by using ground and current detectors that allow the network to indicate off-hook or seizure of an incoming call independent of the ringing signal and allow for positive recognition of connects and disconnects.

For these reasons, the ground-start method is used as the inter-PBX Trunk line.

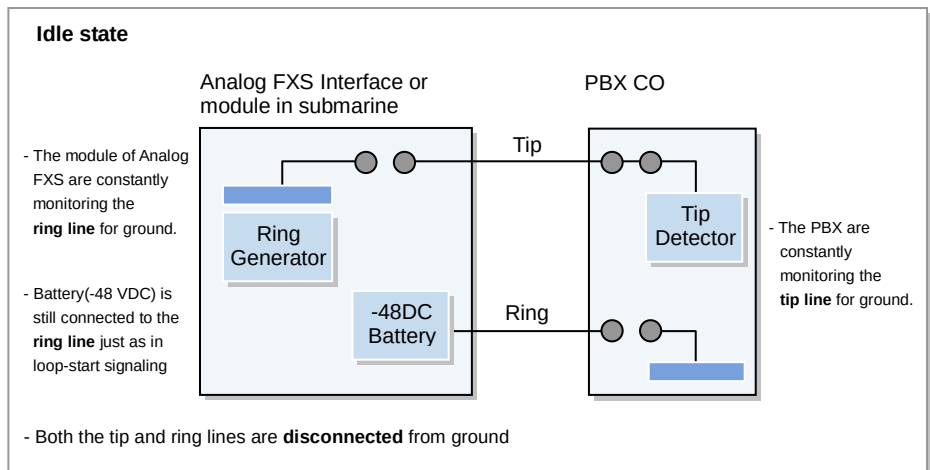


Figure 5.2 Ground-start signaling for Analog FXS (Idle-state)

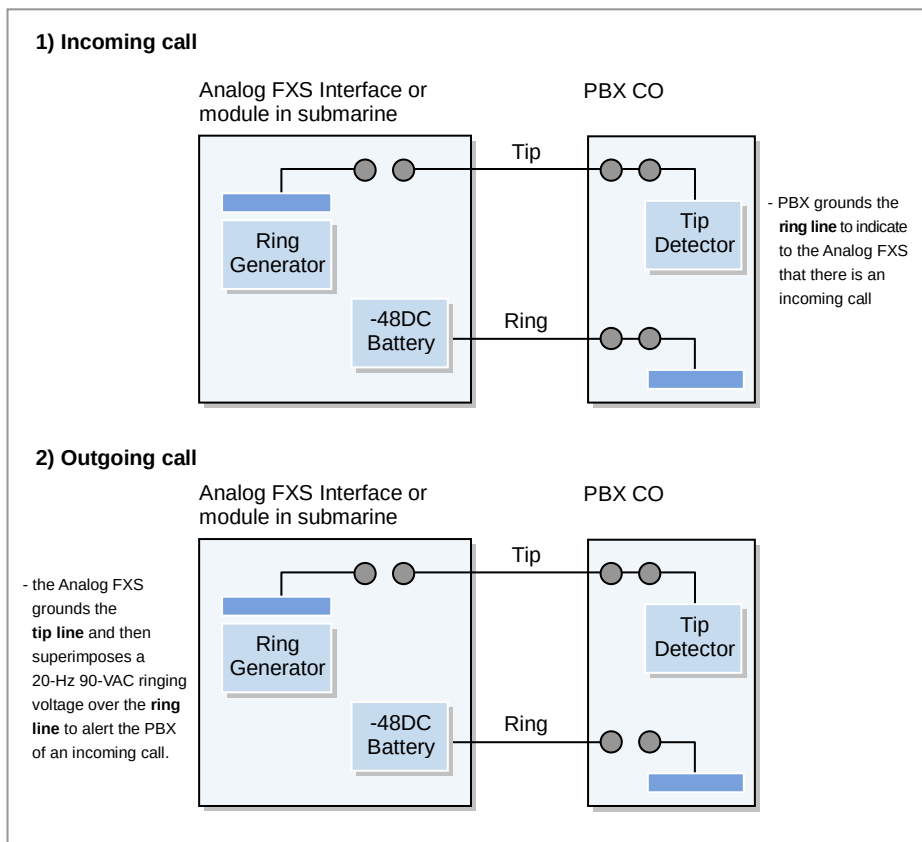


Figure 5.3 Ground-start signaling for Analog FXS (seizure-state)

Analog E & M Interface

Analog E & M Interface

Analog E & M interface uses special signaling paths that are separate from the trunk's audio path to convey information about the calls.

The signaling paths are known as the E-lead and the M-lead. The name E & M is thought to be derived from the phrase Ear and Mouth or rEceive and transMit although it could also come from Earth and Magnet.

E & M method, having an Answer/Disconnect Message, is preferred to FXS/FXO.

The physical E & M interface is an RJ-48 connector that connects to PBX trunk lines, which are classified as either two-wire or four-wire. This refers to whether the audio path is full duplex on one pair of wires (two-wire) or on two pair of wires (four-wire).

A connection may be called a four-wire E & M circuit although it actually has six to eight physical wires. It is an analog connection although an analog E & M circuit may be emulated on a digital line. For more information on digital voice port configuration of E & M signaling, see the 'Digital Trunk T1-CAS Features' section.

Immediate-Start Method

Immediate-start is the simplest E & M Access signaling. Calling side hooks off E-lead to enter 'seizure' action, and sends address information. Use Dual-Tone Multi-Frequency (DTMF) digits or MF for address information.

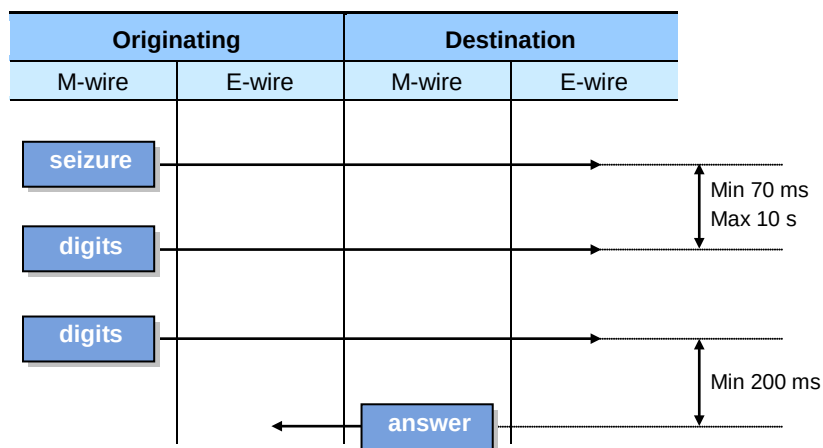


Figure 5.4 Immediate method signaling sequence

Wink-Start Method

Wink-start is the most used E & M Access method, and the default voice port signaling. Wink-start method hooks off E-lead to enter ‘seizure’ action, and then receives ‘Wink’ of M-lead on the counterpart office, and transmits address information.

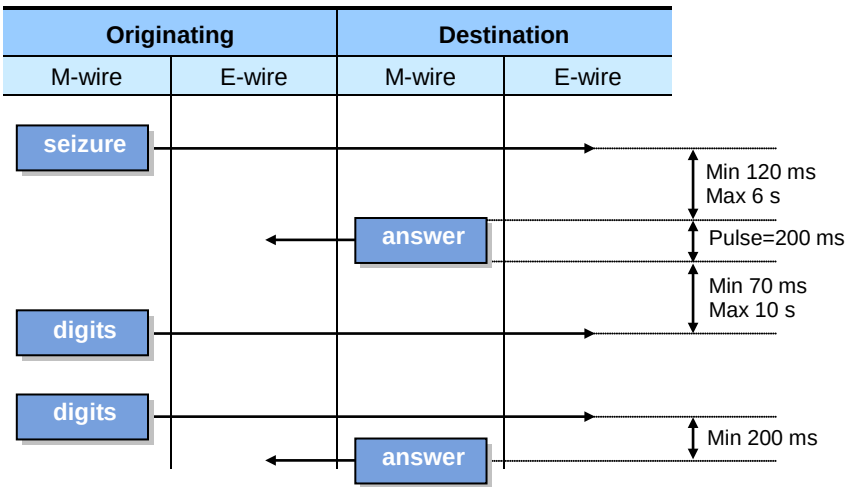


Figure 5.5 wink method signaling sequence

Delay-Dial Method

Delay-dial method enters 'seizure' action by hooking off E-lead from the calling side, after a given time, about 200ms, when the calling side takes a look at the status of the terminating side, if the terminating side is on hook status (or he/she awaits till the terminating side enters into on-hook status), the calling side sends address information.

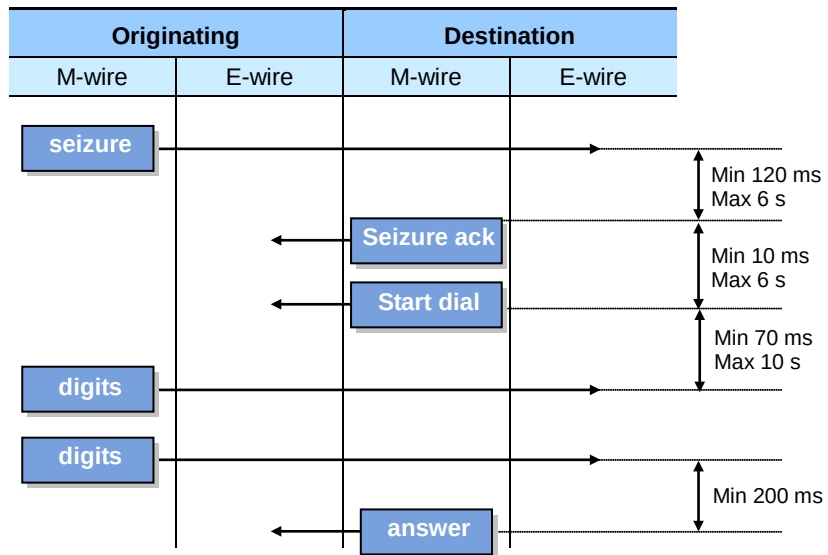


Figure 5.6 delay method signaling sequence

Analog E & M Type

For Analog E & M, the type (I-V) distinguished depending on the status of On-hook/off-hook is used, Ubigate iBG supports E & M Type I, II, III, and V Type. Table 5.1 explains the difference on signaling for the E & M type.

Table 5.1 E & M Wiring and Signaling Methods

E & M Type	E-Lead Configuration	M-Lead Configuration	Signaling Battery Lead	Signaling Ground Lead
I	Output, Relay to ground	Input, referenced to ground	-	-
II	Output, Relay to SG	Input, referenced to ground	Feed for M, connected to -48V	Return for E, Galvanically isolated from ground
III	Output, Relay to ground	Input, referenced to ground	Connected to -48V	Connected to ground
V	Output, Relay to ground	Input, referenced to -48V	-	-

Analog Voice Port Monitoring

This section describes the configuration of the analog voice port. The analog voice port as an architecture to create a basic configuration of a voice port by which Ubigate iBG automatically detects H/W information. Accordingly, when starting up the system, the port number of the analog voice port is shown automatically to an operator, and it is able to enter into a basic service.

Voice port Status.

Voice port enters the following status according to the status of the H/W connection or call processing service.

```
v239# show voice port summary
```

PORT	CH	SIG	TYPE	ADMIN	OPER	IN	STATUS	OUT	STATUS	EC
====	==	=====		=====	=====	==	=====	===	=====	==
0/0/0	--	fxs-ls		up	up	on-hook		idle		y
0/0/1	--	fxs-ls		up	up	on-hook		idle		y
0/0/2	--	fxs-ls		up	up	on-hook		idle		y
0/0/3	--	fxs-ls		up	up	on-hook		idle		y
0/1/0:10	01	r2-mfc		up	up	idle		idle		y
0/1/0:10	02	r2-mfc		up	up	idle		idle		y
0/1/0:10	03	r2-mfc		up	up	idle		idle		y
0/1/0:10	04	r2-mfc		up	up	idle		idle		y
0/1/0:10	05	r2-mfc		up	up	idle		idle		y
0/1/0:10	06	r2-mfc		up	up	idle		idle		y
0/1/0:10	07	r2-mfc		up	up	idle		idle		y
0/1/0:10	08	r2-mfc		up	up	idle		idle		y
0/1/0:10	09	r2-mfc		up	up	idle		idle		y
0/1/0:10	10	r2-mfc		up	up	idle		idle		y

PORT

Presents the logical voice ports created in the analog voice port and digital voice port by using the geographical location presentation method.

Form of slot/sub-slot/port: analog voice card such as analog FXS, analog FXO, analog E & M, ISDN BRI.

Form of slot/sub-slot/port:ds0-group-no: shows ds0-groups created in digital voice port and ds0-channels that belonged to the appropriate ds0-groups.

SIG-TYPE

Indicates signaling type set up in the ds0-group or analog voice port.

ADMIN

Up/down: indicates the status of the voice port in accordance with the operator's control. This appears as 'down' when an operator executes shutdown command in voice port configuration mode, but 'up' when executing 'no shutdown'.

OPER

Indicates status changes while voice port or DS0 channel works. This appears as 'up' in case the voice port or DS0 channel is in normal service, and as 'down' while the voice port is out of service due to failure of voice card. Indicates as 'block' when blocked by an operator, or a channel is not available when it signals.

IN STATUS

Indicates status changes when the analog voice port or DS0 channel handles a call.

At this time, call state is indicated differently according to the signaling method in each SIG-Type analog of the voice port or DS0 channel. 'Idle', 'ringing', 'off-hook', 'out_of_svc', 'busy', 'seized', 'answered' etc.

OUT STATUS

Indicates status changes when analog voice port or DS0 channel handles a call.

At this time, call state is indicated differently according to the signaling method in each SIG-Type analog of the voice port or DS0 channel. 'Idle', 'ringing', 'off-hook', 'out_of_svc', 'busy', 'seized', 'answered' etc.

Also by busyout function, 'static_busyout', 'dynamic_busyout' is indicated. In case of analog voice port, indications such as 'tone_dial', 'tone_rb', 'tone_busy', 'tone_congest', 'ringing' are added.

EC

Indicates the working of the echo cancellation function set up in analog voice port or DS0.

Prerequisites to Configure Analog Voice ports

Before configuration of the Voice port, the user should predefine the following information and determine the following with interworking Opposite PBX in advance.

- Telephony signaling interface: Analog FXO, FXS or E & M
- Locale Code (usually the country) for Call Progress Tone or DTMF/MF Variant
- If FXO, type of Signal: loop-start or ground-start
- If FXS, type of Signal: loop-start or ground-start or DID
- If E & M, type: I, II, III, or V
- If E & M, type of line: two-wire or four-wire
- If E & M, type of start signal: wink, immediate, delay-dial
- If E & M, type of Dialing: DTMF or MF

Configuring Analog FXS Voice Port

This section describes the configuration of the analog FXS voice port.

How to Configure Analog FXS Voice Port

To set up each parameter of the basic analog voice port, follow the next procedures.

- Configuration Steps
 - configure terminal
 - voice-port
 - dial-peer voice pots
 - exit
- Detailed Steps

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters global configuration mode.
2	voice-port slot/subslot/port	Enter voice port Configuration Mode. Slot - Specifies the number of the router slot where the voice module in installed. Subslot - Specifies the number of subslot in the slot Port - Indicates the voice port.
3	shutdown	Change status of voice port to shutdown.
4	signal {loop-start ground-start}	Selects the access signaling type to match that of the telephony connection you are making. The keywords are as follows: Loop-start - (default) Uses a closed circuit to indicate off-hook status; used for residential loops. Ground-start - Uses ground and current detectors; preferred for PBXs and trunks.

(Continued)

Step	Command	Purpose
5	ring frequency {20 25 30 50}	Selects ring frequency 20 Hz frequency 25 Hz frequency 30 Hz frequency 50 Hz frequency
6	ring cadence on-net {cadence define pulse interval pulse interval pulse interval}	Changes Ring Cadence for on-net Call.
7	ring cadence off-net {cadence define pulse interval pulse interval pulse interval}	Changes Ring Cadence for off-net Call.
8	locale locale	Selects the two-letter locale for the voice call progress tones and other locale-specific parameters to be used on this voice port. The Default is us ex) locale us.
9	timeouts timer-name timer-value	To change timeouts parameters. Initial - Sets the number of seconds that the system waits between the caller input of the initial digit and the subsequent digit of the dialed string. A valid entry is from 0 to 120. The default is 10. Interdigit - Configures the number of seconds that the system waits after the caller has input the initial digit or a subsequent digit of the dialed string. If the timeout ends before the Destination is identified, a tone sounds and the call ends. This value is important when using variable-length dial peer destination patterns (dial plans). The seconds argument is the interdigit timeout wait time in seconds. A valid entry is an integer from 0 to 120. The default is 5.

(Continued)

Step	Command	Purpose
9	timeouts <i>timer-name timer-value</i>	Ringing - Specifies the duration that the voice port allows ringing to continue if a call is not answered. The range is from 0 to 60000. The default is 180. 0 means infinity. Wait-release - Specifies the duration that a voice port stays in the call-failure state while the device sends a busy tone, reorder tone, or an out-of-service tone to the port. The range is from 0 to 3600. The default is 30. 0 means infinity.
10	timing hookflash-out <i>timer-value</i>	The duration of the hookflash, in milliseconds.
11	no shutdown	Change shutdown Status of voice-port to in-Service.
12	exit	Exits voice port configuration mode.
13	dial-peer voice {pots voip} <i>tag</i> Example) /configure# dial-peer voice pots 11	Enters dial-peer configuration mode and defines a local dial peer that connects to a POTS interface. The <i>number</i> argument is one or more digits. Identifying the dial peer. Valid entries are from 1 to 10000. The pots keyword indicates a dial peer using basic telephone service.
14	destination-pattern WORD Example) /configure# voice-port> destination-pattern 1004	Setting Destination-pattern Matches dialed digits to a telephony device. The string argument is a series of digits that specify the E.164 or private dialing plan telephone number. Valid entries are the numbers 0 through 9 and the letters A through D.

(Continued)

Step	Command	Purpose
14	destination-pattern WORD Example) /configure# voice-port> destination-pattern 1004	You can also enter the following special characters: - The asterisk(*) or pound sign(#) on standard touch-tone dial pads can be used anywhere in the pattern. - The period(.) acts as a wildcard character. When the timer(T) character is included at the end of the destination pattern, the router collects dialed digits until the interdigit timer expires (5 seconds, by default) or until you dial the termination character (the default is #). The timer character must be a capital T.
15	port slot/subslot/port	Maps the dial peer to a specific Port Number.
16	exit	Exits voice dial-peer configuration mode.

Predefined ring cadence patterns.

The Analog FXS Ring Cadence has a predefined pattern as follows, and can be set up by on-net, or off-net respectively. On-net means an inbound call coming from the FXS line within Ubigate iBG, while off-net means inbound transit call.

Voice-port> ring cadence on-net|off-net {cadence|define pulse interval pulse interval pulse interval}

Each pattern specifies a ring-pulse time and a ring-interval time.

- **pattern01** - 2 seconds on, 4 seconds off
- **pattern02** - 1 second on, 4 seconds off
- **pattern03** - 1.5 seconds on, 3.5 seconds off
- **pattern04** - 1 second on, 2 seconds off
- **pattern05** - 1 second on, 5 seconds off
- **pattern06** - 1 second on, 3 seconds off
- **pattern07** - 0.8 second on, 3.2 seconds off
- **pattern08** - 1.5 seconds on, 3 seconds off
- **pattern09** - 1.2 seconds on, 3.7 seconds off

- **pattern09** - 1.2 seconds on, 4.7 seconds off
- **pattern11** - 0.4 second on, 0.2 second off, 0.4 second on, 2 seconds off
- **pattern12** - 0.4 second on, 0.2 second off, 0.4 second on, 2.6 seconds off

In case of SIP Inbound call, which may contain the following ring cadence in the message, in this case, Ubigate iBG manually plays ring.

- **bellCore1** - 2 seconds on, 4 seconds off, 2 seconds on, 4 seconds off
- **bellCore2** - 0.8 second on, 0.4 second off, 0.8 second on, 4 seconds off
- **bellCore3** - 0.4 second on, 0.2 second off, 0.4 second on, 0.2 second off, 0.8 second on, seconds off
- **bellCore4** - 0.3 second on, 0.2 second off, 1 second on, 0.2 second off, 0.3 second on, seconds off
- **bellCore5** - 0.5 second on, 0 second off

User-defined ring cadence patterns.

`Voice-port> ring cadence on-net|off-net {cadence|define pulse interval pulse interval pulse interval}`

Each number pair specifies one ring-pulse time and one ring-interval time. You must enter numbers in pairs, and you can enter from 1 to 3 pairs. The second number in the last pair that you enter specifies the interval between rings.

pulse - Number (1 or 2 digits) specifying ring-pulse (on) time in hundreds of milliseconds. Range is from 1 to 50, for pulses of 100 to 5000 ms.

For example: 1 = 100 ms; 10 = 1 s, 40 = 4 s.

interval - Number (1 or 2 digits) specifying ring-interval (off) time in hundreds of milliseconds. Range is from 1 to 50, for pulses of 100 to 5000 ms.

For example: 1 = 100 ms; 10 = 1 s, 40 = 4 s.

Dualtone

The dualtone command enters the custom-cptone configuration mode and specifies a call-progress tone to be detected. You can specify additional call-progress tones without exiting the custom-cptone configuration mode.

Configure>voice class custom-cptone *tag* dualtone {busy|dialtone|number-unobtainable|ringback}

busy - Busy tone.

dialtone - Dial tone.

number-unobtainable - Number-unobtainable tone.

ringback - Ringback tone.

Cadence

To define the tone-on and tone-off duration for a call-progress tone, use the cadence command in the call-progress dualtone configuration mode.

Configure>voice class custom-cptone *tag* dualtone busy cadence {cycle-1-on-time cycle-1-off-time [cycle-2-on-time cycle-2-off-time] [cycle-3-on-time cycle-3-off-time] [cycle-4-on-time cycle-4-off-time]}

cycle-1-on-time - Tone-on duration for the first cycle of the cadence pattern, in milliseconds (ms). Range is from 0 to 1000. The default is 0.

cycle-1-off-time - Tone-off duration for the first cycle of the cadence pattern, in milliseconds (ms). Range is from 0 to 1000. The default is 0.

cycle-2-on-time - (Optional) Tone-on duration for the first cycle of the cadence pattern, in milliseconds (ms). Range is from 0 to 1000. The default is 0.

cycle-2-off-time - (Optional) Tone-off duration for the first cycle of the cadence pattern, in milliseconds (ms). Range is from 0 to 1000. The default is 0.

cycle-3-on-time - (Optional) Tone-on duration for the first cycle of the cadence pattern, in milliseconds (ms). Range is from 0 to 1000. The default is 0.

cycle-3-off-time - (Optional) Tone-off duration for the first cycle of the cadence pattern, in milliseconds (ms). Range is from 0 to 1000. The default is 0.

cycle-4-on-time - (Optional) Tone-on duration for the first cycle of the cadence pattern, in milliseconds (ms). Range is from 0 to 1000. The default is 0.

cycle-4-off-time - (Optional) Tone-off duration for the first cycle of the cadence pattern, in milliseconds (ms). Range is from 0 to 1000. The default is 0.

Configuring Analog FXO Voice Port

This section describes the configuration of analog FXO voice port.

How to Configure Analog FXO Voice Port

To set up each parameter of the basic analog FXO voice port, follow these procedures:

- Configuration Steps
 - configure terminal
 - voice-port
 - dial-peer voice pots
 - exit
- Detailed Steps

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters global configuration mode.
2	voice-port <i>slot/subslot/port</i>	Enters voice port Configuration Mode. slot - Specifies the number of the router slot where the voice module is installed. subslot - Specifies the number of subslots in the slot. port - Indicates the voice port.
3	shutdown	Change status of voice port to shutdown.

(Continued)

Step	Command	Purpose
4	signal { <i>loop-start</i> <i>ground-start</i> }	Selects the access signaling type to match that of the telephony connection you are making. The keywords are as follows: loop-start - (default) Uses a closed circuit to indicate off-hook status; used for residential loops. ground-start - Uses ground and current detectors; preferred for PBXs and trunks.
5	dial-type {dtmf mf}	Specifies the dialing method for outgoing calls.
6	ring number <i>number</i>	(FXO only) Specifies the maximum number of rings to be detected before an incoming call is answered by the router. The default is 1.
7	locale <i>locale</i>	Selects the two-letter locale for the voice call progress tones and other locale-specific parameters to be used on this voice port The Default is us ex) locale us.
8	timeouts <i>timer-name</i> <i>timer-value</i>	To change timeouts parameters initial - Sets the number of seconds that the system waits between the caller input of the initial digit and the subsequent digit of the dialed string. A valid entry is from 0 to 120. The default is 10. interdigit - Configures the number of seconds that the system waits after the caller has input the initial digit or a subsequent digit of the dialed string. If the timeout ends before the Destination is identified, a tone sounds and the call ends. This value is important when using variable-length dial peer destination patterns (dial plans). The <i>seconds</i> argument is the interdigit timeout wait time in seconds. A valid entry is an integer from 0 to 120. The default is 5.

(Continued)

Step	Command	Purpose
8	timeouts <i>timer-name</i> <i>timer-value</i>	ringing - Specifies the duration that the voice port allows ringing to continue if a call is not answered. The range is from 0 to 60000. The default is 180. 0 means infinity. wait-release - Specifies the duration that a voice port stays in the call-failure state while the device sends a busy tone, reorder tone, or an out-of-service tone to the port. The range is from 0 to 3600. The default is 30. 0 means infinity.
9	timing digit <i>timer-value</i>	Specifies the DTMF digit signal duration.
10	timing guard-out timer-value	(FXO ports only) specifies the duration in milliseconds of the guard-out period that prevents this remote port from detecting a disconnect signal.
11	no shutdown	Change shutdown Status of the voice-port to in-Service.
12	exit	Exits voice port configuration mode.
13	dial-peer voice {pots voip} <i>tag</i> Example) /configure# dial-peer voice pots 11	Enters dial-peer configuration mode and defines a local dial peer that connects to a POTS interface. The <i>number</i> argument is one or more digits. Identifying the dial peer. Valid entries are from 1 to 10000. The pots keyword indicates a dial peer using basic telephone service.
14	destination-pattern <i>WORD</i> Example) /configure# voice-port> destination-pattern 1004	Setting Destination-pattern matches dialed digits to a telephony device. The <i>string</i> argument is a series of digits that specify the E.164 or private dialing plan telephone number. Valid entries are the numbers 0 through 9 and the letters A through D.

(Continued)

Step	Command	Purpose
14	destination-pattern <i>WORD</i> Example) /configure# voice-port> destination-pattern 1004	You can also enter the following special characters: - The asterisk(*) or pound sign(#) on standard touch-tone dial pads can be used anywhere in the pattern. - The period(.) acts as a wildcard character. When the timer(T) character is included at the end of the destination pattern, the router collects dialed digits until the interdigit timer expires (5 seconds, by default) or until you dial the termination character (the default is #). The timer character must be a capital T.
15	port <i>slot/subslot/port</i>	Maps the dial peer to a specific Port Number.
16	exit	Exits voice dial-peer configuration mode.

How to Configure to detect Caller-ID on Analog FXO Voice Port

When a call is incoming through analog FXO, FXO can detect Caller-ID information if CO or PBX provides Caller-ID service. The Caller-ID standard should be different by country. Also, it should be different by CO exchange type even in same country. So, you must configure FXO voice-port suitably with the Caller-ID standard of your region. There are several cases for it.

- Incoming Caller-ID after 1st Ring

This is Bellcore standard and most used standard worldwide. In this case, Caller-ID is coming between 1st Ring and 2nd Ring.

Step	Command	Purpose
1	configure terminal	Enters global configuration mode.
2	voice-port <i>slot/subslot/port</i>	Enter voice port Configuration Mode
3	shutdown	Change status of voice port to shutdown
4	caller-id enable type1	Enable caller-id on this port
5	caller-id type fsk	use fsk type for caller-id
6	ring number 2	Answering the call after 2 nd ring.
7	no shutdown	Change shutdown Status of voice-port to in-Service

- Incoming caller-Id after Line Reversal signal, before 1st Ring
This is used in some country of Europe. In this case, Caller-ID is coming between Line Reversal signal and 1st Ring.

Step	Command	Purpose
1	configure terminal	Enters global configuration mode.
2	voice-port <i>slot/subslot/port</i>	Enter voice port Configuration Mode
3	shutdown	Change status of voice port to shutdown
4	caller-id enable type1	Enable caller-id on this port
5	caller-id type fsk	use fsk type for caller-id
6	caller-id alerting dsp-pre-alloc	At the receiving end of a line-reversal alerting Caller-ID call, pre-allocates DSPs for caller ID calls.
7	no shutdown	Change shutdown Status of voice-port to in-Service

- Incoming Caller-ID after Line Reversal and off-hook
This is used in some regions of China. In this case, Caller-ID comes when FXO goes off-hook after the Line Reversal signal.

Step	Command	Purpose
1	configure terminal	Enters global configuration mode.
2	voice-port <i>slot/subslot/port</i>	Enter voice port Configuration Mode
3	shutdown	Change status of voice port to shutdown
4	caller-id enable type1	Enable caller-id on this port
5	caller-id type dtmf	use dtmf type for caller-id
6	caller-id alerting dsp-pre-alloc	At the receiving end of a line-reversal alerting Caller-ID call, pre-allocates DSPs for caller ID calls.
7	caller-id alerting line-reversal-hook	Hook on and off by a line-reversal signal to receive caller id information for on-hook (Type 1) Caller ID
8	no shutdown	Change shutdown Status of voice-port to in-Service

- Incoming Caller-ID without alerting signal before 1st Ring
This is used in some regions of India. In this case, caller-ID comes before 1st Ring without alert signal.

Step	Command	Purpose
1	configure terminal	Enters global configuration mode.
2	voice-port <i>slot/subslot/port</i>	Enter voice port Configuration Mode
3	shutdown	Change status of voice port to shutdown
4	caller-id enable type1	Enable caller-id on this port
5	caller-id type dtmf	use dtmf type for caller-id
6	caller-id alerting ring 0	for caller ID without alerting signal
7	no shutdown	Change shutdown Status of voice-port to in-Service

Configuring Analog E & M Voice Port

This section describes the configuration of the analog E & M voice port.

How to Configure Analog E & M Voice Port

Unlike FXO, FXS, E & M voice port is not enough to send voice data as a default value, the set up values of the E & M voice port should be sure to be matched with the features of the interworked PBX unit.

Two-wire or Four-wire Jumper Setting

A user should set up a Cabling scheme appropriate to the Analog E & M voice port of Ubigate iBG in Jumper setting.

2-wire		4-wire		E&M Type	J6/J7	J4/J5
PIN Number	Signal	PIN Number	Signal	Type 1	3-4	2-3
1	SB	1	SB	Type 2	1-2	1-2
2	M	2	M	Type 3	1-2, 3-4	1-2
3	-	3	RING	Type 5	3-4	2-3
4	RING	4	RING 1			
5	TIP	5	TIP 1	E&M	J1/J2 (CH0)	J11/J12 (CH1)
6	-	6	TIP	2-wire	1-2	1-2
7	E	7	E	4-wire	2-3	2-3
8	SG	8	SG			

Figure 5.7 E & M 2-Wire, 4-Wire loop Cable Pin Map

- **E** (Ear or Earth) - Signal wire from trunking (CO) side to signaling side.
- **M** (Mouth or Magnet) - Signal wire from signaling side to trunking (CO) side.
- **SG** (Signal Ground) - Used on E & M Types II, III, IV
- **SB** (Signal Battery) - Used on E & M Types II, III, IV
- **TIP/RING** - T/R leads carry audio between the signaling unit and the trunking circuit. On a 2-wire audio operation circuit, this pair carries the full-duplex audio path.
- **TIP1/RING1** - Used on 4-wire audio operation circuits only. The 4-wire implementation provides separate paths for receiving and sending audio signals.

The following Figure 5.8 shows complete Jumper information for E & M Board.

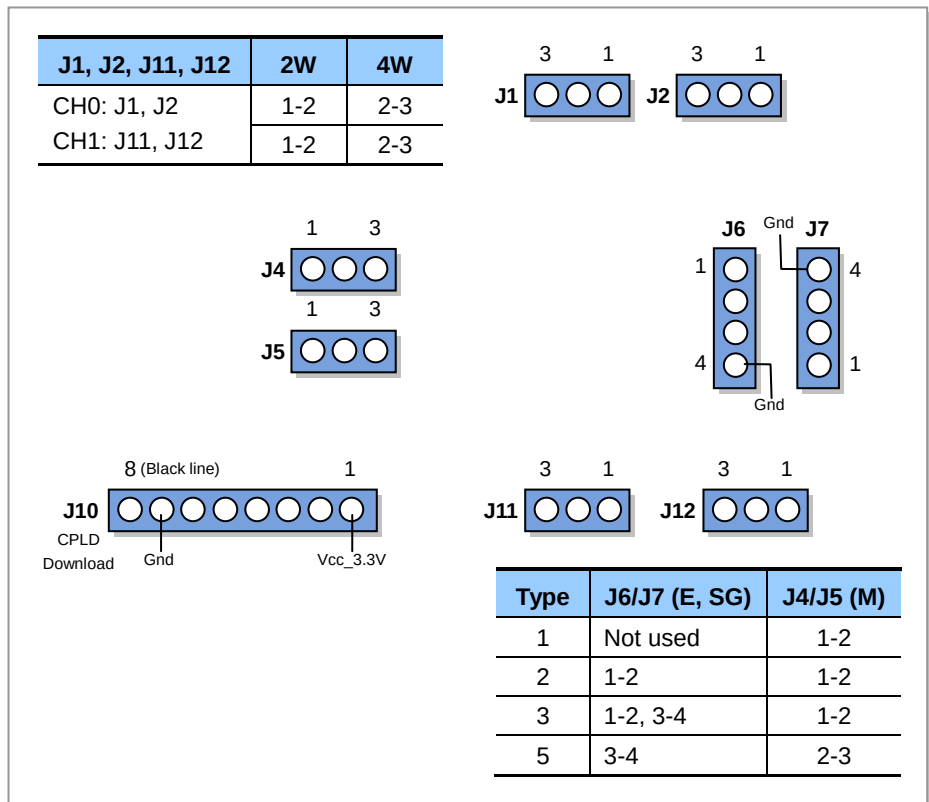


Figure 5.8 E & M Jumper Information

Type I, II, III, V

There are five different E & M interface types or models: Type I, II, III, IV, and V (Type IV is not supported). Each type has a different wiring arrangement, hence a different approach to transmitting E & M supervision signaling (on-hook/off-hook signaling). The signaling side sends its on-hook/off-hook signal over the E-lead. The trunking side sends the on-hook/off-hook over the M-lead.

• E & M Type I

This is the most common interface in North America.

Type I uses two leads for supervisor signaling: E and M. During inactivity, the E-lead is open and the M-lead is connected to the ground. The PBX Indicates the off-hook condition by connecting the M-lead to battery.

- **E & M Type II**

Two signaling nodes can be connected back-to-back. Type II uses four leads for supervision signaling: E, M, SB, and SG. During inactivity both the E-lead and M-lead are open. The PBX indicates the off-hook condition by connecting the M-lead to the signal battery (SB) lead connected to the signaling side battery.

- **E & M Type III**

Not commonly used in modern systems. Type III uses four leads for supervision signaling: E, M, SB, and SG. During inactivity, the E-lead is open and the M-lead is set to ground connected to the signaling side SG lead. The PBX indicates the off-hook condition by disconnecting the M-lead from the SG lead and connecting it to the SB lead of signaling side.

- **E & M Type IV**

Not supported by Ubigate iBG

- **E & M Type V**

Type V is symmetrical and allows two signaling nodes to be connected back-to-back. This is the most common interface type used outside of North America. Type V uses two leads for supervisor signaling: E and M. During inactivity the E-lead and M-lead are open. The PBX (acting as trunk circuit side) indicates off-hook condition by connecting the M-lead to ground.

How to Configure Analog E & M Voice Port

To set up each parameter of the basic analog E & M voice port, follow the next procedures.

- Configuration Steps
 - configure terminal
 - voice-port
 - dial-peer voice pots
 - exit
- Detailed Steps

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters global configuration mode.
2	voice-port slot/subslot/port	Enter voice port Configuration Mode. slot - Specifies the number of the router slot where the voice module is installed. subslot - Specifies the number of subslots in the slot. port - Indicates the voice port.
3	shutdown	Change status of voice port to shutdown.
4	signal { <i>wink-start</i> <i>immediate-start</i> <i>delay-dial</i> }	This command enables Direct Inward Dialing on the voice port immediate - if the voice port must use the immediate start protocol. wink-start - if the voice port must use the wink-start protocol. delay-dial - if the voice port must use the delay start protocol.
5	operation { <i>2-wire</i> <i>4-wire</i> }	Specifies the number of wires used for voice transmission at this interface (the audio path only, not the signaling path).
6	dial-type { <i>dtmf</i> <i>mf</i> }	Specifies the dialing method for outgoing calls.
7	locale <i>locale</i>	Selects the two-letter locale for the voice call progress tones and other locale-specific parameters to be used on this voice port. The Default is us ex) locale us.

(Continued)

Step	Command	Purpose
8	<i>timing {wait-wink wink-wait wink-duration delay-duration delay-start } timing-value</i>	To change timing parameters. wait-wink - Specifies maximum amount of time to wait wink for Outbound Call. wink-wait - Specifies maximum wink-wait duration, in milliseconds, for a wink-start signal. Valid entries are from 100 to 5000. The Default is 200. wink-duration - Specifies maximum wink-signal duration, in milliseconds, for a wink-start signal. delay-duration - Specifies the delay signal duration for delay-dial signaling in milliseconds. Valid entries are from 100 to 5000. The default is 2000. delay-start - Specifies minimum delay time, in milliseconds, from outgoing seizure to outdial address. Valid entries are from 20 to 2000. The default is 300.
9	<i>timeouts timer-name timer-value</i>	To change timeouts parameters initial - Sets the number of seconds that the system waits between the caller input of the initial digit and the subsequent digit of the dialed string. A valid entry is from 0 to 120. The default is 10. interdigit - Configures the number of seconds that the system waits after the caller has input the initial digit or a subsequent digit of the dialed string. If the timeout ends before the Destination is identified, a tone sounds and the call ends. This value is important when using variable-length dial peer destination patterns (dial plans). The <i>seconds</i> argument is the interdigit timeout wait time in seconds. A valid entry is an integer from 0 to 120. The default is 5. ringing - Specifies the duration that the voice port allows ringing to continue if a call is not answered. The range is from 0 to 60000. The default is 180. 0 means infinity. wait-release - Specifies the duration that a voice port stays in the call-failure state while the device sends a busy tone, reorder tone, or an out-of-service tone to the port. The range is from 0 to 3600. The default is 30. 0 means infinity.

(Continued)

Step	Command	Purpose
10	no shutdown	Change shutdown Status of voice-port to in-Service.
11	exit	Exits voice port configuration mode.
12	dial-peer voice {pots voip} <i>tag</i> Example) /configure# dial-peer voice pots 11	Enters dial-peer configuration mode and defines a local dial peer that connects to a POTS interface. The <i>number</i> argument is one or more digits identifying the dial peer. Valid entries are from 1 to 10000. The pots keyword indicates a dial peer using basic telephone service.
13	destination-pattern <i>WORD</i> Example) /configure# voice-port> destination-pattern 1004	Setting Destination-pattern Matches dialed digits to a telephony device. The <i>string</i> argument is a series of digits that specify the E.164 or private dialing plan telephone number. Valid entries are the numbers 0 through 9 and the letters A through D. You can also enter the following special characters: - The asterisk(*) or pound sign (#) on standard touch-tone dial pads can be used anywhere in the pattern. - The period(.) acts as a wildcard character. When the timer(T) character is included at the end of the destination pattern, the router collects dialed digits until the interdigit timer expires (5 seconds, by default) or until you dial the termination character (the default is #). The timer character must be a capital T.
14	port <i>slot/subslot/port</i>	Maps the dial peer to a specific Port Number.
15	exit	Exits voice dial-peer configuration mode.

Configuring Analog DID

This section describes the configuration of the analog DID Feature.

DID Feature Overview

This section describes the analog DID Feature Direct Inward Dialing (DID), which is the service proposed by Telephone service providers. This service allows a caller to dial to the PBX extension without help of an attendant. The DID Feature enables every extension of a PBX to work as if every extension is connected directly to PSTN.

Start Signal

- Immediate Start
The originating end seizes the line by going off hook and, without waiting for a response, it begins to output digits. The address signaling used with immediate-start signaling consists only of dial-pulsing.
- Wink-Start
The originating end seizes the line by going off-hook. It waits for acknowledgment from the other end before outputting digits. This serves as an integrity check that will identify a malfunctioning trunk and allow the network to send a re-order tone to the calling party.
- Delay Dial
The originating end seizes the line and waits 200 ms to see if the far end is on-hook. If so, the originating end then outputs digits. If the far end is off-hook, the originating end waits until the far end is on-hook before outputting digits.

Restrictions of DID Trunk

- Dial Tone is not present.
- Outgoing Calls are not allowed. If an outgoing call is attempted, the caller will get a fast busy signal.

How to Configure Analog DID

To set up each parameter of the basic analog voice port, follow these procedures:

- Configuration Steps
 - configure terminal
 - voice-port
 - dial-peer voice pots
 - exit
- Detailed Steps

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters global configuration mode.
2	voice-port <i>slot/subslot/port</i>	Enters voice port Configuration Mode. slot - Specifies the number of the router slot where the voice module in installed. subslot - Specifies the number of subslots in the slot. port - Indicates the voice port.
3	shutdown	Changes status of the voice port to shutdown.
4	signal did { <i>immediate</i> <i>wink-start</i> <i>delay-dial</i> }	This command enables Direct Inward Dialing on the voice port. immediate - if the voice port must use the immediate start protocol. wink-start - if the voice port must use the wink-start protocol. delay-dial - if the voice port must use the delay start protocol.
5	locale <i>locale</i>	Selects the two-letter locale for the voice call progress tones and other locale-specific parameters to be used on this voice port. The Default is us ex) locale us

(Continued)

Step	Command	Purpose
6	timeouts <i>timer-name timer-value</i>	To change timeouts parameters initial - Sets the number of seconds that the system waits between the caller input of the initial digit and the subsequent digit of the dialed string. A valid entry is from 0 to 120. The default is 10. interdigit - Configures the number of seconds that the system waits after the caller has input the initial digit or a subsequent digit of the dialed string. If the timeout ends before the Destination is identified, a tone sounds and the call ends. This value is important when using the variable-length dial peer destination patterns (dial plans). The <i>seconds</i> argument is the interdigit timeout wait time in seconds. A valid entry is an integer from 0 to 120. The default is 5. ringing - Specifies the duration that the voice port allows ringing to continue if a call is not answered. The range is from 0 to 60000. The default is 180. 0 means infinity. wait-release - Specifies the duration that a voice port stays in the call-failure state while the device sends a busy tone, reorder tone, or an out-of-service tone to the port. The range is from 0 to 3600. The default is 30. 0 means infinity.
7	timing wink-wait <i>timer-value</i>	Sets the maximum time to wait before sending wink signal after an incoming seizure is detected.
8	timing wink-duration <i>timer-value</i>	Sets the duration of a wink-start signal.

(Continued)

Step	Command	Purpose
9	timing delay-duration <i>timer-value</i>	Sets the duration of a delay signal.
10	timing delay-start <i>timer-value</i>	Sets the delay interval after an incoming seizure is detected.
11	no shutdown	Changes shutdown Status of voice-port to in-Service.

Configuring E911 CAMA

This section describes Voice-grade Enhanced 911 Switched Access function. CAMA of Ubigate iBG is connected to PSAP using Analog FXO Line.

E911 CAMA Feature Overview

The North American emergency E911 phone system consists of a voice network that is built largely outside of the normal public switched telephone network (PSTN) on which common voice traffic rides. It is treated especially because they are routed differently within the PSTN than normal traffic. Calls to emergency services are routed based on the calling number, not the called number. The calling number is checked against a database of emergency service providers that cross-references the service providers for the caller's particular location. When this information is known, the call is then routed to the proper public service answering point (PSAP), which, in turn, dispatches those services for the caller's location.

CAMA is a signaling protocol that was originally designed for toll call billing purposes but has been adapted to carry a single telephone number for Enhanced 911 (E911) purposes. E911 is an emergency telephone system capable of automatically displaying the callback number (and in some cases the location) of a person who dials 911 to request emergency help from public safety agencies.

For further information on E911, see ‘American National Standard T1.422-2001’.

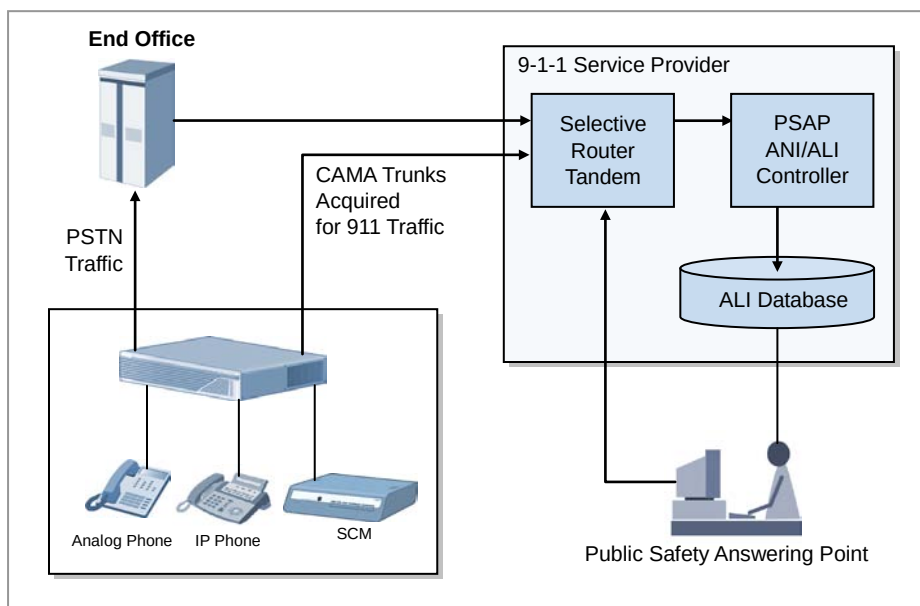


Figure 5.9 E911 Network Diagram

E911/CAMA related terminology

- ALI: Automatic Location Identification
- ANI: Automatic Number Identification
- CAMA Centralized Automatic Message Accounting
- NPA Numbering Plan Area
- NPD Numbering Plan Digit
- NRF No Record Found
- PBX Private Branch Exchange
- PSAP Public Safety Answering Point or Primary Public Safety Answering Point
- SR Selective Routing

Address information

E911 CAMA Access function should transmit Calling number for the following reasons.

1. For that PSAP is able to search the Automatic Location Identification (ALI) database using the Calling Number.
2. If an emergency call is disconnected to E911, it is because the CAMA system should be able to display the calling number or connect to the callback number.

Depending on the method that Ubigate iBG transmits ANI, the CAMA mode is divided into the following:

- KP-0-NXX-XXXX-ST - 7-digit Automatic Number Identification (ANI) transmission. The Numbering Plan Area (NPA) or area code is implied by the trunk group and is not transmitted.
- KP-0-NPA-NXX-XXXX-ST - 10-digit transmission. The E.164 number is fully transmitted.
- KP-2-ST - Default transmission when the CAMA trunk cannot obtain a corresponding Numbering Plan Digit (NPD) in the look-up table, or when the calling number is fewer than 10 digits. (NPA digits are not available.)
- KP-NPD-NXX-XXXX-ST - 8-digit ANI transmission, in which the NPD is a single multifrequency (MF) digit that is expanded into the NPA. The NPD table is preprogrammed by configuring ANI mapping in the sending and receiving equipment (on each end of the MF trunk); for example: 0= 408, 1=510, 2=650, 3=415.

Bell-South Case

The 'signal cama-bellsouth' Option is the option for the time to transmit CAMA ANI functions. General CAMA immediately transmits ANI right after transmission of KP+911+ST, whereas if the cama-bellsouth Option is applied, it transmits ANI once after reception of the off-hook.

When the PSAP receives the complete ANI information, the PSAP equipment will signal the call takers and return audible ringing to the calling PBX party. Upon answer, the PSAP will disconnect audible ringing, connect the call to the answering attendant, display the ANI at the answering position, and return an off-hook signal to the PBX indicating that the call has been answered.

```

PBX E911 SWITCH
1. SEIZE ----- (OFF-HOOK) ----->
2. <----- WINK START (140 ms TO 290 ms) ----->
3. KP 911 ST ----->
4. <-----OFF-HOOK
5. KP I NXXXXXX ST (ANI) ----->
6. <----- TALKING PATH CONNECTED ----->
   Calling party goes on-hook
7. PBX DISCONNECTS ----- (ON-HOOK) ----->
8. <----- 911 SWITCH DISCONNECTS ----- ON-HOOK

```

How to Configure CAMA

To configure the CAMA function using the analog FXO, follow these procedures:

- Configuration Steps
 - configure terminal
 - voice-port
 - dial-peer voice pots
 - exit
- Detailed Steps

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters global configuration mode.
2	voice-port <i>slot/subslot/port</i>	Enters voice port Configuration Mode. slot - Specifies the number of the router slot where the voice module is installed. subslot - Specifies the number of subslots in the slot port - Indicates the voice port.
3	shutdown	Changes voice port status to shutdown.
4	ani mapping 0-3 digits for example: ani mapping 0 415 0= 415, 1=510, 2=650, 3=916 05551234 = (415) 555-1234, 15551234 = (510) 555-1234, and so on. NPD range is from 0 to 3	To preprogram the Numbering Plan Area (NPA), or area code, into a single Multi Frequency (MF) digit.

(Continued)

Step	Command	Purpose
5	signal {groundstart loopstart} signal {cama {kp-0- nxx-xxxx-st kp-0-npa- nxx-xxxx-st kp-2-st kp-npd-nxx-xxxx-st}	Selects the access signaling type to match that of the telephony connection you are making. The keywords are as follows: loop-start - (default) Uses a closed circuit to indicate off-hook status; used for residential loops. ground-start - Uses ground and current detectors; preferred for PBXs and trunks. kp-0-npa-nxx-xxxx-st 10-digit transmission. The E.164 number is fully transmitted. kp-0-nxx-xxxx-st 7-digit automatic number identification (ANI) transmission. The Numbering Plan Area (NPA) or area code is implied by the trunk group and is not transmitted. kp-2-st Default transmission when the CAMA trunk cannot get a corresponding Numbering Plan Digit (NPD) in the look-up table, or when the calling number is fewer than 10 digits in length. (NPA digits are not available.) kp-npd-nxx-xxxx-st 8-digit ANI transmission, where the NPD is a single multifrequency (MF) digit that is expanded into the NPA. The NPD table is preprogrammed in the sending and receiving equipment (on each end of the MF trunk); for example: 0= 415, 1=510, 2=650, 3=916 05551234 = (415) 555-1234, 15551234 = (510) 555-1234, and so on. NPD range is from 0 to 3.
8	signal cama-bellsouth	apply Bell South E911 Case.
9	locale <i>locale</i>	Selects the two-letter locale for the voice call progress tones and other locale-specific parameters to be used on this voice port. The Default is us ex) locale us

(Continued)

Step	Command	Purpose
10	timeouts <i>timer-name</i> <i>timer-value</i>	To change timeouts parameters initial - Sets the number of seconds that the system waits between the caller input of the initial digit and the subsequent digit of the dialed string. A valid entry is from 0 to 120. The default is 10. interdigit - Configures the number of seconds that the system waits after the caller has input the initial digit or a subsequent digit of the dialed string. If the timeout ends before the Destination is identified, a tone sounds and the call ends. This value is important when using variable-length dial peer destination patterns (dial plans). The <i>seconds</i> argument is the interdigit timeout wait time in seconds. A valid entry is an integer from 0 to 120. The default is 5. ringing - Specifies the duration that the voice port allows ringing to continue if a call is not answered. The range is from 5 to 60000. The default is 180. wait-release - Specifies the duration that a voice port stays in the call-failure state while the device sends a busy tone, reorder tone, or an out-of-service tone to the port. The range is from 3 to 3600. The default is 30.
11	timing digit <i>timer-value</i>	specifies the DTMF digit signal duration.
12	timing guard-out <i>timer-value</i>	(FXO ports only) specifies the duration in milliseconds of the guard-out period that prevents this remote port from detecting a disconnect signal.
13	no shutdown	Changes shutdown Status of voice-port to in-Service.
14	exit	Exits voice port configuration mode.
15	dial-peer voice {pots voip} <i>tag</i> Example) /configure# dial-peer voice pots 11	Enters dial-peer configuration mode and defines a local dial peer that connects to a POTS interface. The <i>number</i> argument is one or more digits identifying the dial peer. Valid entries are from 1 to 10000. The pots keyword indicates a dial peer using basic telephone service.

(Continued)

Step	Command	Purpose
16	destination-pattern WORD Example) /configure# voice- port> destination- pattern 1004	Setting Destination-pattern Matches dialed digits to a telephony device. The <i>string</i> argument is a series of digits that specify the E.164 or private dialing plan telephone number. Valid entries are the numbers 0 through 9 and the letters A through D. You can also enter the following special characters: - The asterisk(*) or pound sign(#) on standard touch-tone dial pads can be used anywhere in the pattern. - The period(.) acts as a wildcard character. When the timer(T) character is included at the end of the destination pattern, the router collects dialed digits until the interdigit timer expires (5 seconds, by default) or until you dial the termination character (the default is #). The timer character must be a capital T.
17	port slot/subslot/port	Maps the dial peer to a specific Port Number.
18	exit	Exits voice dial-peer configuration mode.



This page is intentionally left blank.



CHAPTER 6. Digital Voice Port

This chapter describes the digital voice port Features. The digital voice port commands discussed in this section configure channelized T1 or E1 connections.

- Digital Trunk E1-R2 Features
- Digital Trunk T1-CAS Features

Digital Trunk E1-R2 Features

E1-R2 signaling is a generally used international signaling standard for PSTN E1 trunk. A detailed specification for R2 signaling is included in ITU-T Q.400 to Q.490.

Digital E1 Trunk

E1 trunk working in TDM method has 32 timeslots (each timeslot is called DS0). One of R2 signaling working in the E1 digital trunk is used as frame synchronization of the E1 trunk, and the other one is used for signal transmission for R2 signaling. The remaining 30 timeslots are used to carry a voice in a PCM mode.

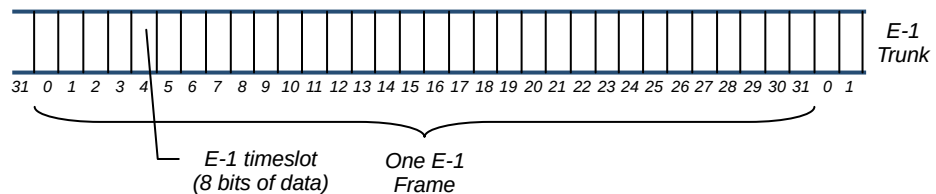


Figure 6.1 an E1 frame

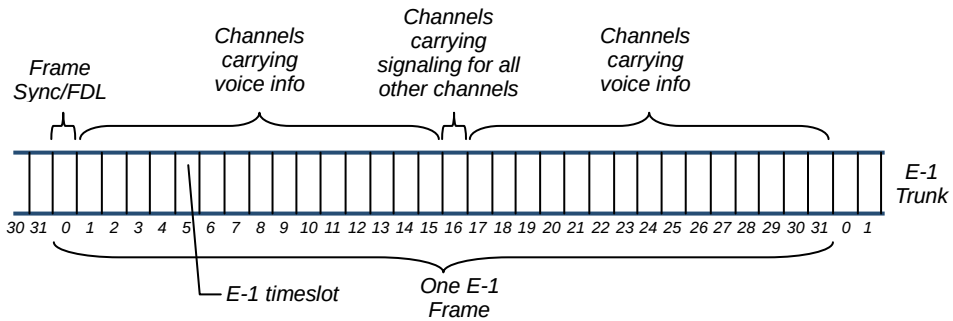


Figure 6.2 E1 timeslots for R2 signaling

Trunk Information Management

Requirements

Prerequisites

Before you attempt this configuration, ensure that you meet these prerequisites:

- R2 signaling applies to E1 only
- In order to run R2 signaling on the SBM routers, these hardwares are required:
 - WTE-2M or WTE-4
- Define the command **cas-ds0-group** on the E1 trunk (module) to create ds0-group.
- Use the **voice-port** and **cas-custom** command in order to customize the E1-R2 variants for different countries or regions.

Configuration Steps

- Complete physical layer of E1 trunk settings.
- Create ds0-groups to manage the DS0 channels on the E1 trunk.
- Configure ds0-group with sub-commands such as 'timeslots' and 'signal cas'.
- Customize country variants in 'cas-custom' configuration mode.
- Configure basic voice port parameters in 'voice-port' configuration mode.

Network Diagram

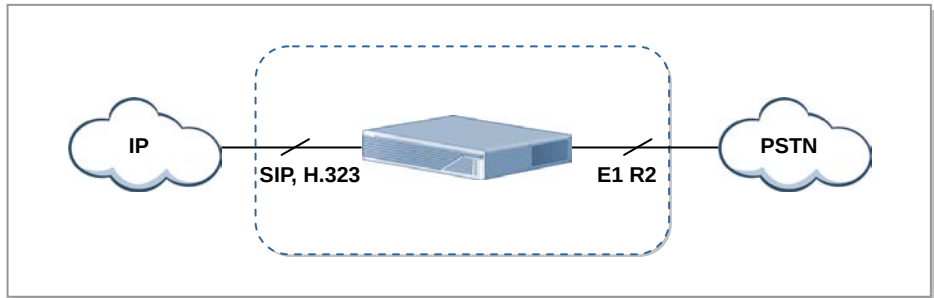


Figure 6.3 E1-R2 Network Diagram

Configure E1 Trunk

This section shows the process of configuring physical layers of the E1 trunk.

Configuring E1 Trunk Settings

To make an E1 connection with a neighboring equipment interworking on the PSTN, the configuration should be set up to a characteristic specific to the E1 trunk line. Such configuration is made typically in **module** configuration mode.

To configure E1-R2, do the following steps:

1. Set up the E1 trunk that connects to the private automatic branch exchange (PBX) or switch.
2. Ensure that the framing and linecoding of the E1 are properly set.
3. For E1 framing, choose either **CRC** or **non-CRC**.
4. For E1 linecoding, choose either **HDB3** or **AMI**.
5. For the E1 clock source, choose either **internal** or **line**. Keep in mind that different PBXs have different requirements on the clock source. Configuration of the clock source is only used in module command.
6. Configure line signaling and interregister signaling for R2.
7. Customize the configuration with the **cas-custom** command.

Step	Command	Purpose
1	show voice card all	List all the voice cards installed in the system. If you find any of the WTE_XX cards you can choose the one to use an E1 trunks card. <pre> v239# show voice card all SLOT CARD TYPE STATUS VS VSL0TNAME [DSP] VoIP_ M510 NORMAL 13 VoIP_VSL0T [0/0] FXS_ 4M NORMAL 7 MM_2_VSL0T [0/1] WTE_ 2M NORMAL 6 MM_1_VSL0T [0/2] - - -- [1/0] - - -- [1/1] - - -- [2/0] - - -- [2/1] - - -- </pre>
2	show module configuration all	Displays all the digital trunk active in the system. So if you use this command it helps you to recognize the carrier-types of the trunks installed in the system. <pre> v239# show module configuration all E1 # Framing Coding ClkSrc LB0-CableLength State Alarm ----- ----- 0/1/1 crc hdb3 int long haul up N/A 0/1/0 crc hdb3 int long haul up N/A </pre>
3	configure terminal	Enters the global configuration mode to advance the E1 setting.

(Continued)

Step	Command	Purpose
4	system carrier-type slot # e1	Input the <i>slot#</i> which is qualified to be E1 trunk card. And if the previous carrier-type of the slot is configured as E1, rebooting is not required. Otherwise the system will prompt you to reboot the system for the change to take effect. <pre> v239/configure# system carrier-type 0/1 e1 E1 carrier set for slot 0/1 You need to REBOOT for the change to take effect. v239/configure# exit v239# reboot WARNING: Configuration changes not yet saved! Continue with reboot ?(y/n): y </pre>
5	configure terminal	-
6	module e1 trunk#	Specifies the E1 trunk that you want to use to configure physical layer settings. <i>trunk#</i> is a simple notation of <i>slot/sub-slot/port</i>, for convenience.
7	clock_source { internal line }	Configures the clock source. line-Specifies that the clock-facility on this port derives clocking from the external source to which the port is connected (generally the CO). internal - (Optional) Specifies that the clock is generated from the voice card's internal clock-facility.
8	framing {crc non_crc disable }	Selects frame type for T1 or E1 line. crc-Provides 4 bits of error protection. non_crc-Disables crc4. disable-Disables E1 framer.
9	linecode	Specifies the line encoding to use. The keywords are as follows: ami-Specifies the alternate mark inversion (AMI) line code type. (T1 and E1). hdb3-Specifies the high-density bipolar 3 (HDB3) line code type. (E1 only).

(Continued)

Step	Command	Purpose
10	exit	Exits to the global configuration mode. Keep in mind that no shutdown is necessary as the settings are applied instantly.
11	show module configuration e1 trunk#	Check out the status of the specified trunks and the sanity. <i>trunk#</i> is a simple notation of <i>slot/sub-slot/port</i> , for convenience.

Create Logical Voice Port on Digital E1 Trunks

Understanding DS0 Group

The terminology necessary to understand the DS0 Group is as follows:

- Digital Trunk: Means T1/E1 trunk working as a physical layer.
- Voice Port: doesn't mean simply PSTN I/F, but means a functional entity responsible for the function to provide VoIP services at the border area between PSTN and Packet Network.
- Digital Voice Port: means a digital PSTN interface, as an entity to provide VoIP service having implications on the digital trunk and voice port at the same time.
- DS0 Group: is a logical voice port configurable in the digital voice port, consisting of one or more DS0-channels.
- Logical voice port: is used with the same meaning as the DS0 group. It is a logical unit that can exist in multiple units in the digital voice port of the E1/T1 unit, each logical voice port is able to work with its own property. In summary, the logical voice port is a multi-phased abstract unit having both signaling and voice properties in the PSTN at the same time.

Properties that can be set up in the voice port are very variable, and closely involved with the dial peer. Especially for a part of the media features, the logical voice port may be set up in the dial peer in order to reflect the feature of the packet network in view of a call connection, or reflect the factors determined in the course of the call progress. The following properties may be set up for a media.

- Fax setup works in a setup negotiated in the course of the call connection with IP terminal.
- Packet delay control: controls the delay buffer of the voice packet by the delay control policy set up in the dial peer. Its relationship is made up of the voice port and dial peer pair which is determined in a call unit.

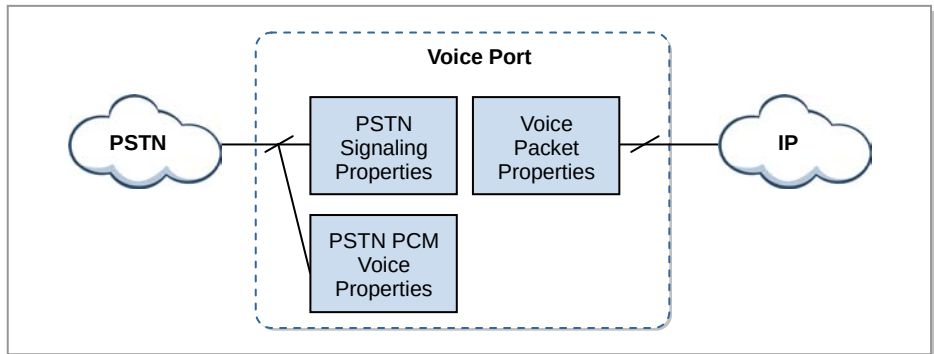


Figure 6.4 Conceptual view of voice port

DS0 group is a concept of a logical voice port controllable in a system by combining several DS0 channels in a digital trunk.

E1 has 30 DS0 channels, it can make a logical digital voice port using the **cas-ds0-group** command. This bundle of channels are referred to as DS0. This created DS0 group can set up specific properties via the **voice-port** command.

Here is the visual depiction of DS0 groups on a digital trunk:

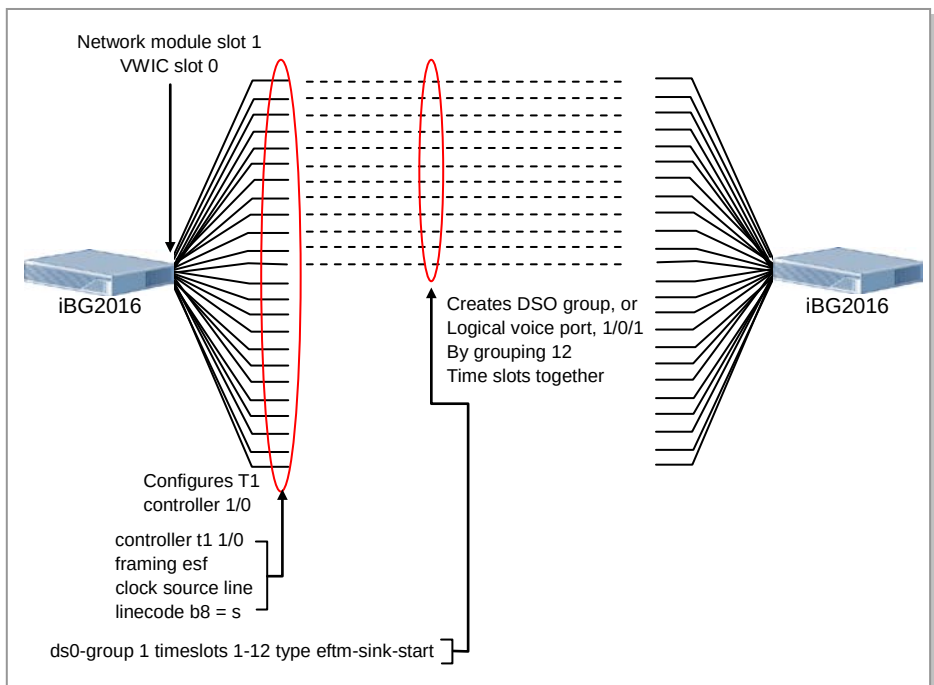


Figure 6.5 DS0 groups on a digital voice port

Creating DS0 Groups on E1 Trunk

To create DS0 groups and a logical voice port in the digital trunk, just use the `cas-ds0 group` command.

The numbering for the logical voice port created as a result of this command is *trunk-id:ds0-group-no*, where *trunk-id* is defined as the platform-specific address for a particular trunk. Usually the *trunk-id* is expanded to *slot/sub-slot/port*.

For example, 'cas-ds0-group 1' automatically creates the voice port 0/1/0:1 when issued in the configuration mode for module 0/1/0.

To map individual DS0s, define additional DS0 groups under the E1 trunk, specifying different time slots. Defining additional DS0 groups also creates individual DS0 voice ports.

Step	Command	Purpose
1	configure terminal	Assumes the trunk becomes normal and active according to the steps above. Here the description starts with configuring R2 signaling to the trunk.
2	module e1 trunk#	Enters the module configuration mode.
3	cas-ds0-group ds0-group-no	Enters the ds0-group number to create it in this E1 trunk.
4	exit	Exits module configuration mode.
5	show voice port summary	Checks if ds0-group is created normally. The DS0-group created in the system is indicated in the form of <i>slot/sub-slot/port:ds0-group-no</i> .

v239# show voice port summary								
PORT	CH	SIG-TYPE	ADMIN	OPER	IN STATUS	OUT STATUS	EC	
=====	==	=====	=====	=====	=====	=====	==	
0/0/0	--	fxs-ls	up	up	on-hook	idle	y	
0/0/1	--	fxs-ls	up	up	on-hook	idle	y	
0/0/2	--	fxs-ls	up	up	on-hook	idle	y	
0/0/3	--	fxs-ls	up	up	on-hook	idle	y	
0/1/0:10	--	---	down	--	----	----	y	

Configure R2 on DS0 group

R2 Signaling

R2 signaling is the channelized E1 signaling used in Europe, Asia, and South America. It is equivalent to the channelized T1 signaling in North America. There are two types of R2 signaling: line signaling and interregister signaling. R2 line signaling includes R2 digital. R2 interregister signaling includes R2 compelled, R2 DTMF. These signaling types are configured using the '**signal cas**' command in the **voice-port** configuration mode.

Many countries and regions have their own E1-R2 variant specifications, which supplement the ITU-T Q.400-Q.490 recommendation for R2 signaling. Unique E1-R2 signaling parameters for specific countries and regions are set by entering the **cas-custom** channel command followed by the country name command.

Configuring R2 Signaling

Step	Command	Purpose
1	configure terminal	Enters the global configuration mode.
2	voice-port slot/sub-slot/port:ds0-group-no	Enters the module configuration mode.
3	Shutdown	Shuts down the voice port for further configuration.
4	timeslots timeslot-list	timeslots-Specifies the single time slot number, single range of numbers, or multiple ranges of numbers separated by commas. For E1, allowable values are from 1 to 31. Examples are as follows: -2, 3-5 -1, 7, 9 -1-12
5	signal cas { r2-mfc r2-dtmf } [ani]	Determines the type of R2 signaling. if it is set up as an any-optional entity, it transmits ANI.
6	no shutdown	Activates the appropriate voice port to reflect the subject matter set up.
7	show voice port summary	Checks out if the ds0-group was created normally. The created ds0-group is displayed in the form of <i>slot/sub-slot/port:ds0-group-no</i> .

```
v239# show voice port sum
```

PORT	CH	SIG-TYPE	ADMIN	OPER	IN STATUS	OUT STATUS	EC
=====	==	=====	=====	=====	=====	=====	==
0/0/0	--	fxs-ls	up	up	on-hook	idle	y
0/0/1	--	fxs-ls	up	up	on-hook	idle	y
0/0/2	--	fxs-ls	up	up	on-hook	idle	y
0/0/3	--	fxs-ls	up	up	on-hook	idle	y
0/1/0:10	01	r2-mfc	up	up	idle	idle	y
0/1/0:10	02	r2-mfc	up	up	idle	idle	y
0/1/0:10	03	r2-mfc	up	up	idle	idle	y
0/1/0:10	04	r2-mfc	up	up	idle	idle	y
0/1/0:10	05	r2-mfc	up	up	idle	idle	y
0/1/0:10	06	r2-mfc	up	up	idle	idle	y
0/1/0:10	07	r2-mfc	up	up	idle	idle	y
0/1/0:10	08	r2-mfc	up	up	idle	idle	y
0/1/0:10	09	r2-mfc	up	up	idle	idle	y
0/1/0:10	10	r2-mfc	up	up	idle	idle	y

Trunk Status Monitoring

The next sub chapter addresses digital trunk status and information configured in the trunk. We will check the following subject in detail:

- check if the configured digital trunk works normally.
- check if the logical voice ports configured in digital trunk are configured normally.
- check if the configuration information of DS0 group, logical voice port are set up correctly from the detailed configuration information.

Physical Layer Status

Checks all the voice cards set up in the system by using show voice card all.

```
v239# show voice card all
```

SLOT	CARD	TYPE	STATUS	VS	VSLOTNAME
[DSP]	VoIP_M510		NORMAL	13	VoIP_VSL0T
[0/0]	FXS_4M		NORMAL	7	MM_2_VSL0T
[0/1]	WTE_2M		NORMAL	6	MM_1_VSL0T
[0/2]	-		-	--	
[1/0]	-		-	--	
[1/1]	-		-	--	
[2/0]	-		-	--	
[2/1]	-		-	--	

By using show module configuration, it is possible to check if the carrier type of the trunk is working.

```
v239# show module configuration t1 0/1/0
T1 0/1/0 is ENABLED
Alarm Hierarchy: TRUE,
Yellow Alarm: DISABLE
Framing:ESF, LineCode:B8ZS, ClockSource: INT, LineMode:CSU,
LB0:0 db
FDL: ANSI Unit Protocol enabled ,ATT Unit Protocol
disabled ,
CsuDsuType: CSU , Loopback Framing(In-band): Overwrite,
CIRCUIT-ID: Not Configured ,CONTACT-INFO: Not Configured ,
DESCRIPTION: Not Configured , LINK NAME: Not Configured ,

Line Status:
  RLOS:OFF   RAIS:OFF   RLOF:OFF   RRAI:OFF   TAIS:OFF
  TRAI:OFF   TPtrn:OFF   Loop:OFF

Timeslot Map:
1  2  3  4  5  6  7  8  9 10 11 12 13 14 15 16 17 18 19 20 21
22 23 24

_____

|0 |0 |0 |0 |0 |0 |0 |0 |0 |0 |0 |0 |0 |0 |0 |0 |0 |0 |0 |
|0 |0 |0 |0 |
|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|
|_|_|_|_|_|
```

```
v239# show module configuration all

T1 # Framing Coding ClkSrc LB0-CableLength State Alarm
-----
0/1/1 esf b8zs int csu/0db up N/A
0/1/0 esf b8zs int csu/0db up N/A
```

Logical Voice Port Summary

By using show voice port summary, checks the status of the created logical voice ports (DS0 groups). It displays all voice ports created in the system containing the DS0 group.

```
v239# show voice port sum
```

PORT	CH	SIG-TYPE	ADMIN	OPER	IN STATUS	OUT STATUS	EC
=====	==	=====	=====	=====	=====	=====	==
0/0/0	--	fxs-ls	up	up	on-hook	idle	y
0/0/1	--	fxs-ls	up	up	on-hook	idle	y
0/0/2	--	fxs-ls	up	up	on-hook	idle	y
0/0/3	--	fxs-ls	up	up	on-hook	idle	y
0/1/0:10	01	r2-mfc	up	up	idle	idle	y
0/1/0:10	02	r2-mfc	up	up	idle	idle	y
0/1/0:10	03	r2-mfc	up	up	idle	idle	y
0/1/0:10	04	r2-mfc	up	up	idle	idle	y
0/1/0:10	05	r2-mfc	up	up	idle	idle	y
0/1/0:10	06	r2-mfc	up	up	idle	idle	y
0/1/0:10	07	r2-mfc	up	up	idle	idle	y
0/1/0:10	08	r2-mfc	up	up	idle	idle	y
0/1/0:10	09	r2-mfc	up	up	idle	idle	y
0/1/0:10	10	r2-mfc	up	up	idle	idle	y

- **PORT**
Presents the logical voice ports created in the analog voice port and digital voice port by using the geographical location presentation method.
Form of slot/sub-slot/port: analog voice card such as analog FXS, analog FXO, analog E & M, ISDN BRI.
Form of slot/sub-slot/port:ds0-group-no: shows ds0-groups created in the digital voice port and ds0-channels that belong to the appropriate ds0-groups.
- **SIG-TYPE**
Indicates signaling type set up in ds0-group or analog voice port.
- **ADMIN**
Up/down: indicates the status of the voice port in accordance with the operator's control. This appears as 'down' when an operator executes the shutdown command in voice port configuration mode, but 'up' when executing 'no shutdown'.

- OPER

Indicates status changes while voice port or DS0 channel works.

This appears as 'up' in the case that the voice port or DS0 channel is normally in service, and as 'down' while the voice port is out of service due to voice card failure.

It is indicated as 'block' when blocked by an operator, or a channel is not available when it signals.

- IN STATUS

Indicates status changes when the analog voice port or DS0 channel handles a call.

At this time, call state is indicated differently according to the signaling method in each SIG-Type analog of voice port or DS0 channel.

It may be 'idle', 'ringing', 'off-hook', 'out_of_svc', 'busy', 'seized', 'answered' etc.

- OUT STATUS

Indicates status changes when the analog voice port or DS0 channel handles a call.

At this time, call state is indicated differently according to the signaling method in each SIG-Type analog voice port or DS0 channel.

It may be 'idle', 'ringing', 'off-hook', 'out_of_svc', 'busy', 'seized', 'answered' etc.

- EC

Indicates the echo cancellation function set up in analog voice port or DS0 is working.

Logical Voice Port In Detail

Displays the concrete setup values of the parameters used in a specific voice port.

```
v239# show voice port 0/1/0:10
Voice Port protocol is DS0_SIG_R2_compelled
Description is not set
Noise Regeneration is enable
Echo Cancellation is enable
Echo Cancel Coverage is 48ms
Echo Non Linear Processing is disable
Input Gain is set to 0 dB
Output Attenuation is set to 0 dB
```

```
Playout-delay Mode is set to DjbmMode_Static
Playout-delay Nominal is set to 40ms
Playout-delay Maximum is set to 200ms
Playout-delay Minimum is set to 20ms
Translation Rule for Calling is set to none
Translation Rule for Called is set to none
Translation Profile for Incoming is set to NULL
Translation Profile for Outgoing is set to NULL
Trunk Group is set to NULL
ANI request is set to on
CAS Custom Country is itu
CAS-custom ANI min digits is set to 0
CAS-custom ANI max digits is set to 0
CAS-custom answer signal group is set to 2
CAS-custom answer signal is set to 6
CAS-custom caller digits are set to 1
CAS-custom debounce time is set to 40
CAS-custom invert ABCD is set to 0
CAS-custom signal KA is set to 0
CAS-custom signal KD is set to 0
CAS-custom nc congestion is set to 4
CAS-custom request category is set to 0
CAS-custom release guard time is set to 2000
CAS-custom seize ack time is set to 100
CAS-custom ANI timeout is set to 0
CAS-custom answer guard time is set to 0
CAS-custom DNIS digit complete is set to 0
CAS-custom DNIS min digits is set to 0
CAS-custom DNIS max digits is set to 0
CAS-custom metering is set to 0
Timeout initial is set to 10
Timeout interdigit is set to 5
Timeout ringing is set to 180
Timeout wait-release is set to 30
Timing clear-wait is set to 400
Timing delay-start is set to 300
Timing delay-duration is set to 2000
Timing delay-with-integrity is set to 0
Timing wink-wait is set to 200
Timing wink-duration is set to 200
Timing wait-wink is set to 2000
Timing digit is set to 100
Timing guard-out is set to 2000
Timing hook-flash-input is set to 480
Timing hook-flash-output is set to 400
Timing percent-break is set to 50
Region Tone is set to United States
Dialing Type is set to dialType_mf
```

Trunk Voice port Management

This section describes management of logical voice ports configured in the digital E1 trunk.

- create a DS0 group
- delete a DS0 group
- configure DS0 group

Create Trunk Voice Port

Logically combines DS0 channels in a digital trunk to manage ds0 group. The following describes the process to create a DS0 group:

Step	Command	Purpose
1	configure terminal	Enters the global configuration mode.
2	module e1 <i>slot/sub-slot/port</i>	selects the trunk to create DS0 group.
3	cas-ds0-group ds0-group-no	ds0-group-no: Identifies the unique DS0 group (number from 0 to 23, for T1, or from 0 to 30, for E1) in a specific trunk.
4	exit	Exits the module configuration mode.
5	show voice port summary	Displays all the voice-ports configured in the system. Checks whether the ds0-group just created exists or not.

Delete Trunk Voice Port

Deletes the DS0 group created in a specific digital trunk.

The following describes the process to delete a DS0 group:

Step	Command	Purpose
1	configure terminal	Enters the global configuration mode.
2	module e1 <i>slot/sub-slot/port</i>	Selects the DS0 group trunk to delete..
3	no cas-ds0-group ds0-group-no	ds0-group-no: Identifies the unique DS0 group (number from 0 to 23, for T1, or from 0 to 30, for E1) in a specific trunk.
4	exit	Exits the module configuration mode.
5	show voice port summary	Displays all the voice-ports configured in the system. Checks whether the ds0-group just deleted is still remaining or not.

Configure Basic Parameters

Enables interworking with PSTN or PBX which is directly connected to the voice port by using some DS0 group setup functions configured in digital trunk. Mostly, to start the voice port function with a minimum setup, each command is initialized to a default value when a voice port is created.

In order to support further setup, it supports advanced configuration function.

Step	Command	Purpose
1	configure terminal	Enters the global configuration mode.
2	voice-port slot/sub-slot/port:ds0-group-no	Enters the module configuration mode.
3	locale locale	Selects a two-letter country name defined in the voice-port mode. It decides call progress tone parameters and other locale-specific parameters.
4	compand-type { u-law a-law }	Specifies companding standard used. Even though the set up values are different from each other, a conversion is made by the internal TDM switch.
5	description	(optional) a representative ID set up in this voice-port, names text string.
6	exit	Exits the voice-port configuration mode.
7	show voice port slot/sub-slot/port:ds0-group-no	Checks if the values set in the voice port are set up normally.

Configure Advanced Parameters

Is able to tune signaling specific setup or voice quality setup using advanced configuration.

Since the signaling specific parameters on E1-R2 are set up via CAS customizing, this section describes voice quality tuning.

Echo Adjustment

The most prevalent cause of echo in PSTN is impedance mismatches within the hybrid where 4-wire phone circuits are converted to 2-wire circuits. This electrically generated echo occurs when the incoming energy from the far end speaker is reflected back toward the speaker as a slightly altered and delayed replication due to impedance mismatch in the hybrid (Figure 6.6).

The presence of an echo occurs whenever the replicated signal delay exceeds 10 ms, and becomes apparent to the speaker as reflected voice when the delay exceeds as little as 16 ms. It is manifested to the far end as an altered replica of the speaker original. If the echo interval exceeds approximately 25 milliseconds, it is distracting. In order to combat the echo phenomenon, an echo canceller is employed.

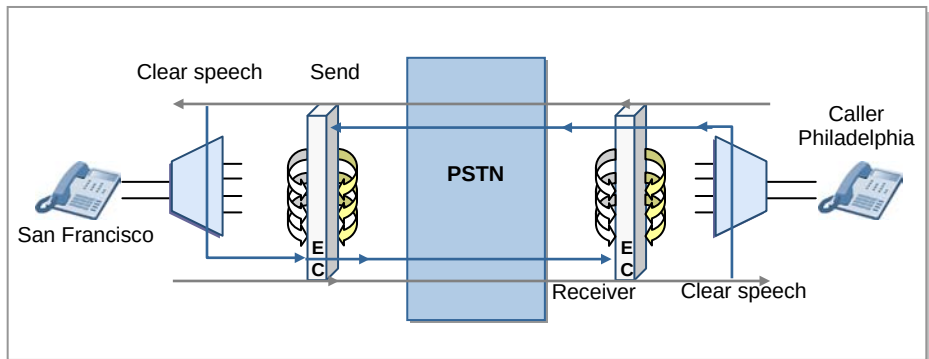


Figure 6.6 Echo problem

Step	Command	Purpose
1	configure terminal	Enters the global configuration mode.
2	voice-port slot/sub-slot/port:ds0-group-no	Enters the module configuration mode.
3	echo-cancel enable	Enables echo cancellation on this voice port. Echo cancellation works on the echo cancellation coverage which is configured by user or as default.
4	echo-cancel coverage { 8 16 ... 128 }	Chooses the echo tail length (echo cancel coverage) to which echo canceller is committed.
5	non-linear	Enables nonlinear processing (residual echo suppression) in the echo canceller.
6	exit	Exit the voice-port configuration mode.
7	show voice port slot/sub-slot/port:ds0-group-no	checks if the values set up in the voice port are set up normally.

Voice Volume Adjustment

It is recommended that voice volume be as uniform as possible when the subscriber makes a call through a packet voice network, but in some countries, adjusting input or output volume may be required depending on kinds of network equipment. To provide this kind of gain adjustment function on the network, the command for input gain and output attenuation is supported. A user should be cautious in using this command. Setting input/output gain the wrong may greatly affect voice quality. For example, if you set input gain too high, the voice may be disconnected or too loud, otherwise setting too low input gain may cause the voice to be too low to hear.

Step	Command	Purpose
1	configure terminal	Enter the global configuration mode.
2	dial-peer voice voip <i>num</i>	Enter the dial-peer configuration mode.
3	digital-gain input <i>vaueI</i>	Sets the PCM-to-encoder input gain, in decibels ranging from -13.9 to 6.0. The changes take effect at the next trial of voice connection
4	digital-gain output <i>value</i>	Sets the decoder-to-PCM output gain, in decibels ranging from -13.9 to 6.0. The changes take effect at the next trial of voice connection.
5	Exit	Exit the voice-port configuration mode.
6	show voice port <i>slot/sub-slot/port:ds0- group-no</i>	checks out if the values set up in the voice port are set up normally.

Jitter Adjustment

In order to compensate variable-length voice delay, Jitter Adjustment sets up a method to cope with packet jitter depending on the features of the packet network on which the voice connection is made. The call route on the IP side in case of a VoIP call is determined by the dial peer. From this reason, the features of the IP network can be easily known, and the optimal setup easily determined. Accordingly, the initial setup and control of the dynamic jitter buffer in order to cope with voice delay is executed on the basis of information configured in the dial peer, and set up with the **playout-delay** command.

Step	Command	Purpose
1	configure terminal	Enters the global configuration mode.
2	dial-peer voice voip <i>number</i>	Enters the dial-peer configuration mode.
3	playout-delay mode {adaptive fixed}	Determines the mode in which the jitter buffer will operate for calls on this dial-peer. - adaptive-adjusts the size of the jitter buffer depending on the condition of the present network to manage QoS. - fixed-the size of jitter buffer set up initially continues to be used instead of being variable depending on network conditions.
4	playout-delay nominal <i>value</i>	A call beginning sets the jitter buffer size to be adapted. If network delay is uniform, after a call is made, playout delay is kept on basis of this setup value. In the mode above, if it is set as fixed, jitter buffer is kept with setup value of normal.
5	playout-delay maximum <i>value</i>	In case the jitter buffer size is set up in an adaptive mode, a maximum size is set in which the jitter buffer can be extended dynamically. This allows one to establish a delay limit where instant delay may increase dramatically on the network, and discards packets over the limit.
6	playout-delay minimum <i>value</i>	In case that jitter buffer size is set up in an adaptive mode, sets a maximum size in which the jitter buffer can be extended dynamically. On the network, delay reduces gradually to keep a value set to a minimum.
7	Exit	Exits the dial-peer configuration mode.

- Example of jitter buffer operation
 - Jitter buffer settings: minimum delay is 20 ms. maximum delay is 200 ms.
 - Network conditions: network delay changes from 200 ms to 10 ms to 500 ms.

When jitter is 200 ms, the jitter buffer will quickly adapt up to 200 ms (maximum). If network jitter decrease to 10 ms and stays there for a LONG time, the jitter buffer will slowly adapt down to 20 ms (minimum), and stay there until the jitter increases to 500 ms. If network jitter decrease to 10 ms for just a little while and goes up again, the jitter buffer may just adapt down for a little and go up again, or may not adapt down at all.

For 500 ms jitter, the jitter buffer will not go over 200 ms (maximum).

Country Variants

In case of E1-R2, use subcommands of cas-custom for PSTN signaling-related setting. To accommodate Country variants of E1-R2, one can set the variant value by country. The following describes the setup process of cas-custom. CLI commands after the 'country' command setting are necessary for customizing the set up values.

Step	Command	Purpose
1	configure terminal	Enters the global configuration mode.
2	voice-port slot/sub-slot/port:ds0-group-no	Enters the module configuration mode.
3	cas-custom	Enters cas-custom configuration mode. Customizes E1-R2 signaling parameters for the particular ds0-group on a channelized E1 line.
4	country name [use-defaults]	Selects a country to initialize the parameters of the CAS variant. if you select the appropriate country using the commands below, parameters available for the setting may be initialized to the appropriate values for the corresponding country. if you don't input use-defaults, apply signaling state by country. The countries supported are as follows: - australia-australia country specification. - brazil-brazil country specification. - china-china country specification. - east europe-easteurope country specification. - hongkong-hongkong country specification. - India-india country specification. - itu-itu country specification. - korea-korea country specification. - thailand-thailand country specification. - mexico-mexico country specification.
4	country name [use-defaults]	Using the country default command, after setting the parameters as a default value used in a specific country, and using the command for each CLI, it is possible to tune each command.
5	ani-digits	Specifies the number of ANI digits expected to be collected.
6	answer-signal	Specifies answer signal to be used which can be group-A or group-B.

(Continued)

Step	Command	Purpose
7	caller-digits	Specifies the number of digits needed to be collected before it requests ANI.
8	default	Sets a command to its default setting.
9	dnis-digits	Specifies the expected number of DNIS digits.
10	invert-abcd	Specifies the inversion of the ABCD bits before tx and after rx.
11	ka	Specifies the KA signal code ranging from 1 to 15.
12	kd	Specifies the KD signal code ranging from 1 to 15.
13	metering	Specifies sending a metering pulse when the gateway is making an outgoing call.
14	nc-congestion	Specifies the none compelled congestion signal.
15	request-category	DNIS digits to be collected before requesting a line category.
16	unused-abcd	Specifies unused ABCD bit values.
17	exit	Exits the cas-custom configuration mode.
18	exit	Exits the voice-port configuration mode.

Country Variant Parameters

1. ANI digits
Expected number of ANI digits.
Sets up the maximum and minimum number of ANI digits that the receiver expects to receive from the calling side.
2. Answer signal
Answer signal to be used.
Determines a signal to inform that the terminating side has collected all information for call connection. Distinguishes Group A and Group B, and sets up the signal number of the group determined.
3. Caller digits
The number of digits to collect before requesting ANI or CallerID information.
The receiver side sets up the number of DNIS digits to receive ANI digits. After reception of the number digits set up, requests ANI.

- 4.** Category
The category type of incoming call.
- 5.** DNIS digits
Expected number of DNIS digits.
The calling side sets up maximum and minimum number of ANI digits that the receiver expects to receive. The receiver collects the determined digits from the receiver, and then determines the progress of a call.
- 6.** Invert ABCD
Inverts the ABCD bits before tx and after rx.
- 7.** KA
Determines signal number that may be used in KA signal.
- 8.** KD
Determines signal number that may be used in KD signal.
- 9.** Metering
Determines whether to create a metering pulse for outgoing call.
- 10.** Request category
DNIS digits to be collected before requesting line category.
When it works as R2 calling side, is used to send call priority defined in R2 to the receiver.
- 11.** Unused ABCD
Specifies unused ABCD bit values.

Digital Trunk T1-CAS Features

T1 Robbed Bit Signaling Concept

On T1 trunks, a frame consists of 24 timeslots, sent every 1/8000 sec.

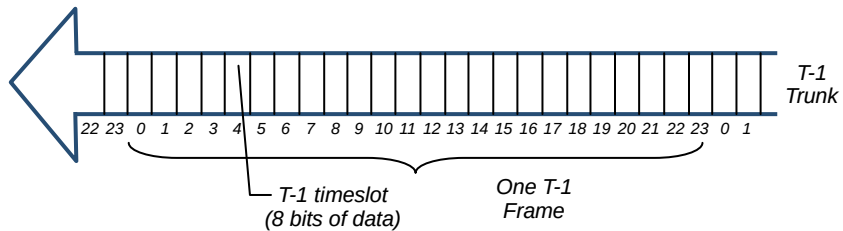


Figure 6.7 T1 frame and T1 timeslots for CAS signaling

On T1 trunks using a CAS protocol, signaling information for each channel is transmitted using a method called *robbed-bit signaling*.

The information for each channel consists of a set of bits (called *ABCD bits*). Whenever a channel's state changes, the ABCD bit pattern for that channel changes to convey the signaling bits. Signaling information is carried on a T1 trunk by two signaling bits, an A-bit and a B-bit.

The biggest disadvantage of CAS signaling is its use of user bandwidth in order to perform signaling functions.

The most common forms of CAS signaling are loopstart, groundstart, Equal Access North American (EANA), and E & M.

T1 CAS Signaling

CAS stands for Channel Associated Signaling and various types of CAS signaling are available in the T1 world. The most common forms of CAS signaling are loopstart, groundstart, and E & M signaling. These protocols provide information such as the number that was called, and what state the call is in. They're limited as to what information they can carry, and are slow to set up.

With this kind of signaling, a set of bits is used to replicate opening and closing the circuit (as if picking up the telephone receiver and pulsing digits on a rotary phone), or using tone signaling which is passed through on the voice circuits themselves.

The biggest disadvantage of CAS signaling is that the network uses bits from IP information packets, such as voice packets, to perform signaling functions. CAS signaling is often referred to as robbed-bit signaling.

Digital T1 trunk to be used in connection with most switch-to-switch is an E & M signaling type, but there is the case of partially forming a connection with FXS and FXO.

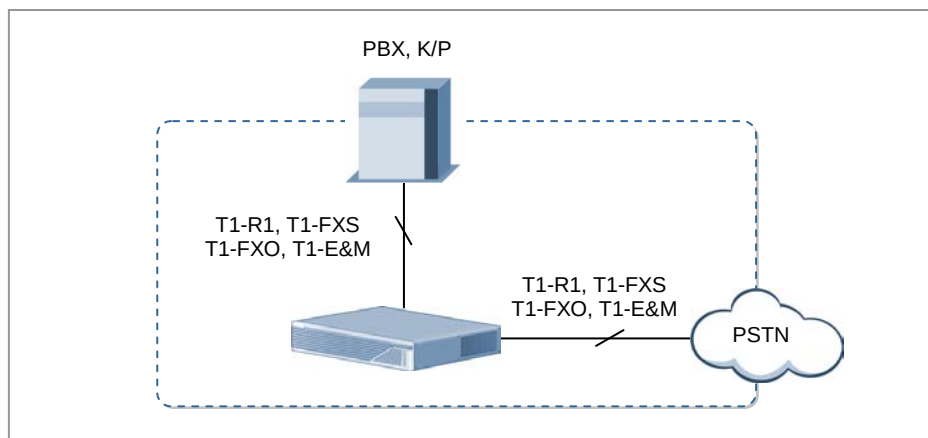


Figure 6.8 T1 CAS signaling network

1. Loopstart signaling

This is the simplest type of CAS signaling, which changes the operation type of analog FXS into digital signaling type as is. Thus, there are more defects than with other CAS signaling.

One of the defects is that there is no way to notify users of a far-end disconnect or answer, making it impossible for users to know the status. In the case of loop-start signaling, FXS only uses the A-bit and the FXO side only uses the B-bit to communicate call information..

2. Groundstart signaling

This is similar to loop-start signaling in many ways.

Its merits when compared with loop-start signaling are it supports far-end disconnect supervision which loop-start does not provide. This is done by using the A- and B- bit on the network side instead of just the B-bit. The A-bit is also used on the CPE side. However, the B-bit can also be involved, according to the switch's implementation.

Provides emulated-OPX from a PBX to remote stations using FXS and FXO connection. When FXS interworks with FXO, FXO and FXS should be directly connected between switches. When FXS connects to FXO, signaling should be matched using either ground-start or loop-start signaling. FXO provides better disconnect supervision than FXS. In this case, disconnect supervision means the function of noticing the fact that other party hung up call. Ground start provides this function, but connection should be formed after understanding the PBX characters due to the fact that not all PBXs possess FXS/FXO port supporting ground-start.

3. Groundstart signaling

Generally used for trunk lines. Because it is the signaling type devised to complement FXS/FXO defects, E & M connections are preferable to FXS/FXO. E & M connections from routers to telephone switches or to PBXs provide better answer and disconnect supervision.

E & M signaling has many advantages over the previous CAS signaling methods discussed in this document. It provides both disconnect and answer supervision as well as glare avoidance. E & M signaling is simple to understand and is the preferred choice when you use CAS.

Trunk Information Management

Requirements

Prerequisites

Before you attempt this configuration, ensure that you meet these prerequisites:

- T1-CAS signaling applies to T1 trunk only
- In order to run T1-CAS signaling on the UBIGATE iBG routers, this hardware is required:
 - WTE-2M or WTE-4
- Define the command **cas-ds0-group** on the T1 trunk (module) to create ds0-group.
- Use the command **voice-port** in order to choose the proper signaling and its subsequent properties.

Configuration Steps

- Complete physical layer of T1 trunk settings-‘**system carrier**’ and ‘**module**’
- Create ds0-groups to manage the DS0 channels on the T1 trunk-‘**cas-ds0-group**’
- Configure ds0-group with sub-commands such as ‘**timeslots**’ and ‘**signal cas**’
- Customize CAS signaling properties with the ‘**define**’ and ‘**condition**’ command.

Configure T1 Trunk

This section describes the procedure to configure physical layer of the T1 trunk.

Configuring T1 Trunk Settings

To make a T1 connection with neighboring equipment interworking on PSTN, the specific characteristics of the T1 trunk line should be met. This configuration is made typically in **module** configuration mode.

To configure T1 CAS, the following procedure should be completed.

1. Set up a T1 trunk that connects to the private automatic branch exchange (PBX) or switch.
2. Ensure that the framing and linecoding of the T1 are set properly.
3. For T1 framing, choose either **ESF** or **D4**.
4. For T1 linecoding, choose either **B8ZS** or **AMI**.
5. For the T1 clock source, choose either **internal** or **line**. Keep in mind that different PBXs have different requirements on the clock source. Configuration of the clock source is only used in module command.
6. Configure line signaling and interregister signaling for CAS.
7. Customize the configuration with the **cas-custom** command.

This procedure is similar to the configuration of E1 trunk.

Step	Command	Purpose
1	show voice card all	List all the voice cards installed in the system. If you find any of the WTE_XX card you can choose the one to use a T1 trunks card.
2	show module configuration all	Displays all the digital trunks active in the system. So if you use this command it helps you to recognize the carrier-types of the trunks installed in the system.
3	configure terminal	Enters the global configuration mode to advance the T1 setting.
4	system carrier-type slot # t1	Inputs the <i>slot#</i> which is qualified to be a T1 trunk card. And if the previous carrier-type of the slot is configured T1, rebooting is not required. Otherwise the system will prompt you to reboot the system for the change to take effect.
5	configure terminal	-
6	module t1 trunk#	Specifies the T1 trunk for which you want to configure physical layer settings. <i>trunk#</i> is a simple notation of <i>slot/sub-slot/port</i> , for convenience.
7	clock_source { internal line }	Configures the clock source. line-Specifies that the clock-facility on this port derives clocking from the external source to which the port is connected (generally the CO). internal - (Optional) Specifies that the clock is generated from the voice card's internal clock-facility.
8	framing { esf d4 }	Selects frame type for T1 or E1 line. esf-Extended super frame framing format for T1. d4-Super frame framing format for T1. disable-Disables E1 framer.
9	linecode { b8zs ami }	Specifies the line encoding to use. The keywords are as follows: ami-Specifies the alternate mark inversion (AMI) line code type. (T1 and E1) b8zs-Specifies the binary 8 zero substitution line code type. (T1)

(Continued)

Step	Command	Purpose
10	Exit	Exits to the global configuration mode. Keep in mind that shutdown is not necessary as the settings are applied instantly.
11	show module configuration t1 trunk#	Check out the status of the specified trunks and the sanity. <i>trunk#</i> is a simple notation of <i>slot/sub-slot/port</i> , for convenience.

Create DS0 Groups on a Digital T1 Trunk

This procedure is similar to the configuration of E1 trunk.

Step	Command	Purpose
1	configure terminal	Assumes the trunk becomes active normally according to the steps above. Here the description starts with configuring CAS signaling to trunk.
2	module t1 trunk#	Enters the module configuration mode.
3	cas-ds0-group ds0-group-no	Enters the ds0-group number to create in this T1 trunk.
4	exit	Exits the module configuration mode.
5	show voice port summary	Check if ds0-group is created normally. Ds0-group created in the system is displayed in the <i>slot/sub-slot/port:ds0-group-no</i> status.

```
v239# show voice port summary
PORT      CH SIG-TYPE  ADMIN  OPER  IN STATUS  OUT STATUS  EC
=====  == =====  =====  =====  =====  =====  ==
0/0/0     -- fxs-ls    up      up    on-hook  idle       y
0/0/1     -- fxs-ls    up      up    on-hook  idle       y
0/0/2     -- fxs-ls    up      up    on-hook  idle       y
0/0/3     -- fxs-ls    up      up    on-hook  idle       y
0/1/0:10  -- ---      down    --    ----    ----       y
```

Trunk Status Monitoring

This procedure is similar to the configuration of E1 trunk.

Details in each following section refer to 'Trunk Status Monitoring'.

Physical Layer Status

Using show voice card all, check all the voice card installed in the system.

```
v239# show voice card all
```

SLOT	CARD TYPE	STATUS	VS VSLOTNAME
[DSP]	VoIP_M510	NORMAL	13 VoIP_VSLOT
[0/0]	FXS_4M	NORMAL	7 MM_2_VSLOT
[0/1]	WTE_2M	NORMAL	6 MM_1_VSLOT
[0/2]-	-	-	--
[1/0]-	-	-	--
[1/1]-	-	-	--
[2/0]-	-	-	--
[2/1]-	-	-	--

Using the show module configuration, carrier- type and status of trunk in operation can be checked.

```
v239# show module configuration t1 0/1/0
```

T1 0/1/0 is ENABLED

Alarm Hierarchy: TRUE,
Yellow Alarm: DISABLE
Framing:ESF, LineCode:B8ZS, ClockSource: INT, LineMode:CSU,
LBO:0 db
FDL: ANSI Unit Protocol enabled ,ATT Unit Protocol
disabled ,
CsuDsuType: CSU , Loopback Framing(In-band): Overwrite,
CIRCUIT-ID: Not Configured ,CONTACT-INFO: Not Configured ,
DESCRIPTION: Not Configured , LINK NAME: Not Configured ,

Line Status:

RLOS:OFF	RAIS:OFF	RLOF:OFF	RRAI:OFF	TAIS:OFF
TRAI:OFF	TPtrn:OFF	Loop:OFF		

Timeslot Map:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
22	23	24																		

[illegible]

v239# show module configuration all						
T1 #	Framing	Coding	ClkSrc	LB0-CableLength	State	Alarm

0/1/1	esf	b8zs	int	csu/0db	up	N/A
0/1/0	esf	b8zs	int	csu/0db	up	N/A

Using show voice port summary, check the status of the logical voice port (DS0 Groups) created in digital trunk. It displays all the voice ports created in the system including DS0 group.

Using `show voice port port#`, check the detailed setup value of the parameters used in the particular voice port.

This section describes management of logical voice ports configured in the digital E1 trunk.

- create a DS0 group
- delete a DS0 group
- configure DS0 group

Create Trunk Voce Port

It manages the DS0 group by logically combining with the DS0 channel, which belongs to digital trunk. The following describes the procedure to create the DS0 group.

Step	Command	Purpose
1	configure terminal	Enter the global configuration mode
2	module t1 slot/sub-slot/port	Select trunk to create DS0 group.
3	cas-ds0-group ds0-group-no	ds0-group-no: Identifies the unique DS0 group (number from 0 to 23, for T1, or from 0 to 30, for E1) in a specific trunk.
4	exit	Exit the module configuration mode
5	show voice port summary	Displays all the voice-port configured in the system. Checks out whether the ds0-group just created exists or not.

Delete Trunk Voce Port

This is a function to delete the DS0 group created in a specific digital trunk. The following describes the procedure to delete the DS0 group.

Step	Command	Purpose
1	configure terminal	Enter the global configuration mode
2	module e1 slot/sub-slot/port	Select trunk to delete DS0 group.
3	no cas-ds0-group ds0-group-no	ds0-group-no: Identifies the unique DS0 group (number from 0 to 23, for T1, or from 0 to 30, for E1) in a specific trunk.
4	exit	Exit the module configuration mode
5	show voice port summary	Displays all the voice-port configured in the system. Checks out whether the ds0-group just deleted remains or not.

Configure Basic Trunk Voice Port Parameters

Use the partial setup function of the DS0 group configured in the digital trunk. In most cases, if the voice port is created for operating the voice port function with the minimum setup, each command is initialized with the default value.

Also supports advanced configuration function to support more detailed setup or additional setup.

Step	Command	Purpose
1	configure terminal	Enters the global configuration mode.
2	voice-port slot/sub-slot/port:ds0-group-no	Enters the module configuration mode.
3	locale locale	Selects a two-letter country name defined in the voice-port mode. It decides the call progress tone parameters and other locale-specific parameters.
4	compand-type { u-law a-law }	Specifies companding standard used. Even though values setup here are different, TDM switch enables conversion.
5	description	Optional-the setup-representative ID for voice-port, and names text string.
6	exit	Exits the voice-port configuration mode.
7	show voice port slot/sub-slot/port:ds0-group-no	Checks out if the values set in voice-port are set up normally.

Configure Advanced Trunk Voice Port Parameters

It is the same as the creation of the E1 trunk voice port, and for T1 CAS signaling, and the following advanced setting is possible.

T1-CAS Bit Modification Settings

The bit modification commands for digital voice ports modify sent or received bit patterns. Different versions of E & M use different ABCD signaling bits to represent idle and seize. For example, North American CAS E & M represents idle as 0XXX and seize as 1XXX, where X indicates that the state of the BCD bits is ignored. In MELCAS E & M, idle is 1101 and seize is 0101.

The commands in this section are provided to modify bit patterns to match particular E & M schemes.

To manipulate bit patterns for trunk voice ports, use the following commands as necessary, in voice-port configuration mode:

Step	Command	Purpose
1	voice-port slot/sub-slot/port:ds0-group-no	To set up the attribute values of the created ds0-group, starts with voice-port configuration mode. if ds0-group was created normally, there is no error in this CLI command.
2	shutdown	Shuts down the voice port to manipulate 'timeslots' and 'signal cas' command.
3	condition {tx-a-bit tx-b-bit tx-c-bit tx-d-bit} {rx-a-bit rx-b-bit rx-c-bit rx-d-bit} {on off invert}	Manipulates sent or received bit patterns to match expected patterns on a connected device. Repeat the command for each transmit and/or receive bit to be modified, but be careful not to destroy the information content of the bit pattern. The default is that the signaling format is not manipulated (for all transmit or receive A, B, C, and D bits). on-Sets the bit to 1 permanently. off-Sets the bit to 0 permanently. invert-Changes the state to the opposite of the original transmit or receive state.
4	define {tx-bits rx-bits} {seize idle} {0000 0001 0010 0011 0100 0101 0110 0111 1000 1001 1010 1011 1100 1101 1110 1111}	Defines specific transmit or receive signaling bits to match the bit patterns required by a connected device for North American E & M and E & M MELCAS voice signaling, if patterns different from the preset defaults are required. Also specifies which bits a voice port monitors and which bits it ignores, if patterns that are different from the defaults are required. tx-bits-Indicates that the pattern applies to transmit signaling bits. rx-bits-Indicates the pattern applies to receive signaling bits. seize-Indicates that the pattern represents line seizure. idle-Indicates that the pattern represents an idle condition. 0000...1111-Represents the bit pattern to use.

(Continued)

Step	Command	Purpose
5	ignore {rx-a-bit rx-b-bit rx-c-bit rx-d-bit}	Configures the voice port to ignore the specified receive bit for North American E & M, if patterns different from the defaults are required.
6	no shutdown	Activates the voice port at the final step of configuration.
7	exit	-

Calling Number Outbound Settings

If T1 CAS is configured with the FGD-EANA signaling, the automatic number identification (ANI) can be sent for outgoing calls by using the calling-number outbound command.

FGD-EANA is a FGD signaling protocol of type EANA, which provides certain call services, such as emergency (USA 911) calls. ANI is a series of digits in the call to identify the telephone number of the calling device. In other words, ANI identifies the number of the calling party.

Step	Command	Purpose
1	voice-port slot/sub-slot/port:ds0-group-no	To set up the attribute values of created ds0-group, enters voice-port configuration mode.
2	shutdown	Shuts down the voice port to manipulate 'timeslots' and 'signal cas' command.
3	calling-number outbound range string1 string2	Specifies ANI to be sent out when the T1-CAS fgd-eana command is configured as signaling type. The string1 and string2 arguments are valid E.164 telephone number strings. Only the last four digits are used for specifying the range (<i>string1</i> to <i>string2</i>) and for generating the sequence of ANI by rotating through the range until <i>string2</i> is reached and then starting from <i>string1</i> again. If strings are less than four digits in length, then entire strings are used.

(Continued)

Step	Command	Purpose
4	calling-number outbound sequence [string1] [string2] [string3] [string4] [string5]	Specifies ANI to be sent out when the T1-CAS fgd-eana command is configured as the signaling type. This option configures a sequence of discrete strings (<i>string1...string5</i>) to be passed out as ANI for successive calls using the dial peer or voice port. Limit is five (5) strings. All strings must be valid E.164 numbers, up to 32 digits in length.
5	calling-number outbound null	Suppresses ANI. No ANI is passed when this voice port is selected.
6	no shutdown	Activates the voice port at the final step of configuration.
7	exit	-

Timeouts Settings

To change timeouts parameters, use the following commands as appropriate, in voice-port configuration mode:

Step	Command	Purpose
1	voice-port slot/sub- slot/port:ds0-group-no	To set up the attribute values of created ds0-group, enters voice-port configuration mode.
2	Shutdown	Shuts down the voice port to manipulate 'timeslots' and 'signal cas' command.
3	timeouts call- disconnect seconds	Configures the call disconnect timeout value in seconds.
4	timeouts initial seconds	Sets the number of seconds that the system waits between the caller input of the initial digit and the subsequent digit of the dialed string. If the wait time expires before the destination is identified, a tone sounds and the call ends. The seconds argument is the initial timeout duration. A valid entry is an integer from 0 to 120. The default is 10.

(Continued)

Step	Command	Purpose
5	timeouts interdigit seconds	Configures the number of seconds that the system waits after the caller has input the initial digit or a subsequent digit of the dialed string. If the timeout ends before the destination is identified, a tone sounds and the call ends. This value is important when using variable-length dial peer destination patterns (dial plans). The <i>seconds</i> argument is the interdigit timeout wait time in seconds. A valid entry is an integer from 0 to 120. The default is 5.
6	timeouts ringing seconds	Specifies the duration that the voice port allows ringing to continue if a call is not answered. 0 means 'infinity' of ringing.
7	timeouts wait-release seconds	Specifies the duration that a voice port stays in the call-failure state while the Cisco device sends a busy tone, reorder tone, or an out-of-service tone to the port. If <i>seconds</i> is set to 0, it means 'infinite' ringing.
8	no shutdown	Activates the voice port at the final step of configuration.
9	Exit	-

Timing Settings

To change timing parameters, use the following commands as appropriate, in voice-port configuration mode.

Step	Command	Purpose
1	voice-port slot/sub-slot/port:ds0-group-no	To set up the attribute values of created ds0-group, enters voice-port configuration mode.
2	timing clear-wait milliseconds	(E & M only) Specifies the minimum amount of time between the inactive seizure signal and clearing of the call. Valid entries for the <i>milliseconds</i> argument are from 200 to 2000 milliseconds. The default is 400.
3	timing delay-duration milliseconds	(E & M only) Specifies the delay signal duration for delay-dial signaling in milliseconds. Valid entries are from 100 to 5000. The default is 2000.

(Continued)

Step	Command	Purpose
4	timing delay-start milliseconds	(E & M only) Specifies minimum delay time, in milliseconds, from outgoing seizure to outdial address. Valid entries are from 20 to 2000. The default is 300.
5	timing dialout-delay milliseconds	Specifies dialout delay, in milliseconds, for the sending digit or cut-through on an FXO trunk or an E & M immediate trunk. Valid entries are from 100 to 5000. The default is 300.
6	timing digit milliseconds	Specifies the DTMF digit signal duration in milliseconds. Valid entries are from 50 to 100. The default is 100.
7	timing guard-out milliseconds	(FXO ports only) Specifies the duration in milliseconds of the guard-out period that prevents this port from seizing a remote FXS port before the remote port detects a disconnect signal. The range is from 300 to 3000. The default is 2000.
8	timing hookflash-out milliseconds	Specifies the duration, in milliseconds, of the hookflash. Valid entries are from 50 to 500. The default is 300.
9	timing wink-duration milliseconds	(E & M only) Specifies maximum wink-signal duration, in milliseconds, for a wink-start signal. Valid entries are from 100 to 400. The default is 200.
10	timing wink-wait milliseconds	(E & M only) Specifies maximum wink-wait duration, in milliseconds, for a wink-start signal. Valid entries are from 100 to 5000. The default is 200.
11	Exit	Exits the voice-port configuration mode.

T1-CAS FXO Features

Foreign eXchange (FX) signaling was originally developed to connect remote Private Branch Exchanges (PBX's) to the (Bell System) Central Office. These PBXs (and other Central Offices) were considered 'Foreign' not because they were outside the country, but because they didn't belong to the 'Phone Company.' A FXS (FX-Subscriber) interface will be connected to a matching FXO (FX-Office) interface at the far end.

Note that audio paths (such as the 'CO sends Dial Tone' path) are not usually considered part of the FX signaling. They are included to make the examples easier to understand.

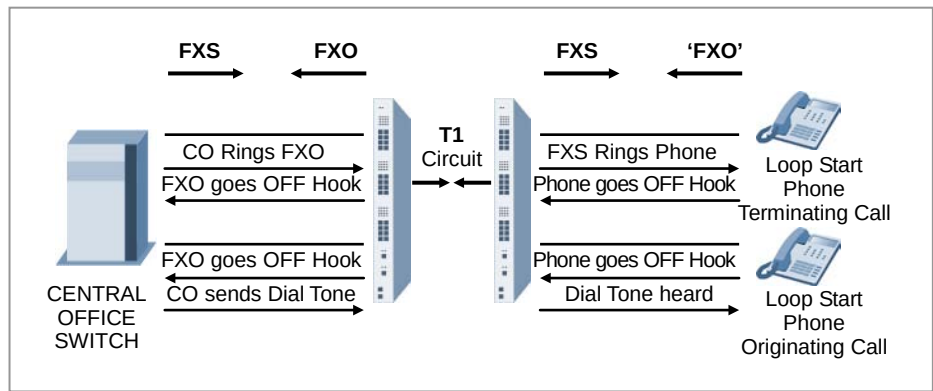


Figure 6.9 T1 CAS FXS/FXO signaling operation

Loop Start

As shown in the POTS diagram above, Loop Start signaling uses only two basic states: Ringing (sent to the FXO interface) and Off-Hook (sent to the FXS interface). Loop Start signaling is the most common type of signaling deployed in the PSTN.

Although it is not very common, problems can occur whenever automatic answering equipment is used as the phone. Since there is no way for the CO to tell the phone to hang up (go On-Hook), if the answering equipment never times out then the circuit can be permanently seized. This is usually not a problem for 'real' phones, since the end user will realize that there is no one on the call and hang up. This problem can be solved by using Ground Start signaling.

Ground Start

Ground Start signaling was originally developed to aid in resolving Glare. In Loop Start the only way to indicate an inbound call from the network is to Ring the phone. During a full 6-second ringing cycle there is a 4-second period when the phone is not physically ringing. So how do you know whether a PBX is trying to answer an inbound call or if it is trying to initiate a new call? Ground Start eliminates this problem by adding an additional state (Tip Closed) which tells the FXO circuit that there is an inbound call in progress, even during the 'quiet' ringing cycle.

For outbound calls, the PBX (or FXO interface) must first seize the line by applying ground to the Ring lead of the Tip/Ring pair (Ring Ground). The CO (or FXS interface) now knows that the FXO is trying to make an outbound call, and it will not terminate inbound calls on that circuit.

Digital Loop-Start signaling

In case of Loop-start signaling, it works according to the following state table.

Incoming Call

State	Sent		Received	
	a[f]	b[f]	a[b]	b[b]
Idle	0	1	0	1
Seizured	0	1	1	1

Outgoing Call

State	Sent		Received	
	a[f]	b[f]	a[b]	b[b]
Idle	0	1	0	1
Seizing	0	0	0	1
Seizure Ack.	0	0	1	1
Seizured	0	1	1	1

Digital Ground-Start signaling

In case of Ground-start signaling, it works according to the following state table.

Incoming Call

State	Sent		Received	
	a[f]	b[f]	a[b]	b[b]
Idle	1	1	0	1
Seizured	1	1	0	0
Responding	0	1	0	0
Responded	0	1	1	1

Outgoing Call

State	Sent		Received	
	a[f]	b[f]	a[b]	b[b]
Idle	1	1	0	1
Seizing	0	0	0	1
Seizure Ack.	0	0	1	1
Seizured	0	1	1	1

Configure T1-CAS FXO signaling

Step	Command	Purpose
1	configure terminal	Enters the global configuration mode.
2	module t1 slot/sub-slot/port	Enters the module configuration mode.
3	cas-ds0-group ds0-group-no	Enters the ds0-group number to create in this E1 trunk.
4	Exit	Exits module configuration mode.
5	voice-port slot/sub-slot/port:ds0-group-no	To set up the attribute values of created ds0-group, enters voice-port configuration mode. if ds0-group was created normally, there is no error in this CLI command.
6	shutdown	Shuts down the voice port to manipulate 'timeslots' and 'signal cas' command.

(Continued)

Step	Command	Purpose
7	timeslots <i>timeslot-list</i>	timeslots -Specifies the single time slot number, single range of numbers, or multiple ranges of numbers separated by commas. For T1, allowable values are from 1 to 24. Examples are as follows: -2, 3-5 -1, 7, 9 -1-12
8	signal cas fxo-loop-start or signal cas fxo-ground-start	Chooses FXO signaling method.
9	no shutdown	Activates the voice port at the final step of configuration.
10	exit	-

T1-CAS FXS Features

Digital Loop-Start signaling

In case of Loop-start signaling, it works according to the following state table.

Incoming Call

State	Sent		Received	
	a[f]	b[f]	a[b]	b[b]
Idle	0	1	0	1
Seizured	0	1	0	0
Responding	1	1	0	0
Responded	1	1	0	1

Outgoing Call

State	Sent		Received	
	a[f]	b[f]	a[b]	b[b]
Idle	0	1	0	1
Seizing	1	1	0	1

Digital Ground-Start signaling

In case of Ground-start signaling, it works according to the following state table.

Incoming Call

State	Sent		Received	
	a[f]	b[f]	a[b]	b[b]
Idle	0	1	1	1
Seizured	0	1	0	0
Responding	1	1	0	0
Response Ack	1	1	0	1

Outgoing Call

State	Sent		Received	
	a[f]	b[f]	a[b]	b[b]
Idle	0	1	1	1
Seizing	0	0	1	1
Seizure Ack.	0	0	0	1
Responded	1	1	0	1

Configure T1-CAS FXS signaling

Step	Command	Purpose
1	configure terminal	Enters the global configuration mode.
2	module t1 slot/sub-slot/port	Enters the module configuration mode.
3	cas-ds0-group ds0-group-no	Enters the ds0-group number to create in this E1 trunk.
4	exit	Exits the module configuration mode.
5	voice-port slot/sub-slot/port:ds0-group-no	To set up the attribute values of created ds0-group, enters voice-port configuration mode. if ds0-group was created normally, there is no error in this CLI command.
6	shutdown	Shuts down the voice port to manipulate 'timeslots' and 'signal cas' command.

(Continued)

Step	Command	Purpose
7	timeslots <i>timeslot-list</i>	timeslots-Specifies the single time slot number, single range of numbers, or multiple ranges of numbers separated by commas. For T1, allowable values are from 1 to 24. Examples are as follows: -2, 3-5 -1, 7, 9 -1-12
8	signal cas fxs-loop-start or signal cas fxs-ground-start	Chooses FXS signaling method.
9	no shutdown	Activates the voice port at the final step of configuration.
10	exit	-

T1-CAS E & M Features

For digital T1 Channel Associated Signaling (CAS) trunks running ear and mouth (E & M) signaling, there are generally only two states that a voice channel can be in. When there is no call on a channel, it is in the Idle, or On-Hook state. When there is an active call on a channel, then it is in the Seized, or Off-Hook state.

State	Originate (Transmit)				Destination (Receive)			
	a[f]	b[f]	c[f]	d[f]	a[b]	b[b]	c[b]	d[b]
Idle/On-hook	0	0	0	0	0	0	0	0
Seized/Off-hook	1	1	1	1	1	1	1	1

Wink-Start signaling

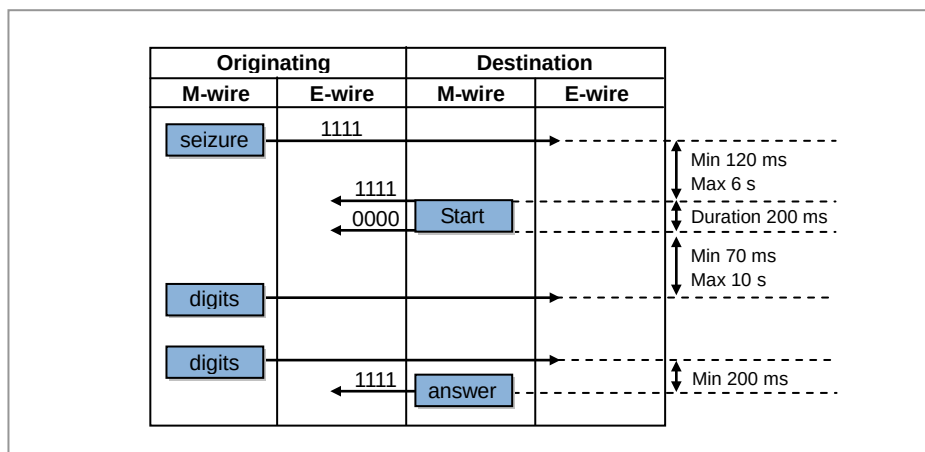


Figure 6.10 Wink-start method signaling sequence

Immediate-Start signaling

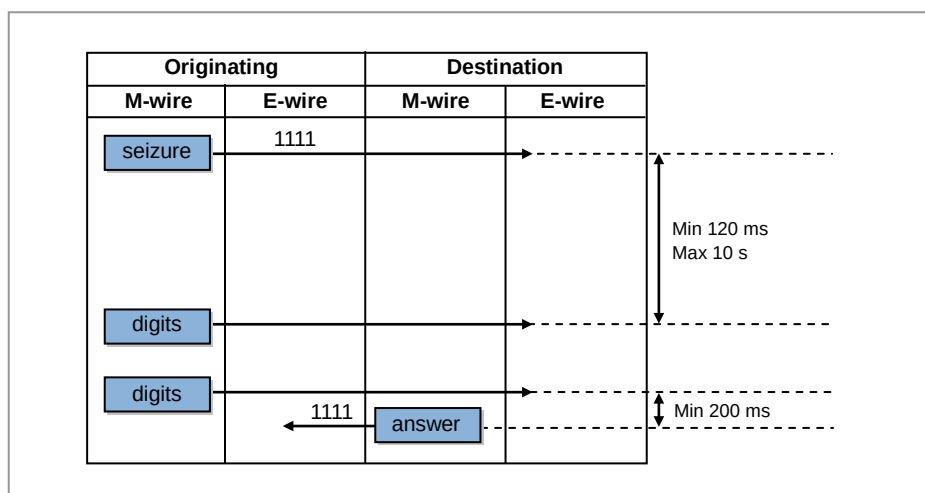


Figure 6.11 Immediate-start method signaling sequence

Delay-Dial signaling

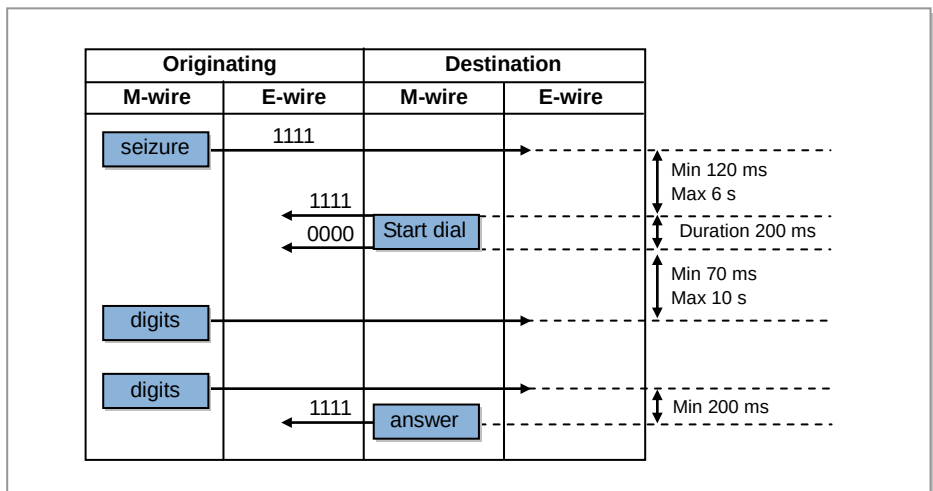


Figure 6.12 Delay-dial method signaling sequence

Configure T1-CAS E & M signaling

Step	Command	Purpose
1	configure terminal	Enters the global configuration mode.
2	module t1 slot/sub-slot/port	Enters the module configuration mode.
3	cas-ds0-group ds0-group-no	Enters the ds0-group number to create in this E1 trunk.
4	exit	Exits the module configuration mode.
5	voice-port slot/sub-slot/port:ds0-group-no	To set up the attribute values of created ds0-group, starts with voice-port configuration mode. if ds0-group was created normally, there is no error in this CLI command.
6	shutdown	Shuts down the voice port to manipulate 'timeslots' and 'signal cas' command.
7	timeslots timeslot-list	timeslots-Specifies the single time slot number, single range of numbers, or multiple ranges of numbers separated by commas. For T1, allowable values are from 1 to 24. Examples are as follows: -2, 3-5 -1, 7, 9 -1-12

(Continued)

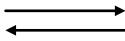
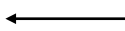
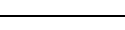
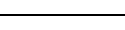
Step	Command	Purpose
8	signal cas enm-delay-dial or signal cas enm-immediate-start or signal cas enm-wink-start	Chooses E & M signaling method. enm-delay-dial-delay dial signaling method enm-immediate-start-immediate start signaling method enm-wink-start-wink start signaling method
9	no shutdown	Activates the voice port at the final step of configuration.
10	exit	-

T1-CAS R1 Features

T1-CAS R1 is a type of Channel-Associated Signaling (CAS) used widely in places other than North America.

Line Signaling

Is in compliance with ITU-T Q.311/Q.314/Q.315 Recommendation.

Signal	Signal direction	Transmitted duration	Transmitted state	
			Originating end	Terminating end
Idle		continuous	0	0
Connect (seizing)		continuous	1	0
Delay-dialing		continuous	1	1
Start-dialing		continuous	1	0
Answer		continuous	1	1
Hang-up (Clear-back)		continuous	1	0
Disconnect (Clear-forward)		continuous	0	0 or 1
Ring-forward		65-135 ms	0	0 or 1
Busy, Re-order		-	off	on

Address Signaling

Is in compliance with the ITU-T Q.316~Q.326 recommendation.

Signals	Frequencies (Hz)	Signals	Frequencies (Hz)
KP (start-of-pulsing)	1100 + 1700	Digit 8	900 + 1500
Digit 1	700 + 900	Digit 9	1100 + 1500
Digit 2	700 + 1100	Digit 0	1300 + 1500
Digit 3	900 + 1100	SP(end-of-pulsing)	1500 + 1700
Digit 4	700 + 1300	spare	700 + 1700
Digit 5	900 + 1300	spare	900 + 1700
Digit 6	1100 + 1300	spare	1300 + 1700
Digit 7	700 + 1500	-	-

Configure T1-CAS E & M signaling

Step	Command	Purpose
1	configure terminal	Enters the global configuration mode.
2	module t1 <i>slot/sub-slot/port</i>	Enters the module configuration mode.
3	cas-ds0-group <i>ds0-group-no</i>	Enters the ds0-group number to create in this E1 trunk.
4	exit	Exits the module configuration mode.
5	voice-port <i>slot/sub-slot/port:ds0-group-no</i>	To set up the attribute values of created ds0-group, enters voice-port configuration mode. if ds0-group was created normally, there is no error in this CLI command.
6	shutdown	Shuts down the voice port to manipulate 'timeslots' and 'signal cas' command.
7	timeslots <i>timeslot-list</i>	timeslots-Specifies the single time slot number, single range of numbers, or multiple ranges of numbers separated by commas. For T1, allowable values are from 1 to 24. Examples are as follows: -2, 3-5 -1, 7, 9 -1-12

(Continued)

Step	Command	Purpose
8	signal cas r1-itu or signal cas r1-modifited	Chooses T1-R1 signaling method. r1-itu-R1 signaling compliant with ITU-T recommendation. r1-modified-R1 signaling variants.
9	no shutdown	Activates the voice port at the final step of configuration.
10	exit	Exits the voice-port configuration mode.



CHAPTER 7. ISDN

Overview

Integrated Services Digital Network (ISDN) is composed of data service and telephone service provided by a telephone carrier. Since ISDN includes telephone digitalization, it can transmit voice, data, text, graphic, music, video and data transmissible by telephone line. The appearance of ISDN enables standardizing the subscriber service standard, the user network interface, and the network and inter-network capacity. ISDN application can provide services such as image, telephone, transmission of high-capacity file and videoconferencing at high speeds.

This section briefly introduces ISDN service.

Services

BRI Service

BRI (Basic Rate Interface) service possesses two B channels and one D channel (2B+D). BRI B-channel service is operated with 64 Kbps User data. BRI D-channel service is operated with 16 Kbps, transmitting signal information and management information. According to OSI reference model, D CH ranges from Layer1 to Layer3. BRI is made up of 192 Kbps. The BRI physical layer specification is the International Telecommunication Union-Telecommunications Standards Section (ITU-T) (formerly the Consultative Committee for International Telegraph and Telephone [CCITT]) I.430.

PRI Service

In America and Japan, PRI (Primary Rate Interface) service is made up of 23 B channel and 1 D channel, which is 1.544 Mbps (the PRI D channel runs at 64 kbps) in total (T1). Countries in Europe and Australia use PRI service made up of 30 B channels plus one 64-kbps D channel, which is 2.048 Mbps in total (E1). The PRI physical layer specification is ITU-T I.431.

ISDN Call Flow.

Two Layer 3 specifications are used for ISDN signaling: ITU-T (formerly CCITT) I.450 (also known as ITU-T Q.930) and ITU-T I.451 (also known as ITU-T Q.931). Together, these protocols support user-to-user, circuit-switched, and packet-switched connections. A variety of call-establishment, call-termination, information, and miscellaneous messages are specified, including SETUP, CONNECT, RELEASE, USER INFORMATION, CANCEL, STATUS, and DISCONNECT. These messages are functionally similar to those provided by the X.25 protocol.

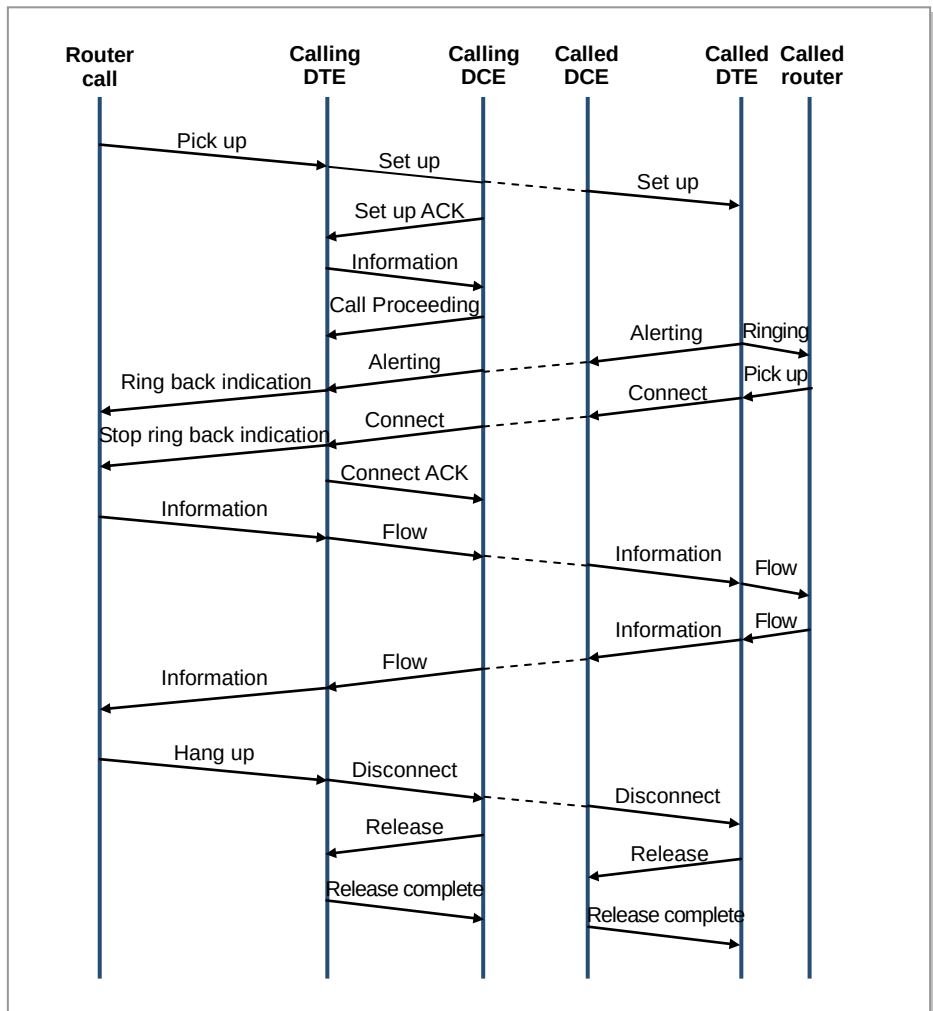


Figure 7.1 ISDN Call Flow

Configuring ISDN BRI

Requirements

Prerequisites

Before you attempt this configuration, ensure that you meet these prerequisites:

- If the router will be the only device attached to the BRI, ask for point-to-point service and a data-only line.
- If the router will be attached to an ISDN bus (to which other ISDN devices might be attached), ask for point-to-multipoint service and a voice-and-data line.

Configuration Steps

- Create an interface bundle to manage the bundle channels on the BRI-**'bundle'**
- Configure the ISDN switch type.
- Configure Voice set-up.
- Activate the ISDN.
- Delete the ISDN.
- Optional ISDN Configuration.

Create interface bundle

To create the interface bundle, use the following command.

Step	Command	Purpose
1	configure terminal	Configures to set up bundle.
2	interface bundle <i>bundle-name</i>	Designates bundle name.
3	link bri <i>slot/sub-slot/port:timeslot</i>	Sets the pertinent physical link.

Configuring the ISDN BRI Switch-type

To configure the switch type, use the following command.

Step	Command	Purpose
1	configure terminal	Configures to set up bundle.
2	interface bundle bundle-name	Sets up bundle name.
3	link bri slot/sub- slot/port:timeslot	Sets up the pertinent physical link. (slot/subslot/port:*timeslots)
4	isdn	Sets up ISDN.
5	switch-type switch-type	Sets the pertinent switch-type with the content like the below table 36.1.

* timeslots: BRI is just 1 or 2. (but ignored value)

Table 7.1 switch-type parameter description (BRI)

Switch Type Keywords	Description
Basic-ni	National ISDN Basic Rate Switch Type (only user side)
Basic-dms	NT DMS-100 Basic Rate Switch Type.
Basic-5ess	AT & T Basic Rate Switch Type (default).
Basic-ntt	NTT Basic Rate Switch Type.
Basic-euro	Euro ISDN Basic Rate Switch Type.
Basic-ccitt	CCITT/ITU-T Basic Rate Switch Type.
Basic-aus	Australian Telecom Basic Rate Switch Type (only user side).

Configuring Voice set-up

To configure the voice type, use the following command:

Step	Command	Purpose
1	configure terminal	Configures to set up bundle.
2	interface bundle <i>bundle-name</i>	Sets up bundle name.
3	link bri <i>slot/sub-slot/port:timeslot</i>	Sets up the pertinent physical link.
4	isdn	Sets up ISDN.
5	switch-type <i>switch-type</i>	Sets up the pertinent switch-type with the content like the following table.
6	incoming-voice	Sets up for voice.

Activate the ISDN

To activate the ISDN, use the following command:

Step	Command	Purpose
1	configure terminal	Configures to set up bundle.
2	interface bundle <i>bundle-name</i>	Sets up bundle name.
3	link bri <i>slot/sub-slot/port:timeslot</i>	Sets up the pertinent physical link.
4	isdn	Sets up ISDN..
5	switch-type <i>switch-type</i>	Sets up the pertinent switch-type with the content like the following table.
6	incoming-voice	Sets up for voice.
7	activate	Activates ISDN.
8	exit	-
9	voice-port <i>slot/sub-slot/port</i>	Configures to set up voice port
10	no shutdown	Turns on the port.

Delete the ISDN

To delete the ISDN, use the following command:

Step	Command	Purpose
1	configure terminal	Configures to set up bundle.
2	voice-port <i>slot/sub-slot/port</i>	Configures to set up voice-port.
3	shutdown	Shuts down voice port.
4	no interface bundle <i>bundleName</i>	Deletes interface bundle.



NOTE

When an existing ISDN interface bundle used for voice (configured 'incoming-voice') is configured, the ISDN voice-port should be shutdown before the ISDN bundle is deleted or 'no activate'.

Configuring ISDN: Overlap-receiving

A system should be configured with this commands to allow the router to wait for all the digits to be received before the call is routed. To enable this feature, use the following command:

Step	Command	Purpose
1	Configure terminal	Configures to set up bundle.
2	Interface bundle <i>bundle-name</i>	Sets up bundle name.
3	link bri <i>slot/sub-slot/port:timeslot</i>	Sets up the pertinent physical link.
4	Isdn	Sets up ISDN.
5	switch-type <i>switch-type</i>	Sets up the pertinent switch-type with the content like the following table.
6	Incoming-voice	Sets up for voice.
7	calling-number <i>calling-number</i>	Specifies the calling party number.
8	overlap-receiving	(Optional) Specifies if the interface will do Overlap Receiving. *(note)
9	Activate	Activates ISDN.
10	Exit	-
11	voice-port <i>slot/sub-slot/port</i>	Configures to set up voice port.
12	no shutdown	Turns on the port.



NOTE

When the peer system or switch is using overlap signaling, the system may not receive whole digits of the incoming call, while the system is configured to use enblock signaling. This can be resolved by the overlap-receiving command which makes the system receive overlapped digits. When a system uses the overlap-receiving command, the system may need additional configuration such as timeouts interdigit or decision limit.

Configuring ISDN: Calling Number

A router with an ISDN BRI interface might need to supply the ISDN network with a billing number for outgoing calls. Some networks offer better pricing on calls in which the number is present. When configured, this information is included in the outgoing call Setup message. To configure the interface to identify the billing number, use the following command in interface configuration mode:

Step	Command	Purpose
1	configure terminal	Configures to set up bundle.
2	interface bundle <i>bundle-name</i>	Sets up bundle name.
3	link bri slot/sub- <i>slot/port:timeslot</i>	Sets up the pertinent physical link.
4	isdn	Sets up ISDN.
5	switch-type switch-type	Sets up the pertinent switch-type with the content like the following table.
6	incoming-voice	Sets up for voice.
7	calling-number calling- <i>number</i>	Specifies the calling party number.
8	activate	Activates ISDN.
9	exit	-
10	voice-port slot/sub- <i>slot/port</i>	Configures to set up voice port.
11	no shutdown	Turns on the port.

Configuring ISDN: Sending Complete

Some ISDN switches require that the Sending Complete information element be included in the outgoing Setup message to indicate that the entire number is included.



NOTE

If a system takes too long to make a call connection after dial, the system may be configured to wait a specific time from the last. This command can decrease this wait-time by sending the set-up message with the complete information element.

To configure the interface to include the Sending Complete information element in the outgoing call Setup message, use the following command in interface configuration mode:

Step	Command	Purpose
1	configure terminal	Configures to set up bundle.
2	interface bundle bundle-name	Sets up bundle name.
3	link bri slot/sub- slot/port:timeslot	Sets up the pertinent physical link.
4	isdn	Sets up ISDN.
5	switch-type switch-type	Sets up the pertinent switch-type with contents like the following table.
6	incoming-voice	Sets up for voice.
7	sending-complete	Includes the Sending Complete information element in the outgoing call Setup message...
8	activate	Activates ISDN.
9	exit	-
10	voice-port slot/sub-slot/port	Configures to set up voice port.
11	no shutdown	Turns on the port.

Configuring ISDN: tei-mode

To choose the ISDN interface bundle with static-TEI or automatic TEI, use the following command in interface configuration mode:

Step	Command	Purpose
1	configure terminal	Configures to set up bundle.
2	interface bundle <i>bundle-name</i>	Sets up bundle name.
3	link bri slot/sub- slot/port :timeslot	Sets up the pertinent physical link.
4	Isdn	Sets up ISDN.
5	switch-type switch- type	Sets up the pertinent switch-type with contents like the following table.
6	incoming-voice	Sets up for voice.
7	Tei-mode <i>tei_mode</i>	Configures ISDN BRI operation as point-to-point (static TEI) or point-to-multipoint (automatic TEI).
8-1	Tei-value <i>tei_value</i>	(point-to-point) Configures a static ISDN terminal endpoint identifier (TEI). <0-64>
8-2	Spid1 spid1-number Spid2 spid2-number	(point-to-multipoint) Specifies a SPID1 and SPID2.
9	Activate	Activates ISDN.
10	Exit	-
11	voice-port slot/sub- slot/port	Configures to set up voice port.
12	no shutdown	Turns on the port.

Configuring ISDN: spid1, spid2

Some service providers use SPIDs to define the services subscribed to by the ISDN device that is accessing the ISDN service provider. The service provider assigns the ISDN device one or more SPIDs when you first subscribe to the service. If you are using a service provider that requires SPIDs, your ISDN device cannot place or receive calls until it sends a valid SPID to the service provider when accessing the switch to initialize the connection.

Currently, only the DMS-100 and NI switch types require SPIDs. The AT & T 5ESS switch type may support a SPID, but we recommend that you set up that ISDN service without SPIDs.

To configure the spid1, spid2, use the following command in interface configuration mode:

Step	Command	Purpose
1	configure terminal	Configures to set up bundle.
2	interface bundle bundle-name	Sets up bundle name.
3	link bri slot/sub- slot/port :timeslot	Sets up the pertinent physical link.
4	Isdn	Sets up ISDN.
5	switch-type switch- type	Sets up the pertinent switch-type with contents like the following table.
6	incoming-voice	Sets up for voice.
7	sendling-complete	Includes the Sending Complete information element in the outgoing call Setup message...
8	Spid1 spid1-number	Specifies a SPID1 for the B1 channel.
9	Spid2 spid2-number	Specifies a SPID2 for the B2 channel.
10	Activate	Activates ISDN.
11	Exit	-
12	voice-port slot/sub- slot/port	Configures to set up voice port.
13	no shutdown	Turns on the port.

Configuration Example

The following example shows the commands used to configure the ISDN BRI.

```
Router# configure terminal
Router/configure# interface bundle bri000
Router/configure/interface/bundle bri000# link bri 0/0/0:2
Router/configure/interface/bundle bri000# isdn
Router/configure/interface/bundle bri000/isdn# switch-type
basic-ni
Router/configure/interface/bundle bri000/isdn# side USR
Router/configure/interface/bundle bri000/isdn# incoming-voice
Router/configure/interface/bundle bri000/isdn# tei-mode
point-to-multipoint
Router/configure/interface/bundle bri000/isdn# spid1
14085552001
Router/configure/interface/bundle bri000/isdn# spid2
14085552002
Router/configure/interface/bundle bri000/isdn# activate
[warning] 0/0/0 : Voice device driver will be changed after
"no shutdown" command
Router/configure/interface/bundle bri000/isdn# exit
Router/configure/interface/bundle bri000# exit
Router/configure/interface# voice-port 0/0/0
Router/configure/voice-port (0/2/0)# no shutdown
up bri link 0/2/0
Router/configure/voice-port (0/2/0)# end
Router#
```

Monitoring and Maintaining ISDN Interfaces

Command	Purpose
show isdn interface <i>WORD</i>	Displays the ISDN interface information. <pre> Router# show isdn interface ISDN Information: bri000 ----- caller - answer1 - answer2 - called-number - spid1 - spid2 - idle-timeout 5 connect delay 15 keep-alive 10000 disconnect-cause 17 switch-type basic-dms tei-mode point-to-multipoint </pre>
show isdn interfaces	Displays the ISDN interface information. <pre> Router# show isdn interfaces ISDN Information: bri000 ----- caller - answer1 - answer2 - called-number - spid1 - spid2 - idle-timeout 5 connect delay 15 keep-alive 10000 disconnect-cause 17 switch-type basic-dms tei-mode point-to-multipoint Press any key to continue (q : quit enter : next line) : </pre>

(Continued)

Command	Purpose
show isdn status <i>WORD</i>	Displays the ISDN Line Status. <pre> Router# show isdn status bri000 ==== NETWORK side configuration === Layer 1 Status: NOT ACTIVE Layer 2 Status: NOT ACTIVE TEI MODE MULTIPPOINT Layer 3 Status: 0 Active Calls </pre>
show isdn bri-statistics <i>WORD</i>	Displays the ISDN BRI statistics. <pre> Router# show isdn bri-statistics bri000 ----- HDLC Statistics for D Channel ----- GT0: rx packet counter 0 GT0: rx Byte counter 0 GT0: rx chRxErr counter 0 GT0: rx crc counter 0 GT0: rx abort counter 0 GT0: rx chainedError counter 0 GT0: rx all error counter 0 GT0: tx packet counter 73347 GT0: tx Byte counter 586761 GT0: tx packet request 73347 GT0: tx packet request error 0 GT0: tx packet release 73347 GT0: tx packet stop release 0 GT0: tx packet redo release 0 </pre>

(Continued)

Command	Purpose
show isdn global	Displays the ISDN global information. <pre> Router# show isdn global ISDN Global Configuration ----- Basic Rate Interface Switch Type: basic-5ess Tei Mode : Point to Point Tei value for Point to Point : 0 Side : USR Primary Rate interface Switch Type: primary-5ess Tei value for Point to Point : 0 Side : USR </pre>

Troubleshooting ISDN Interfaces

Command	Purpose
debug isdn q921 WORD	Checks Layer 2.
debug isdn q931 WORD	Checks Layer 3.
debug isdn q921-timers WORD	Displays q921 timers. <pre> Router# show isdn q921-timers bri000 ISDN Layer 2 Timer Values K = 7 Outstanding I Frames N200 = 3 Max number of retransmission of a frame N203 = 260 Max number of TEI notification retransmits T200 = 2 Seconds T203 = 10 Seconds </pre>

(Continued)

Command	Purpose
debug isdn q931-timers WORD	Displays q931 timers. <pre>Router# show isdn q931-timers bri000 ISDN Layer 3 Timer Values T303 = 4 Seconds T304 = 30 Seconds T305 = 30 Seconds T308 = 4 Seconds T310 = 40 Seconds T313 = 4 Seconds T316 = 120 Seconds T319 = 4 Seconds T322 = 4 Seconds</pre>
debug isdn q931Statistics WORD	Displays q931 statistics. <pre>Router# show isdn q931Statistics bri000 ISDN Global Configuration Setup Tx : 0 Setup Ack Tx : 0 Alert Tx : 0 Call P Tx : 0 Conn Tx : 0 Con Ack Tx : 0 Prog Tx : 0 Disc Tx : 0 Rel Tx : 0 Rel Cmp Tx : 0 Stat Tx : 0 Stat Enq Tx : 0 Info Tx : 0 Stat Enq Tx : 0 Stat Enq Tx : 0 Setup Rx : 0 Setup AckRx : 0 Alert Rx : 0 Call P Rx : 0 Conn Rx : 0</pre>

(Continued)

Command	Purpose
debug isdn q931Statistics WORD	Con Ack Rx : 0 Prog Rx : 0 Disc Rx : 0 Rel Rx : 0 Rel Cmp Rx : 0 Stat Rx : 0 Stat Enq Rx : 0 Info Rx : 0 Stat Enq Rx : 0 Stat Enq Rx : 0
debug isdn q921Statistics WORD	Displays q921 statistics. Router# show isdn q921Statistics bri000 Inf Tx : 0 RR Tx : 10036 RNR Tx : 0 REJ Tx : 0 SABM Tx : 2 DISC Tx : 0 UA Tx : 0 DM Tx : 0 FRMR Tx : 0 XID Tx : 0 UI Tx : 0 Inf Rx : 0 RR Rx : 10036 RNR Rx : 0 REJ Rx : 0 SABM Rx : 0 DISC Rx : 0 UA Rx : 1 DM Rx : 0 FRMR Rx : 0 XID Rx : 0 UI Rx : 0 INV Rx : 0 SAB Er Rx : 0 FRMR Er Rx : 0

Troubleshooting ISDN interfaces Example

The following example shows the commands used to display the information of the configured ISDN bundle.

```
Router# show isdn interface bri000
ISDN Information: bri000
-----
caller          -
answer1         -
answer2         -
called-number   -
spid1           -
spid2           -
idle-timeout    5
connect delay   15
keep-alive      10000
disconnect-cause 17
switch-type     basic-euro
side            USR
tei-mode        point-to-point
```

The following example shows the commands used to display the ISDN bundle status information. This example shows the ACTIVE status of the PRI bundle. This command lets us know which layer is in ACTIVE state or not.

```
Router# show isdn interface pri001
iBG-04# show isdn status pri10
== USER (0/0/1) side configuration ==
Layer 1 Status:
ACTIVE
Physical interface type is BRI-ST(TE side)
Current NR1 Status [0/0/0] = 9
FULLY ACTIVATED
NO ERROR INDICATION
NO MULTIFRAME DETECTION
SUPERFRAME SYNC
Layer 2 Status:
ACTIVE TEI MODE POINT-TO-POINT
Layer 3 Status:
4 Active Calls
```

The following example shows the Q931 debug messages on the ISDN interface. (see Figure 5.1 ISDN call flow.)

```
Router# debug isdn q931 bri000
-- 18:53:04.240() -- T --> N (Q931,11) --
MSG      : SETUP
MSGHDR   : 08 01 02 05
BEARCAP  : 04 03 80 90 a3
CHANID   : 18 01 89
PROGIND  : 1e 02 81 88
CGPTYNMB : 6c 09 00 80 37 30 30 36 30 30 30
CDPTYNMB : 70 08 80 35 35 35 33 30 30 30

-- 18:53:04.660() -- N --> T (Q931,11) --
MSG      : CALLPROC
MSGHDR   : 08 01 82 02
CHANID   : 18 01 89

-- 18:53:04.970() -- N --> T (Q931,11) --
MSG      : ALERTING
MSGHDR   : 08 01 82 01
CHANID   : 18 01 89

-- 18:53:09.440() -- N --> T (Q931,11) --
MSG      : CONNECT
MSGHDR   : 08 01 82 07

-- 18:53:09.440() -- T --> N (Q931,11) --
MSG      : CONNACK
MSGHDR   : 08 01 02 0f

-- 18:53:30.880() -- T --> N (Q931,11) --
MSG      : DISC
MSGHDR   : 08 01 02 45
CAUSE    : 08 02 80 90

-- 18:53:31.260() -- N --> T (Q931,11) --
MSG      : RELEASE
MSGHDR   : 08 01 82 4d
CAUSE    : 08 02 80 90

-- 18:53:31.260() -- T --> N (Q931,11) --
MSG      : RELCMPLT
MSGHDR   : 08 01 02 5a
CAUSE    : 08 02 80 90
```

Message Direction

This example shows the direction field of the ISDN Q931 Message. When the direction field is displayed 'T → N', it means that the ISDN message is transmitted from this Gateway to the ISDN network. Likewise, if the direction field is displayed 'N → T' it means that the ISDN message is received from the ISDN network to this Gateway. Following example shows that the SETUP message is transmitted from the Gateway to the network side (or ISDN switch) of the ISDN interface.

```
-- 18:53:04.240() -- T --> N (Q931,11) --
MSG      : SETUP
MSGHDR   : 08 01 02 05
BEARCAP  : 04 03 80 90 a3
CHANID   : 18 01 89
PROGIND  : 1e 02 81 88
CGPTYNMB : 6c 09 00 80 37 30 30 36 30 30 30
CDPTYNMB : 70 08 80 35 35 35 33 30 30 30
```

Calling party number and Called party number

The following example shows the calling party number (CGPTYNMB) and called party number (CDPTYNMB) on Q931 messages. The purpose of these information elements is to identify the calling party and called party of a call. In this example, The calling party number is 700-6000 and the called party number is 5553000.

```
-- 18:53:04.240() -- T --> N (Q931,11) --
MSG      : SETUP
MSGHDR   : 08 01 02 05
BEARCAP  : 04 03 80 90 a3
CHANID   : 18 01 89
PROGIND  : 1e 02 81 88
CGPTYNMB : 6c 09 00 80 37 30 30 36 30 30 30
CDPTYNMB : 70 08 80 35 35 35 33 30 30 30
```

Progress Indicator

The following example shows the Progress indicator information element. The purpose of the Progress indicator information element is to describe an event which has occurred during the life of a call. In this example, The progress description value is 8. The meaning of progress description value is described in the table below.

```
-- 18:53:04.240() -- T --> N (Q931,11) --
MSG      : SETUP
MSGHDR   : 08 01 02 05
BEARCAP  : 04 03 80 90 a3
CHANID   : 18 01 89
PROGIND  : 1e 02 81 88
CGPTYNMB : 6c 09 00 80 37 30 30 36 30 30 30
CDPTYNMB : 70 08 80 35 35 35 33 30 30 30
```

Value	Mean
1	Call is not end-to-end ISDN; further call progress information may be available in-band
2	Destination address is non-ISDN
3	Origination address is non-ISDN
4	Call has returned to the ISDN
5	Interworking has occurred and has resulted in a telecommunication service change
8	In-band information or an appropriate pattern is now available
All others	Reserved

Calling party number and Called party number

The following example shows the calling party number (CGPTYNMB) and called party number (CDPTYNMB) on Q931 messages. The purpose of these information elements is to identify the calling party and called party of a call. In this example, The calling party number is 700-6000 and the called party number is 5553000.

```
-- 18:53:04.240() -- T --> N (Q931,11) --
MSG      : SETUP
MSGHDR   : 08 01 02 05
BEARCAP  : 04 03 80 90 a3
CHANID   : 18 01 89
PROGIND  : 1e 02 81 88
CGPTYNMB : 6c 09 00 80 37 30 30 36 30 30 30
CDPTYNMB : 70 08 80 35 35 35 33 30 30 30
```

Progress Indicator

The following example shows the Progress indicator information element. The purpose of the Progress indicator information element is to describe an event which has occurred during the life of a call. In this example, the progress description value is 8. The meaning of the progress description value is described in the table below.

```
-- 18:53:04.240() -- T --> N (Q931,11) --
MSG      : SETUP
MSGHDR   : 08 01 02 05
BEARCAP  : 04 03 80 90 a3
CHANID   : 18 01 89
PROGIND  : 1e 02 81 88
CGPTYNMB : 6c 09 00 80 37 30 30 36 30 30 30
CDPTYNMB : 70 08 80 35 35 35 33 30 30 30
```

Value	Mean
1	Call is not end-to-end ISDN; further call progress information may be available in-band
2	Destination address is non-ISDN
3	Origination address is non-ISDN
4	Call has returned to the ISDN
5	Interworking has occurred and has resulted in a telecommunication service change
8	In-band information or an appropriate pattern is now available
All others	Reserved

Configuring ISDN PRI

Requirements

Prerequisites

Before you attempt this configuration, make sure that you meet these prerequisites:

- If the router will be the only device attached to the PRI, ask for point-to-point service and a data-only line.
- If the router will be attached to an ISDN bus (to which other ISDN devices might be attached), ask for point-to-multipoint service and a voice-and-data line.

Configuration Steps

- Create interface bundle to manage the bundle channels on the PRI-**'bundle'**
- Configure ISDN switch type.
- Configure Voice type.
- Activate the ISDN.
- Delete the ISDN.
- Optional Configuration ISDN.

Create interface bundle

To create interface bundle for th PRI.

Step	Command	Purpose
1	configure terminal	Configures to set up bundle.
2	interface bundle bundle-name	Sets up bundle name.
3	link [pri_t1 pri_e1] slot/sub- slot/port:timeslot	Sets up the pertinent physical link.

Configuring the ISDN PRI Switch

To configure the switch type, use the following command.

Step	Command	Purpose
1	configure terminal	Configures to set up bundle.
2	interface bundle <i>bundle-name</i>	Sets up bundle name.
3	link [pri_e1 pri_t1] <i>slot/sub-</i> <i>slot/port:timeslot</i>	Sets up the pertinent physical link. (slot/subslot/port:*timeslots)
4	isdn	Sets up ISDN.
5	switch-type switch-type	Sets up the pertinent switch-type with the content like the following table 36.2.

*timeslots: E1 PRI is 1 to 31, T1 PRI is 1 to 24.

Table 7.2 switch-type parameter description (PRI)

Switch Type Keywords	Description
Primary-4ess	AT & T Primary Rate Switch Type
Primary-5ess	AT & T Primary Rate Switch Type (default)
Primary-dms250	DMS250 Primary Rate Switch Type
Primary-dms100	DMS100 Primary Rate Switch Type
Primary-ntt	NTT Primary Rate Switch Type
Primary-qsig	Q Signaling Primary Rate Switch Type (only user (slave) side)
Primary-ni2	National ISDN 2 Primary Rate Switch Type
Primary-euro	Euro ISDN Primary Rate Switch Type
Primary-ccitt	CCITT/ITU-T Primary Rate Switch Type

Configuring Voice type

To configure the voice type, use the following command:

Step	Command	Purpose
1	configure terminal	Configures to set up bundle.
2	interface bundle <i>bundle-name</i>	Sets up bundle name.
3	link [pri_t1 pri_e1] slot/sub-slot/port:timeslot	Sets up the pertinent physical link.
4	isdn	Sets up ISDN.
5	switch-type <i>switch-type</i>	Sets up the pertinent switch-type with content like the following table.
6	incoming-voice	Sets up for voice.

Activate the ISDN

To activate the ISDN, use the following command.

Step	Command	Purpose
1	configure terminal	Configures to set up bundle.
2	interface bundle <i>bundle-name</i>	Sets up bundle name.
3	link [pri_t1 pri_e1] slot/sub-slot/port:timeslot	Sets up the pertinent physical link.
4	isdn	Sets up ISDN.
5	switch-type <i>switch-type</i>	Sets up the pertinent switch-type with the content like the following table.
6	incoming-voice	Sets up for voice.
7	activate	Activate ISDN.
8	exit	-
9	voice-port slot/sub-slot/port:D	Configure to set up voice port.
10	no shutdown	Turns on the port.

Delete the ISDN

To delete the ISDN, use the following command

Step	Command	Purpose
1	configure terminal	Configures to set up bundle.
2	voice-port <i>slot/sub-slot/port:D</i>	Configures to set up voice-port.
3	shutdown	Shutdown voice port..
4	no interface bundle <i>WORD</i>	Delete interface bundle.



NOTE

When an existing ISDN interface bundle used for voice (configured 'incoming-voice') is configured, the ISDN voice-port should be shutdown before the ISDN bundle is deleted or 'no activate'.

Configuring ISDN: Overlap-receiving

A system should be configured with these commands to allow the router to wait for all the digits to be received before the call is routed. To enable this feature, use the following command:

Step	Command	Purpose
1	Configure terminal	Configures to set up bundle.
2	Interface bundle <i>bundle-name</i>	Sets up bundle name.
3	link [pri_t1 pri_e1] <i>slot/sub-slot/port :timeslot</i>	Sets up the pertinent physical link.
4	Isdn	Sets up ISDN.
5	switch-type <i>switch-type</i>	Sets up the pertinent switch-type with the content like the following table.
6	Incoming-voice	Sets up for voice.
7	overlap-receiving	(Optional) Specifies if the interface will do Overlap Receiving. *(note)
8	Activate	Activates ISDN.
9	Exit	-
10	voice-port <i>slot/sub-slot/port:D</i>	Configures to set up voice port.
11	no shutdown	Turns on the port.



When the peer system or switch is using overlap signaling, the system may not receive whole digits of the incoming call, while the system is configured to use enblock signaling. This can be resolved by the overlap-receiving command which makes the system receive overlapped digits. When a system uses the overlap-receiving command, the system may need additional configuration such as timeouts interdigit or decision limit.

Configuring ISDN: Calling Number

A router might need to supply the ISDN network with a billing number for outgoing calls. Some networks offer better pricing on calls in which the number is present. When configured, the calling number information is included in the outgoing Setup message.

To configure the interface to identify the billing number, use the following command in interface configuration mode:

Step	Command	Purpose
1	configure terminal	Configures to set up bundle.
2	interface bundle <i>bundle-name</i>	Sets up bundle name.
3	link [pri_t1 pri_e1] slot/sub-slot/port:timeslot	Sets up the pertinent physical link.
4	isdn	Sets up ISDN.
5	switch-type <i>switch-type</i>	Sets up the pertinent switch-type with the content like the following table.
6	incoming-voice	Sets up for voice.
7	calling-number <i>calling-number</i>	Specifies the calling party number.
8	activate	Activates ISDN.

Configuring ISDN : Sending Complete

Some ISDN switches require that the Sending Complete information element be included in the outgoing Setup message to indicate that the entire number is included.



NOTE

If a system takes too long to make a call connection after dialing, the system may be configured to wait a specific time from the last try. This command can decrease this wait-time by sending set-up message with sending complete information element.

To configure the interface to include the Sending Complete information element in the outgoing call Setup message, use the following command in interface configuration mode:

Step	Command	Purpose
1	configure terminal	Configures to set up bundle.
2	interface bundle <i>bundle-name</i>	Sets up bundle name.
3	link [pri_t1 pri_e1] <i>slot/sub-slot/port:timeslot</i>	Sets up the pertinent physical link.
4	isdn	Sets up ISDN.
5	switch-type <i>switch-type</i>	Sets up the pertinent switch-type with the content like the following table.
6	incoming-voice	Sets up for voice.
7	sendling-complete	Includes the Sending Complete information element in the outgoing call Setup message.
8	activate	Activates ISDN.

Monitoring and Maintaining ISDN Interfaces

Command	Purpose
show isdn interface <i>WORD</i>	Displays the ISDN interface information. <pre> Router# show isdn interface pri000 ISDN Information: pri000 ----- caller - answer1 - answer2 - called-number - spid1 - spid2 - idle-timeout 5 connect delay 15 keep-alive 10000 disconnect-cause 17 switch-type primary-euro side USR tei-mode point-to-point </pre>
show isdn status <i>WORD</i>	Displays the ISDN Line Status. <pre> Router# show isdn status pri000 == USER (0/0/0) side configuration == Layer 1 Status: ACTIVE Layer 2 Status: ACTIVE TEI MODE POINT-TO-POINT Layer 3 Status: 0 Active Calls </pre>

(Continued)

Command	Purpose
show isdn pri-statistics <i>WORD</i>	Displays the ISDN PRI statistics. <pre> Rouer# show isdn pri-statistics pri000 ----- HDLC Statistics for D Channel ----- GT0: rx packet counter 3339 GT0: rx Byte counter 20018 GT0: rx chRxErr counter 0 GT0: rx crc counter 0 GT0: rx abort counter 0 GT0: rx chainedError counter 0 GT0: rx all error counter 0 GT0: tx packet counter 3325 GT0: tx Byte counter 13298 GT0: tx packet request 3325 GT0: tx packet request error 0 GT0: tx packet release 3325 GT0: tx packet stop release 0 GT0: tx packet redo release 0 </pre>
show isdn global	Displays the ISDN global information. <pre> Router# show isdn global ISDN Global Configuration ----- Basic Rate Interface Switch Type: basic-5ess Tei Mode : Point to Point Tei value for Point to Point : 0 Side : USR Primary Rate interface Switch Type: primary-5ess Tei value for Point to Point : 0 Side : USR </pre>

Troubleshooting ISDN Interfaces

Command	Purpose
debug isdn q921 WORD	Checks Layer 2.
debug isdn q931 WORD	Checks Layer 3.
debug isdn q921- timers WORD	Displays q921 timers. <pre> Router# show isdn q921-timers pri000 ISDN Layer 2 Timer Values K = 7 Outstanding I Frames N200 = 3 Max number of retransmission of a frame N203 = 260 Max number of TEI notification retransmits T200 = 2 Seconds T203 = 10 Seconds </pre>
debug isdn q931- timers WORD	Displays q931 timers. <pre> Router# show isdn q931-timers pri000 ISDN Layer 3 Timer Values T303 = 4 Seconds T304 = 30 Seconds T305 = 30 Seconds T308 = 4 Seconds T310 = 40 Seconds T313 = 4 Seconds T316 = 120 Seconds T319 = 4 Seconds T322 = 4 Seconds </pre>

(Continued)

Command	Purpose
debug isdn q931Statistics WORD	Displays q931 statistics. <pre>Router# show isdn q931Statistics pri000 ISDN Global Configuration Setup Tx : 0 Setup Ack Tx : 0 Alert Tx : 0 Call P Tx : 0 Conn Tx : 0 Con Ack Tx : 0 Prog Tx : 0 Disc Tx : 0 Rel Tx : 0 Rel Cmp Tx : 0 Stat Tx : 0 Stat Enq Tx : 0 Info Tx : 0 Stat Enq Tx : 0 Stat Enq Tx : 0 Setup Rx : 0 Setup AckRx : 0 Alert Rx : 0 Call P Rx : 0 Conn Rx : 0 Con Ack Rx : 0 Prog Rx : 0 Disc Rx : 0 Rel Rx : 0 Rel Cmp Rx : 0 Stat Rx : 0 Stat Enq Rx : 0 Info Rx : 0 Stat Enq Rx : 0 Stat Enq Rx : 0</pre>

(Continued)

Command	Purpose
debug isdn q921Statistics WORD	Displays q921 statistics. <pre> Router# show isdn q921Statistics pri000 Inf Tx : 0 RR Tx : 3341 RNR Tx : 0 REJ Tx : 0 SABM Tx : 1 DISC Tx : 0 UA Tx : 1 DM Tx : 0 FRMR Tx : 0 XID Tx : 0 UI Tx : 0 Inf Rx : 0 RR Rx : 3341 RNR Rx : 0 REJ Rx : 0 SABM Rx : 1 DISC Rx : 0 UA Rx : 1 DM Rx : 0 FRMR Rx : 0 XID Rx : 0 UI Rx : 0 INV Rx : 0 SAB Er Rx : 0 FRMR Er Rx : 0 </pre>

Troubleshooting ISDN interfaces Example

The following example shows the commands used to display the information of the configured ISDN bundle.

```
Router# show isdn interface bri000
ISDN Information: pri001
-----
caller          -
answer1         -
answer2         -
called-number   -
spid1           -
spid2           -
idle-timeout    5
connect delay   15
keep-alive      10000
disconnect-cause 17
switch-type     primary-euro
side            USR
tei-mode        point-to-point
```

The following example shows the commands used to display the ISDN bundle status information. This example shows the ACTIVE status of the PRI bundle. This command let us know which layer is in ACTIVE state or not.

```
Router# show isdn interface pri001
iBG-04# show isdn status pri10
== USER (0/0/1) side configuration ==
Layer 1 Status:
ACTIVE
Layer 2 Status:
ACTIVE TEI MODE POINT-TO-POINT
Layer 3 Status:
4 Active Calls
```

The following example shows the Q931 debug messages on the ISDN interface. (see Figure 5.1 ISDN call flow.)

```
Router# debug isdn q931 pri001
-- 18:53:04.240() -- T --> N (Q931,11) --
MSG      : SETUP
MSGHDR   : 08 01 02 05
BEARCAP  : 04 03 80 90 a3
CHANID   : 18 01 89
PROGIND  : 1e 02 81 88
CGPTYNMB : 6c 09 00 80 37 30 30 36 30 30 30
CDPTYNMB : 70 08 80 35 35 35 33 30 30 30

-- 18:53:04.660() -- N --> T (Q931,11) --
MSG      : CALLPROC
MSGHDR   : 08 01 82 02
CHANID   : 18 01 89

-- 18:53:04.970() -- N --> T (Q931,11) --
MSG      : ALERTING
MSGHDR   : 08 01 82 01
CHANID   : 18 01 89

-- 18:53:09.440() -- N --> T (Q931,11) --
MSG      : CONNECT
MSGHDR   : 08 01 82 07

-- 18:53:09.440() -- T --> N (Q931,11) --
MSG      : CONNACK
MSGHDR   : 08 01 02 0f

-- 18:53:30.880() -- T --> N (Q931,11) --
MSG      : DISC
MSGHDR   : 08 01 02 45
CAUSE    : 08 02 80 90

-- 18:53:31.260() -- N --> T (Q931,11) --
MSG      : RELEASE
MSGHDR   : 08 01 82 4d
CAUSE    : 08 02 80 90

-- 18:53:31.260() -- T --> N (Q931,11) --
MSG      : RELCMPLT
MSGHDR   : 08 01 02 5a
CAUSE    : 08 02 80 90
```

Message Direction

This example shows the direction field of the ISDN Q931 Message. When the direction field is displayed 'T → N', it means the ISDN message is transmitted from this Gateway to the ISDN network. Likewise, if the direction field is displayed 'N → T' it means that the ISDN message is received from the ISDN network to this Gateway. The following example shows that the SETUP message is transmitted from the Gateway to the network side (or ISDN switch) of the ISDN interface.

```
-- 18:53:04.240() -- T --> N (Q931,11) --  
MSG      : SETUP  
MSGHDR   : 08 01 02 05  
BEARCAP  : 04 03 80 90 a3  
CHANID   : 18 01 89  
PROGIND  : 1e 02 81 88  
CGPTYNMB : 6c 09 00 80 37 30 30 36 30 30 30  
CDPTYNMB : 70 08 80 35 35 35 33 30 30 30
```

Calling party number and Called party number

The following example shows the calling party number (CGPTYNMB) and called party number (CDPTYNMB) on Q931 messages. The purpose of these information elements is to identify the calling party and called party of a call. In this example, The calling party number is 700-6000 and the called party number is 5553000.

```
-- 18:53:04.240() -- T --> N (Q931,11) --  
MSG      : SETUP  
MSGHDR   : 08 01 02 05  
BEARCAP  : 04 03 80 90 a3  
CHANID   : 18 01 89  
PROGIND  : 1e 02 81 88  
CGPTYNMB : 6c 09 00 80 37 30 30 36 30 30 30  
CDPTYNMB : 70 08 80 35 35 35 33 30 30 30
```

Progress Indicator

The following example shows the Progress indicator information element. The purpose of the Progress indicator information element is to describe an event which has occurred during the life of a call. In this example, the progress description value is 8. The meaning of the progress description value is described in the table below.

```
-- 18:53:04.240() -- T --> N (Q931,11) --
MSG      : SETUP
MSGHDR   : 08 01 02 05
BEARCAP  : 04 03 80 90 a3
CHANID   : 18 01 89
PROGIND  : 1e 02 81 88
CGPTYNMB : 6c 09 00 80 37 30 30 36 30 30 30
CDPTYNMB : 70 08 80 35 35 35 33 30 30 30
```

Value	Mean
1	Call is not end-to-end ISDN; further call progress information may be available in-band
2	Destination address is non-ISDN
3	Origination address is non-ISDN
4	Call has returned to the ISDN
5	Interworking has occurred and has resulted in a telecommunication service change
8	In-band information or an appropriate pattern is now available
All others	Reserved

Calling party number and Called party number

The following example shows the calling party number (CGPTYNMB) and called party number (CDPTYNMB) on Q931 messages. The purpose of these information elements is to identify the calling party and called party of a call. In this example, The calling party number is 700-6000 and the called party number is 5553000.

```
-- 18:53:04.240() -- T --> N (Q931,11) --  
MSG      : SETUP  
MSGHDR   : 08 01 02 05  
BEARCAP  : 04 03 80 90 a3  
CHANID   : 18 01 89  
PROGIND  : 1e 02 81 88  
CGPTYNMB : 6c 09 00 80 37 30 30 36 30 30 30  
CDPTYNMB : 70 08 80 35 35 35 33 30 30 30
```

Progress Indicator

The following example shows the Progress indicator information element. The purpose of the Progress indicator information element is to describe an event which has occurred during the life of a call. In this example, The progress description value is 8. The meaning of progress description value is described in the table below.

```
-- 18:53:04.240() -- T --> N (Q931,11) --  
MSG      : SETUP  
MSGHDR   : 08 01 02 05  
BEARCAP  : 04 03 80 90 a3  
CHANID   : 18 01 89  
PROGIND  : 1e 02 81 88  
CGPTYNMB : 6c 09 00 80 37 30 30 36 30 30 30  
CDPTYNMB : 70 08 80 35 35 35 33 30 30 30
```

Value	Mean
1	Call is not end-to-end ISDN; further call progress information may be available in-band
2	Destination address is non-ISDN
3	Origination address is non-ISDN
4	Call has returned to the ISDN
5	Interworking has occurred and has resulted in a telecommunication service change
8	In-band information or an appropriate pattern is now available
All others	Reserved



CHAPTER 8. Routing and Digit Manipulation

This chapter describes how to implement dial plans by configuring dial peers and using dial peer matching, digit manipulation, access group, trunk-group, PLAR and COR features.

Dial Peer Management

Dial Peer Overview

Configuring dial peer is an important task for establishing dial plan and transmitting voice on packet network. Dial peer is used for defining characters to apply to each call leg in connecting a call and identifying the origination or termination of call.

The call leg is the logical connection between two Ubigate iBG routers or one Ubigate iBG router and a telephony device. One voice call is made up of four call legs. In figure 8.1, it is composed of two call legs from the originating Ubigate iBG router's perspective and two call legs from the terminating Ubigate iBG router's perspective.

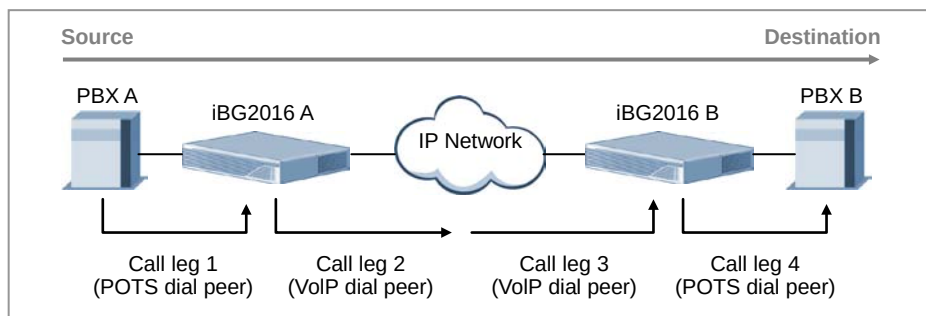


Figure 8.1 Dial Peer Call Legs

A single dial peer is associated with each call leg. In the dial peer, components such as codec, voice activity detection (VAD) and fax rate are defined.

For a voice call, four dial peers like the above figure should be configured.

According to the call leg, a single call is made possible using the following two types of dial peers:

- POTS-dial peer to define characters of PSTN network. Generally, the POTS dial peer connects a particular local PSTN, PBX or telephone voice port and a dialed string.
- VoIP-dial peer to define the necessary components in connecting the packet network. It is the Destination IP address of Ubigate iBG routers.

To connect a voice call through a packet network, both POTS and VoIP dial peers are necessary.

Inbound and Outbound Dial Peers

Dial peer is used in both inbound and outbound call legs. The meaning of Inbound and outbound is defined from the Ubigate iBG router's perspective. When a call enters Ubigate iBG router, an inbound call leg occurs. An outbound call leg occurs when the call exits the Ubigate iBG router.



NOTE

Both figure 33.2 and figure 33.3 are cases that apply to a call through packet network. If the originating and terminating POTS interfaces are in the same Ubigate iBG router, it is sufficient to have two POTS dial peers.

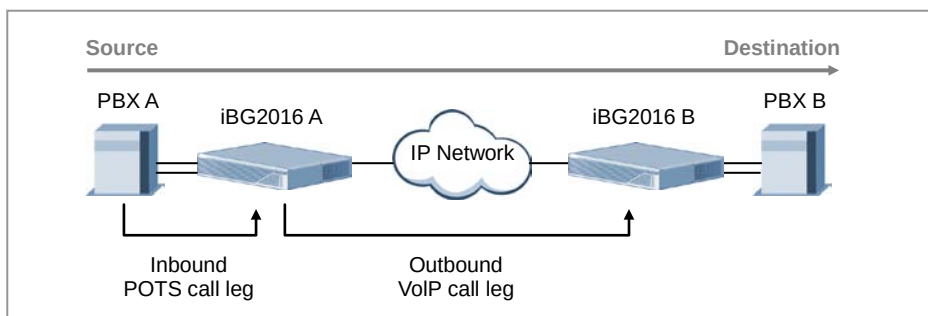


Figure 8.2 Call Legs from the Perspective of the Originating Router

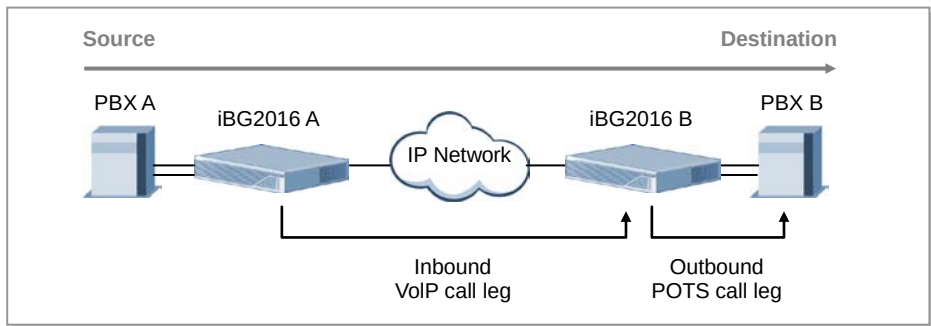


Figure 8.3 Call Legs from the Perspective of the Terminating Router

Ubigate iBG router matches the POTS dial peer with inbound call leg against the incoming call from the POTS interface bound for the packet network. Also it matches the VoIP dial peer with the outbound call leg. Against the incoming call from the packet network, Ubigate iBG router matches the POTS dial peer to make a call and it matches VoIP dial peer with the inbound call leg to apply configuration elements such as a codec.

Matching Inbound Dial Peers

Inbound Dial Peers Elements and Attributes

To match the Inbound call leg with the dial peer, Ubigate iBG router uses three pieces of information in the call setup message. VoIP incoming call uses the IP address and five pieces of configuration information on the dial peer. The three call setup elements are as follows:

- Called number or dialed number identification service (DNIS)-is a series of digit strings, which is derived from the ISDN setup message or CASDNIS representing destination.
- Calling number or dialed number identification service (DNIS)-is a series of digit strings, which is derived from the ISDN setup message or CASDNIS representing destination.
- Voice port-the voice port carrying the call.

Possible configuration information is as follows:

- Incoming called-number-is set up using the digit string. '**incoming-called-number**' dial-peer configuration command representing Called number or DNIS.

- Answer address-used for IP incoming calls and is possible to apply to VoIP dial peer by using a digit string. The '**answer-address**' voip dial-peer configuration command that represents either calling number or ANI.
- Destination pattern-applicable by using the digit string. The '**destination-pattern**' dial-peer configuration command representing the calling number or ANI.



NOTE

When the destination pattern displays calling number, it does inbound dial peer matching.

- Port-displays the that port makes call.
- Session target-The network address of the telephony device or gatekeeper, sip-server.

Inbound Dial Peers Matching Process

Ubigate iBG router tries matching the above information in the following order:

1. **In the case of POTS, VoIP call, called number and incoming-called-number**
2. **In the case of VoIP call, calling number and answer-address**
3. **In the case of POTS, VoIP call, calling number and destination-pattern**
4. Incoming voice port with configured voice port
5. IP address with configured session-target.

The Ubigate iBG router should meet with one condition among the mentioned conditions. To match the dial peer, it is sufficient if a single condition is met.

The Default Dial Peer 0

If there is no condition mentioned above to match, the inbound call leg is automatically matched to the default dial-peer 0. This default dial peer is called **dial-peer 0**.

Inbound VoIP dial peer possesses the following basic information.

- codec: system default codec (g729)
- vad enabled
- fax rate: 14400
- playout-delay mode: system (max: 200 ms, nominal: 80 ms, min: 20 ms)

Matching Outbound Dial Peers

To match the outbound dial peer, use the Ubigate iBG router **destination-pattern** dial peer configuration command.

- When it is a POTS dial peer, input **port** command to transmit call.
- When it is a VoIP dial peer, input session target command to transmit call.

In the case of a POTS incoming call, Ubigate iBG router selects the outbound dial peer based on whether it is DID of the inbound POTS dial peer.

Both cases support longest matching.

DID (Direct Inward Dial) Case

In the DID call characteristic of One-stage dialing, set-up message includes all digits necessary to route call. Ubigate iBG router does not collect additional digits. Ubigate iBG router tries to do matching by using all incoming digit strings.

Non-DID Case

This case is also referred to as two-stage dialing. If DID is not configured on the matched incoming dial-peer, the router or gateway enters the digit collection mode (digits are collected inband). Outbound dial peer is matched on a digit-by-digit basis. Ubigate iBG router or gateway try matching until end-of-digit about all registered dial-peer is judged. From them, the dial-peer that is considered the longest match is selected.

Configuring Dial Peers

Configuring Dial Peers for Call Legs

When the call enters Ubigate iBG router, it is necessary to do dial-peer matching for routing. On calls bound to the packet network after entering POTS interface, Ubigate iBG router should match the POTS dial-peer against the inbound call leg. It also should match the VoIP dial-peer against the outbound call leg. For VoIP incoming calls the case is the opposite.

Figure 8.4 shows the call legs and associated dial peers necessary to complete a voice call.

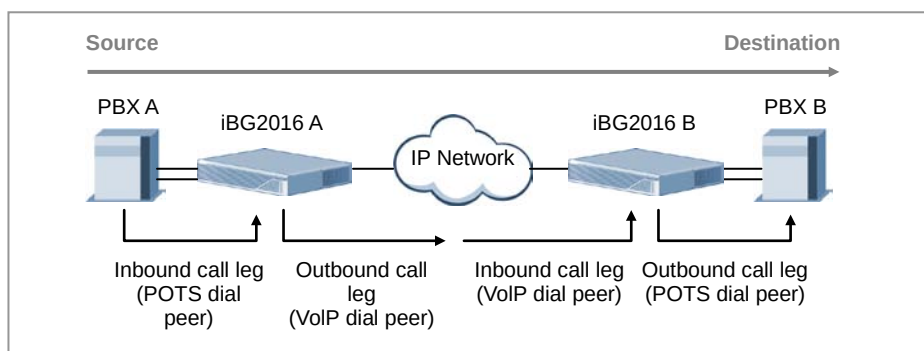


Figure 8.4 Matching Call Legs to Dial Peers

The following example shows the example of a possible call made from number 0315854000 to 0234381000.

Figure 8.5 shows the inbound POTS dial peer and outbound VoIP dial peer set in the originating Ubigate iBG router. POTS dial peer displays the origination of the call after being matched to either calling-number or port information. On the other hand, VoIP dial peer displays the termination of the call by connecting with the called number and session target.

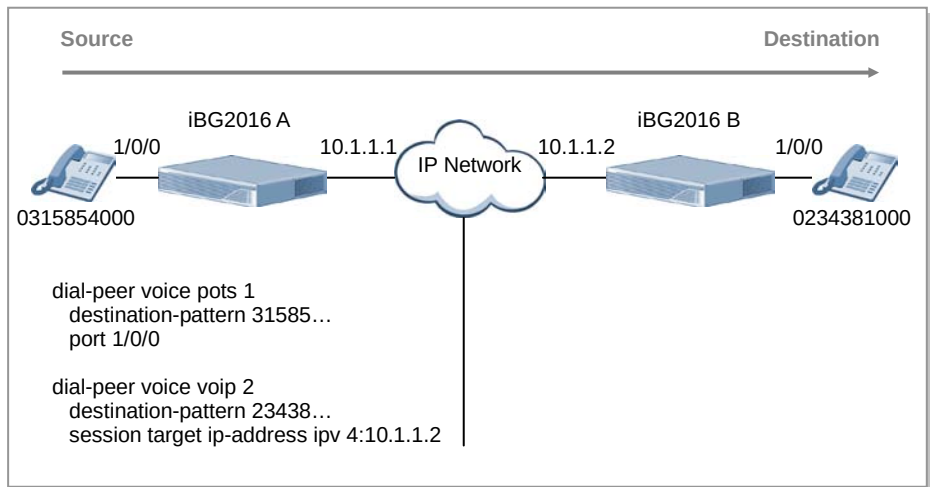


Figure 8.5 Dial Peers from the Perspective of the Originating Ubigate iBG router

Set in compliance with the dialing convention in each region.

Figure 8.6 displays the inbound VoIP dial peer and outbound POTS dial peer in termination at Ubigate iBG router.

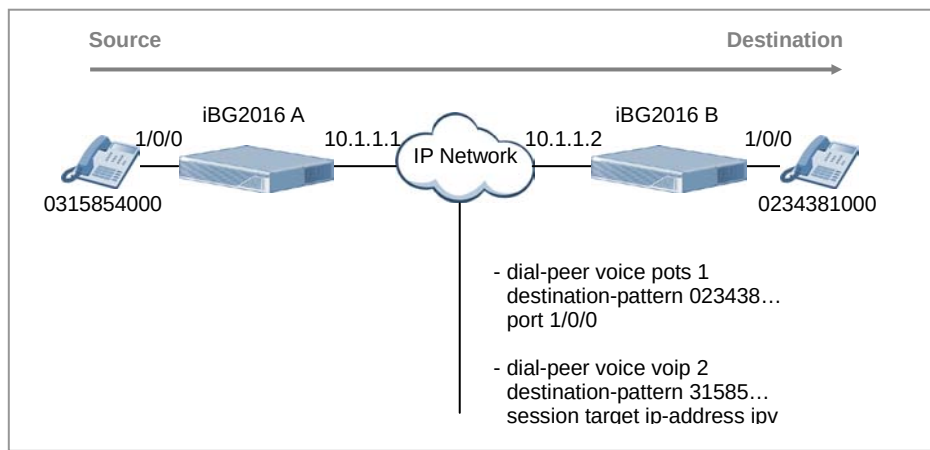


Figure 8.6 Dial Peers from the Perspective of the Terminating Ubigate iBG router

The above setup information shows that in the Ubigate iBG router B VoIP dial peer the last four digits of the destination pattern is replaced as wild card. This means that a call with ITU-T Recommendation P. digit number starting with '023438' in Ubigate iBG router A is possible with Ubigate iBG router B.

**NOTE**

It does not always need Inbound dial peer. If dial peer configured against Inbound call leg does not match, use the already defined default dial peer as inbound dial peer. Dial peer 2 of Ubigate iBG router B in the figure 33.6 is necessary when call is tried with A only in Ubigate iBG router B.

The only exception to the above examples is the case of sharing the same Ubigate iBG router by two POTS dial peers as in Figure 8.7. In that case, it is not necessary to configure the VoIP dial peer.

This case is similar to hairpinning which is the status of being detoured to PSTN after a call bound to the packet network becomes an impossible condition in terms of packet network.

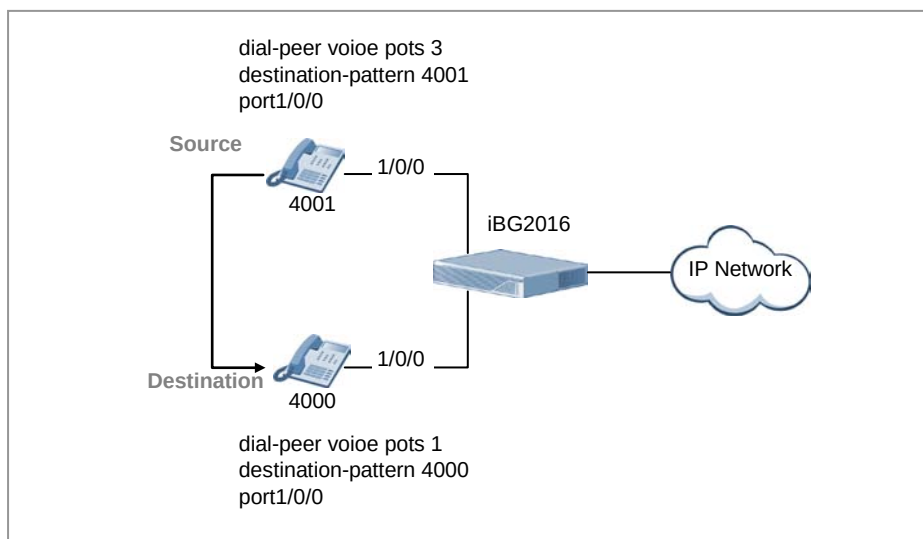


Figure 8.7 Communication Between Dial Peers Sharing the Same Ubigate iBG router

Configuring POTS Dial Peers

To configure the POTS dial peer, the following should be done:

- Assign dial peer with the tag number only.
- Determine termination telephone number and number domain.
- Assign voice port where the call occurs.

In most cases, it is sufficient to connect the call with the basic value of the POTS dial peer configuration command except in the above setup.

To configure the POTS dial peer, use the following command starting in the global configuration mode:

- Configuration Steps
 - configure terminal
 - dial-peer voice pots <num>
 - destination-pattern <digit-string>
 - port <string>
 - exit
- Detailed Steps

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters global configuration mode.
2	dial-peer voice pots <i>num</i> Example) sbm/configure# dial-peer voice pots 10	Enters dial-peer configuration mode and defines a local dial peer that connects to a POTS interface. The <i>number</i> argument is one or more digits identifying the dial peer. Valid entries are from 1 to 10000.
3	destination-pattern [+]string[T]	Matches dialed digits to a telephony device. The <i>string</i> argument is a series of digits that specify the E.164 or private dialing plan telephone number. Valid entries are the numbers 0 through 9. You can also enter the following special characters: - The asterisk (*) or pound sign (#) on standard touch-tone dial pads can be used anywhere in the pattern. - The period (.) acts as a wildcard character.

(Continued)

Step	Command	Purpose
3	Example) sbm/configure/.../pots num# destination-pattern 0234389...	When the timer (T) character is included at the end of the destination pattern, the router collects dialed digits until the interdigit timer expires (5 seconds, by default) or until you dial the termination character (the default is #). The timer character must be a capital T.
4	port <i>string</i> Example) sbm/configure/.../pots num# port 0/0/1	Maps the dial peer to a specific logical interface. The port command syntax is platform-specific.

Configuring Dial Plan Options for POTS Dial Peers

When the dial plan is configured, the different option values should be applied depending on how the dial plan is configured.

To configure the optional feature for the POTS dial peer, see the following command.

Command	Purpose
incoming-called-number Example) sbm/configure/.../pots num# incoming-called-number 3438....	(Optional) Selects the inbound dial peer based on the called number.
direct-inward-dial Example) sbm/configure/.../pots num# direct-inward-dial	(Optional) Enables the Direct Inward Dialing (DID) call treatment for the incoming called number.
forward-digit {all default extra num <i>num</i> } Example) sbm/configure/.../pots num# forward-digit all	(Optional) Configures the digit-forwarding method used by the dial peer. The valid range for the number of digits forwarded (<i>num-digit</i>) is 0 through 32.

(Continued)

Command	Purpose
max-call <i>num</i> Example) sbm/configure/.../pots <i>num</i> # max-call <i>10</i>	(Optional) Specifies the maximum number of allowed connections to and from the POTS dial peer. The valid range is 1 through 256.
preference <i>num</i> Example) sbm/configure.../pots <i>num</i> # preference 1	(Optional) Configures a preference for the POTS dial peer. The valid range is 0 through 10, where the lower the number, the higher the preference.
prefix <i>num</i> Example) sbm/configure.../pots <i>num</i> # prefix <i>string</i>	(Optional) Includes a prefix that the system adds automatically to the front of the dial string before passing it to the telephony interface. Valid entries for the <i>string</i> argument are 0 through 9.

Configuring VoIP Dial Peers

VoIP dial peer makes a call with the particular Ubigate iBG router telephony device possible.

To set VoIP dial peer, the following should be done:

- Assign dial peer with the tag number only.
- Define termination telephone number.
- Define termination IP-address.

Like the POTS dial peer, the default value of other cli is sufficient to make a call with in most environments.

To configure VoIP dial peer, use the following command starting in the global configuration mode.

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters global configuration mode.
2	dia-peer voice voip 11 Example) sbm/configure# dial-peer voice voip <i>number</i>	Enters the dial-peer configuration mode and defines a remote VoIP dial peer. The <i>number</i> argument is one or more digits identifying the dial peer. Valid entries are from 1 to 10000. The VoIP keyword indicates a dial peer using voice encapsulation on the IP network.
3	destination-pattern [+]string[T] Example) sbm/configure/.../pots <i>num</i> # destination-pattern 0234389...	Matches dialed digits to a telephony device. The <i>string</i> argument is a series of digits that specify the E.164 or private dialing plan telephone number. Valid entries are the numbers 0 through 9. You can also enter the following special characters: - The asterisk (*) or pound sign (#) on standard touch-tone dial pads can be used anywhere in the pattern. - The period (.) acts as a wildcard character. When the timer (T) character is included at the end of the destination pattern, the router collects dialed digits until the interdigit timer expires (5 seconds, by default) or until you dial the termination. character (the default is #). The timer character must be a capital T.
4	session-target { ip-address { ipv4: <i>ip-address</i> [: <i>port</i>] ipv6: <i>ip-address</i> [: <i>port</i>] dns: <i>userid</i> @ <i>hostname</i> [: <i>port</i>] } sip-server gatekeeper } Example) sbm/configure/.../voip <i>num</i> # session-target ip-address ipv4:10.10.10.10	Defines the IP address of the router that is connected to the remote telephony device. The IPv4: <i>destination-address</i> , IPv6: <i>destination-address</i> keyword and argument indicate the IP address of the remote router. The dns: <i>host-name</i> keyword and argument indicate that the domain name server will resolve the name of the IP address. Valid entries for this parameter are characters representing the name of the host device.

(Continued)

Step	Command	Purpose
5	<pre>codec { g711alaw g711ulaw g723r53 g723r63 g726 g729 } [ptime] Example) sbm/configure/.../voip num# codec g711alaw</pre>	Defines the codec for the dial peer. Ptime means the time between frames transmitted. The unit is ms and has the value among 10/20/30/40/50/60 (g711alaw, g711ulaw, g726, g729), 30/60 (g723r53, g723r63)

Configuring Codec Selection Order

The VoIP dial-peer can possess the system codec list. System codec list is the list including only g729. Both the codec and codec-list can be designated in dial-peer and the codec list gets priority.

Designating the codec order in the Voice class creates the list. It is possible to designate this list with either a dial-peer or system codec list.

The method to make a codec list is as follows:

Setp	Command	Purpose
1	<pre>voice class codec num Example) sbm/configure# voice class codec 1</pre>	Creates a voice class for a codec preference list. The range for the <i>tag</i> number is from 1 through 10000. The number must be unique on the router.
2	<pre>codec-preference prefer-num { g711alaw g711ulaw g723r53 g723r63 g726 g729 } [10/20/30/40/50/60] Example) sbm/configure/.../codec num# codec-preference g711alaw 50</pre>	Configures the order of preference for selecting a codec. Repeat this command to specify the preferred selection order for additional codecs, if required. g723r53, g723r63: 30/60 g711alaw, g711ulaw, g726, g729: 10/20/30/40/50/60

By using 'voice service codec-list' command, set the created voice class codec with the system global codec list. Using the system global codec list, assign the codec list in the dial-peer.

Configuring Voice Class Sip/H323

The voice class that you assign to the dial peer must be configured using the **voice-class sip/h323** in the global configuration mode. You can assign one voice class to each VoIP dial peer. If you assign another voice class to a dial peer, the last voice class assigned replaces the previous voice class.

The following are commands that may be configured in ‘voice class sip’ mode.

Command	Purpose
offer call-hold { conn-addr dir-send dir-inact } Example) sbm/configure/voice/class/sip num# offer call-hold conn-addr	(optional) Specifies the call hold request value.
rel1xx { supported require system disable } Example) sbm/configure/voice /class/sip num# rel1xx supported.	(optional) Specifies the rel1xx value.
uri { sip sips } Example) sbm/configure/voice/class/sip num# uri sip	(optional) Specifies the uri value.
url { system sip tel } Example) sbm/configure/voice/class/sip num# url sip	(optional) Specifies the url value.

The following are commands that could be configured in ‘voice class h323’ mode.

Command	Purpose
h225 call-start {fast slow system}	Specifies the H.323 call setup method.
h225 early-h245 {on off system}	Specifies whether to perform the normal H.245 procedure before or after CONNECT message.
h225 h245-tunnel {on off system}	Specifies H.245 Tunneling support.

(Continued)

Command	Purpose
h225 T301 <i>seconds</i>	Maximum time to wait for CONNECT or RELCOMP message, after receiving ALERT message.
h225 T303 <i>seconds</i>	Maximum time to wait for CALLPROCEEDING or ALERTING or PROGRESS or RELCOMP message, after sending SETUP message.

For more information on configuring h323 info, see 3.2.8.

Configuring Dial Plan Options for VoIP Dial Peers

When configuring the dial-plan, different options can be designated depending on which dial-plan is applied.

To configure the optional dial plan feature, use the following command in dial peer configuration mode.

Command	Purpose
incoming-called-number <i>string</i> Example) sbm/configure/.../voip num# incoming-called-number 024....	(Optional) Selects the inbound dial peer based on the called number.
answer-address <i>string</i> Example) sbm/configure/.../voip num# answer-address 2445....	(Optional) Selects the inbound dial peer based on the calling number.
dtmf-relay { inband h245-alphanumeric rtp-nte sip-notify sip-info queued-digits } Example) sbm/configure/.../voip num# dtmf-relay rtp-nte	(Optional) Configures the tone that sounds in response to a keypress on a touch-tone telephone. Dual tone multifrequency (DTMF) tones are compressed at one end of a call and decompressed at the other end.

(Continued)

Command	Purpose
fax rate { 2400 4800 7200 9600 12000 14400 } Example) sbm/configure/.../voip num# fax rate 12000	(Optional) Specifies the transmission speed of a fax to be sent to this dial peer. The 14400 keyword, which is the default, specifies the highest possible transmission speed supported by the voice rate.
playout-delay mode { adaptive fixed [value] system } Example) sbm/configure/.../voip num# playout-delay mode adaptive	(Optional) Specifies the type of jitter buffer playout delay to use.
playout-delay { maximum minimum nominal } <20-200> Example) sbm/configure.../voip num# playout-delay maximum 190	(Optional) Specifies the amount of time that a packet is held in the jitter buffer before it is played out on the audio path.
preference <i>value</i> Example) sbm/configure.../voip num# preference 1	(Optional) Configures a preference for the POTS dial peer. The valid range is 0 through 10, where the lower the number, the higher the preference.
tech-prefix <i>string</i> Example) sbm/configure.../voip num# tech-prefix #34	(Optional) Specifies that a particular technology prefix be prepended to the destination pattern of this dial peer.

Configuring CLID Options for Dial Peers

To control the presentation and use of the calling-line ID (CLID) information, use the **clid** command in dial-peer configuration mode.

Command	Purpose
clid network-number <i>string</i> Example) sbm/configure.../voip <i>num</i> # clid network-number 3345	(Optional) Network number. Establishes the calling-party network number in the CLID for this router.
clid remove [name] Example) sbm/configure.../pots <i>num</i> # clid remove	(optional) Remove the calling-party number and name from the CLID.
clid restrict Example) sbm/configure.../voip <i>num</i> # clid restrict	(Optional) Restricts presentation of the caller ID in the CLID.
clid override rdnis Example) sbm/configure.../pots <i>num</i> # clid override rdnis	(Optional; supported for POTS dial peers only) Overrides the CLID with the redirected dialed number identification service (RDNIS) if available.

Verifying Dial Peers

If you have few dial peers configured, you can use the show dial-peer voice command to verify the validity of your dial-peer configuration.

```
Router/configure# show dial-peer voice all
VoiceEncapPeer701
<<< Dial Peer Common Info >>>
id = 701, type = pots,
description = ``,
admin state = 'up', operation state = 'up',
destination-pattern = `1001..`, answer-address = ``,
preference = 2, numbering type = 'none',
incoming called-number = ``,
connections/maximum = 0/ unlimited,
decision limit number = '3',
huntstop = `disabled`,
incoming COR list = `maximum capability`,
```

```
outgoing COR list = `minimum requirement`,
called translation ruleset id = `0`,
calling translation ruleset id = `0`,
incoming translation profile = `none`,
outgoing translation profile = `none`,
CLID restrict = 'disabled', CLID remove = 'disabled',
CLID remove name = 'disabled',
CLID network number = '', CLID override RDNIS =
'disabled',
call block translation-profile = '',
call block disconnect-cause = 'No Service',

<<< Dial Peer POTS Info >>>
prefix = '',
forward digits = 'default',
direct-inward-dial = 'disabled',
digit strip = 'enabled',
port = '0/1/0',
authentication name = '', passwd = '',
sip registration = 'disable',
trunk group = '0 trunk group is registered'
smime = 'disable',
call waiting = 'disabled', call pickup group id = ''
call forwarding = 'disabled'
    all-number = '',
    busy-number = '',
    no-answer-number = ''
auto-alert = '0',
progress-ind :
    alert = '0', call proceed = '0', connect = '0',
    disconnect = '0', progress = '0',
    setup = '0', setup ack = '0',
progress-ind-locate = 'disable',

<<< Dial Peer Statistics Info >>>
Connect Time = 0 seconds,
In Calls = 3, Out Calls = 0
In Ans Num = 0, Out Ans Num = 0
In Fail Num = 1, Out Fail Num = 0
In Abnormal Term Num = 0, Out Abnormal Term Num = 0
In Abandon Num = 2, Out Abandon Num = 0
Last Disconnect Cause is 'CS_NETWORK_OUT_OF_ORDER',
Last Setup Time = 03/11/2000-04:01:49-680 .
```


Troubleshooting Dial Peers

If you are having trouble connecting a call, you can try to resolve the problem by performing the following tasks:

If you suspect the problem is associated with the dial-peer configuration, use the show dial-peer voice command on the local and remote concentrators to verify that the data is configured correctly on both.

Check the inbound dial-peer and the outbound dial-peer on the call-log. If you want to show the call-log, use the debug call-log command. For more information, refer to iBG_TroubleShootingManual (call connecting failure).

```
Router# debug console
Router# debug call-log all
02:45:54.940()::Call-Log Start
02:45:54.940()::In Dial-Peer=7000 Description=
TS#(322)PORT:0/1/1
02:45:54.940()::Out Dial-Peer=6000 Description=
TS#(323)PORT:0/1/0
02:45:54.940()::Receive CalledNumber=6000
CallingNumber=7000 CallerName=
02:45:54.940()::Forward CalledNumber=
CallingNumber=7000
02:45:54.940()::Account_Sess=22 SystemId=TOP57
CallingPartyCategory=1 CallId=22
02:45:54.940()::Time Attempt =03/29/2000-02:45:48-690
02:45:54.940()::    Setup    =03/29/2000-02:45:52-620
02:45:54.940()::    Alert    =03/29/2000-02:45:52-620
02:45:54.940()::    Answer   =--
02:45:54.940()::    Disconn  =03/29/2000-02:45:54-940
02:45:54.940()::Q850_Cause=16:CS_NORMAL_RELEASE
SipStatusCode=SC_200_Ok
02:45:54.940()::causeType_failCode causeLoc1_cgUser
causeLoc2_oBcc
02:45:54.940()::CCA(13/1)CTX(22)DSP#(21)TS#(322)PORT:0/1/1::
Disc Event(DM_nfHon)HOOK(0)from(PIC_0_Alerting)
02:45:54.940()::PacketUsage:Sent=0 Recv=0 jitterDelay=0
Lost=0
02:45:54.940()::Call-Log End
```

Toggle the voice port and/or serial port by entering shutdown, and then no shutdown.

Verifying and Troubleshooting commands

```
Router# show dial-peer voice summary
Router# show dial-peer voice all
Router# show dial-peer voice num <num>
Router# debug call-log all
```

Configuring Dial Peer Matching Features

Destination Pattern

The destination pattern forms a link with the dialed string and the particular telephony device. It is configured in the dial peer by using the **destination-pattern** command.

If the dialed string matches the destination pattern, the POTS dial peer is routed to the voice port and the VoIP dial peer is routed to the session target. When confronted with the Outbound VoIP dial peer, the destination pattern determines the dialed digit that Ubigate iBG router should collect and transmit. The entire dial peer created in Ubigate iBG router should apply the destination pattern. The destination pattern should have the full telephone number or the partial number together with the wildcard digit (ex: period-'.'). Each '.' represents a single digit in a spontaneous way.

For example, '345' means the spontaneous seven digit string starting with '345'. In addition to period (.), there are various symbols applicable to the destination pattern. These symbols provide flexibility in configuring the dial plan and help to save trouble of creating various dial peers according to the range of telephone numbers.



NOTE

When there is no valid outbound dial-peer for the POTS incoming call, the call processed in the order of sip-server, gatekeeper after the confirmation of configuration.

The following table 8.1 represents various wild cards.

Table 8.1 Wild card Symbol

Symbols	Description
.	Indicates any entered digits.
%	Indicates that the preceding digit occurred zero or more times.
+	Indicates that the preceding digit occurred one or more times.
^	Indicates a match to the beginning of the string.
\	Can be used with a single character with no other significance (matching that character).
?	Indicates that the preceding digit occurred zero or one time.
[]	Indicate a range. A range is a sequence of characters enclosed in the brackets; only numeric characters from 0 to 9 are allowed in the range.
()	Indicate a pattern and is the same as the regular expression rule.



NOTE

The only wild card symbol usable in both answer-address and incoming-called-number is a period (.).

Session Target

Session target is the network address of the remote Ubigate iBG router, to which a call intends to transmit. Set it up in the VoIP dial-peer with the '**session target**' command. The destination-pattern is the telephone number of the telephone attempting to connect in the outbound dial-peer. The session target displays the path of the desired voice device and the connected remote Ubigate iBG router.

Figure 8.8 illustrates the relationship between the destination pattern and the session target, as shown from the perspective of the originating router.

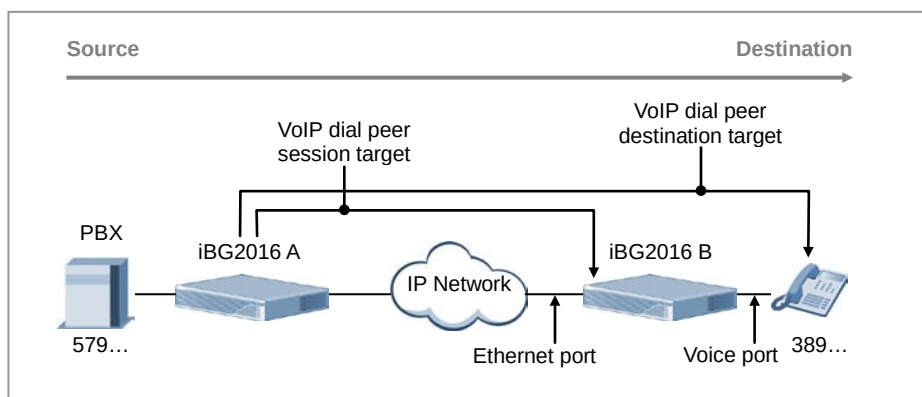


Figure 8.8 Relationship Between Destination Pattern and Session Target

Session target is used for inbound matching. When VoIP incoming does not match due to the number condition, try matching the set session target and the IP address.

VoIP-peer

VoIP-peer has a protocol type and IP-address. To designate a network-specific address to receive calls from a VoIP dial peer in addition to using the **session target ip-address** command, use the **session target name** command in the dial-peer configuration mode. The type of voip-peer should be consistent with the session protocol type of the dial-peer. The Sip-server, gatekeeper can not be configured in VoIP-peer. VoIP-peer could be used in not only dial-peer but also gatekeeper, sip-server, call-server, mwi-server or registrat-server.

The following is an example of the configuration.

```
voip-peer voippeer1 sip
ip-address ipv4:10.254.139.56
```

Incoming Called Number & Answer Address for VoIP

The 'incoming-called-number' command is the top priority to attempt inbound dial-peer matching by comparing the called number of the incoming call.

If a different setup on the call bound for the particular called number is tried, inbound dial-peer matching of the pertinent call is possible by using this command. Even though there is matchable dial-peer, matching according to the condition of incoming called number occurs first.

Answer address attempts dial-peer matching against VoIP incoming call. Top priority applies next to the incoming called number, comparing it with the calling number. If matching does not occur, compare destination-pattern with the calling number. The following dial-peer matches the VoIP call with a calling number of '3091345'.

```
dial-peer voice voip 1
  answer-address 3091345
  session target ip-address ipv4:192.169.10.4
```

DID for POTS Dial Peers

Direct Inward Dialing immediately enables outbound dial peer matching with the called number against the call from the POTS interface. If it is set up in the DID inbound POTS dial-peer, the called number attempts to automatically match with the destination pattern to find the outbound call leg.

If DID is not setup at the moment of the incoming call, Ubigate iBG router transmits a dial tone to the caller and collects additionally numbers to find the outbound dial-peer. This procedure is called two-stage dialing. After selecting the Outbound dial peer, it transmits the call to the set destination in the dial peer. DID immediately enables the outbound call by matching the called number in the dial peer. If DID is set, it does not send a dial tone to the caller or collect additional digits. It immediately sends the call to the configured destination. This is called one-stage dialing.

Hunt Groups and Preferences

Supports the concept of a hunt group against numerous dial peers with the same destination-pattern. With the destination of each POTS dial peer being a single voice port, the hunt group enables the call to be transmitted with another voice port even though the particular voice port is busy.

In the following case, four dial peers from the POTS dial peer 1 to POTS dial peer 4 possess a destination pattern like 5000 and separate ports. In these circumstances, the call should be made possible to other port even though a single port is busy or unavailable.

Router
dial-peer voice pots 1 destination pattern 5000 port 0/0/0 preference 0
dial-peer voice pots 2 destination pattern 5000 port 0/0/1 preference 1
dial-peer voice pots 3 destination pattern 5000 port 0/0/2 preference 2
dial-peer voice pots 4 destination pattern 5000 port 0/0/3 preference 3

If priority should be given between dial peers within the set hunt group, use the preference command. Ubigate iBG router first makes possible the call in terms of the dial peer, which has preference in the hunt group. A low preference number gets higher priority. When the same preference number in the hunt group occurs, it is selected randomly. In the case of the above example, dial peer 1 has priority over 2, 3 and 4 in sequence. Basically, the sequence to hunt within the hunt group is as follows:

1. Longest match in phone number - Destination pattern matches the longest match with dialed digits. For example, a single dial peer has a destination pattern of 123.... and when the other dial peer has 1234567, the latter dial peer is selected. This is because there are clearly more matchable numbers.
2. Priority configured by using the **preference** dial peer command.
3. Random selection.

By using global configuration command called '**dial-peer hunt**', **another method for hunting the dial peer can be selected. As another selective standard, there is** 'least recent use'. This selects the oldest dial-peer in terms of selection.

With basic dial peer hunting being possible, using dial-peer configuration command called 'huntstop' enables one to stop hunting when the call has failed in the particular dial peer.

To select the method of hunting the dial peer, it is possible to use the '**dial-peer hunt**' global configuration command. The content is similar to the following table.

Command	Purpose
sbm/configure# dial-peer hunt hunt-order-num	Set the standard of selecting dial peer within (optional) hunt group. The selection is possible from 0 to 7 and 0 is default value. 0 - longest match in phone number, explicit preference, random selection. 1 - longest match in phone number, explicit preference, least recent use. 2 - explicit preference, longest match in phone number, random selection. 3 - explicit preference, longest match in phone number, least recent use. 4 - Least recent use, longest match in phone number, explicit preference. 5 - Least recent use, explicit preference, longest match in phone number. 6 - Random selection. 7 - Least recent use.

You can configure POTS and VoIP dial peers within a hunt group. If network connectivity fails, you can reroute the calls back through the PBX to the PSTN. This type of configuration is sometimes referred to as *hairpinning* or PSTN fallback. The VoIP dial-peer supports PSTN fallback by default. To disable, use '**no call-fallback port**' command.

Numbering Type Matching

Dial peer checks number type matching in addition to the condition such as the incoming called number, answer address, destination pattern, port and IP-address. It determines the dial-peer number type with the '**numbering-type**' dial-peer configuration command.

The following number type can be used:

- Abbreviated - Abbreviated representation of the complete number as supported by this network.
- International - Number called to reach a subscriber in another country.
- National - Number called to reach a subscriber in the same country, but outside the local network.
- Network - Administrative or service number specific to the serving network.
- Reserved - Reserved for extension.
- Subscriber - Number called to reach a subscriber in the same local network.
- Unknown - Type of number is unknown by the network.

For detailed information about these numbering types, see ITU-T Recommendation Q.931.

Dial Plan Mode

Dial Plan Mode

The dial plan mode is a mode that sets the global configuration for the dial-plan. The Following are commands of the dial-plan mode.

Command	Purpose
cp-tone Example) sbm/configure/dial-plan # cp-tone kr	The cp-tone command is to set the tone voice interface (ring, busy, cadence) for a specific country.
fxs-pattern <i>tag full-fxs-pattern ext-leng ext-pattern</i> Example) sbm/configure/dial-plan # fxs-pattern 1 802343849.. 4 49..	To create a global prefix that can be used to expand the extension numbers for inbound and outbound calls into fully qualified E.164 numbers in toll by pass mode, use the fxs-pattern command. The maximum number that could be configured is 5. Digit and dot (.) could be entered.
max-call <i>num</i> Example) sbm/configure/dial-plan #max-call 512	To set the maximum number of calls that a system can handle, use the max-call command in dial plan configuration mode. Default value is unlimited. Range is from 1 to 10000.
secondary-dialtone <i>string</i> Example) sbm/configure/dial-plan /secondary-dialtone # secondary-dialtone 9	To enable a secondary dial tone, use the secondary-dialtone command. The maximum number that could be configured is 10.

Dialed Number Analysis

Dial Plans

Fixed-Length Dial Plans

Since the length of the telephone number in most cases is already known, a fixed-length dialing plan where all the dial-peers possess the fixed length of the destination-pattern is enough in most voice networks. However, for particular international phones that can be used with different lengths of telephone number need variable-length dial plans.

Variable-Length Dial Plans

Input T-indicator representing timeout at the end of the destination of outbound voice-network dial peer and wait for inputting additional digits after receiving the Ubigate iBG router-fixed length dial string. The timeout letter is a capital 'T'.

The following dial-peer configuration is an example of configuring the T-indicator to enable a variable-length dial string.

dial-peer voice VoIP 1

- destination-pattern 3456T
- session-target ip-address ipv4:10.10.6.8

In the above example, Ubigate iBG router waits to input the additional digit which is undefined after receiving the number 3456. If the inter digit time does not expire, up to the maximum of 31 digits may be input. If inter digit time expires, Ubigate iBG router connects the call.

The basic value of the inter digit timeout is 10 seconds. If this value does not change, it takes 10 seconds of call setup time per each call before the timer runs out. Thus, it is necessary to regulate inter digit time by using the **'timeouts interdigits'** voice-port mode command if users want to use variable-length dial plan.

By inputting '#' or '*', the caller can end inter digit timeout immediately. While '#' or '*' waits to input the additional dial digit, '#' or '*' is recognized as the end character at the moment of input. '#' or '*' character are not recognized as dial digits and are also not transmitted to the opposite PBX. However, if '#' or '*' is input before waiting to enter the additional digits, they are recognized as dialed digits.

Digit Manipulation

Ubigate iBG router may need to manipulate digits in a dial string before it passes the dial string to the telephony device. You may need to consider different strategies for configuring digit manipulation within your dial peers depending on your existing dial plan, the digits users are expected to dial. These digit-manipulation options, in conjunction with the destination pattern, determine the dial string that an iBG router forwards to the telephony device.

Digit Strip and Prefixes

When the Ubigate iBG router on the receiver side matches with the dial string as the outbound POTS dial peer, by default Ubigate iBG router takes out digits matching specifically with the destination pattern. The remaining digits are transmitted to either PBX or PSTN.

But in other circumstances the dial plan applicable to the original digits does not delete the partial digits as above. In this case, it is possible to make the default digit strip execution impossible using the '**no digit-strip**' dial-peer configuration command or enable transmission with the telephony interface by pasting the particular digit using the '**prefix**' dial-peer configuration command. This command is supported only in the POTS dial peer.

The '**no digit-strip**' command prevents the outgoing POTS dial peer from automatically becoming a digit strip. For example, when the configuration is made as in the following, the entire 7 digits including 345 may be transmitted.

dial-peer voice pots 10

- destination-pattern 345...
- no digit-strip
- port 0/1/1:3

Preventing digit strip is useful in the case that telephony interface needs a full dialed string. In terms of dialed digits, the number should be changed in compliance with the particular convention in place in certain circumstances.

Before the '**prefix**' command is transmitted to another telephony device, add the specified digits before the existing digits.

For example, Let's assume that the E.164 called number is 82(02)3438-4968. In the office, the call is made possible by pressing the number 14968, which is the telephone's extension number. If the user sets the destination-pattern with '82023438' in the outbound POTS dial peer which is associated with the telephone, GW strips '82023438' after receiving a call to 82(02)3438-4968. For terminating GW to make a call with the appropriate destination, put a '1' in front of the remaining digit. To do this, the configuration should be as follows:

dial-peer voice pots 20

- destination-pattern 82023438....
- prefix 1
- port 0/1/1:2

Forward Digits

The '**forward-digits**' command regulates the number of digit stripped before the dialed string that transmitted to the other telephony device. Generally, outbound POTS dial peers strips the all digits specifically matchable with the destination-pattern and transmits only the digits matchable in the wildcard pattern. The '**Forward-digits**' command transmits all digits or the fixed number of digit from among the dialed digits regardless of the number of digit clearly matchable to destination pattern.

The '**Forward-digits**' command is supported only in the POTS dial peer.

For example; the '**forward-digits 3**' command transmits the last three digits of the dialed string. The '**Forward-digits all**' command transmits the entire dialed string. The '**Forward-digits all**' command intends to transmit the entire part when the length of dialed digits is greater than that of destination-pattern. In the case in which the destination-pattern of the dial-peer is a variable-length such as '3438...T' and '3438T', it is impossible to transmit.

Number Expansion

In the most business circumstances, the telephone network is configured for the call to reach the destination by dialing a portion of the full E.164 number. The extension number may be registered as a dial-peer destination-pattern. If the '**num-exp**' dial plan configuration command is applied, Ubigate iBG router attempts to match to the destination-pattern by expanding the extension number to the full E.164 number.

Number expansion decreases the number of digits that user need to dial to reach the remote location. This applies to the called number of the entire incoming call. Number expansion is similar to the '**prefix**' command except that it is applied to the entire dial-peer and the status before matching to the destination-pattern.

The figure 8.9 shows a small company network wishing to use VoIP for integrating the telephone network into the current IP network. The Ubigate iBG router A Destination-pattern is 408 115-xxxx, 408 116-xxxx, 408 117-xxxx. The Destination-pattern towards Ubigate iBG router B is 729 555-xxxx.

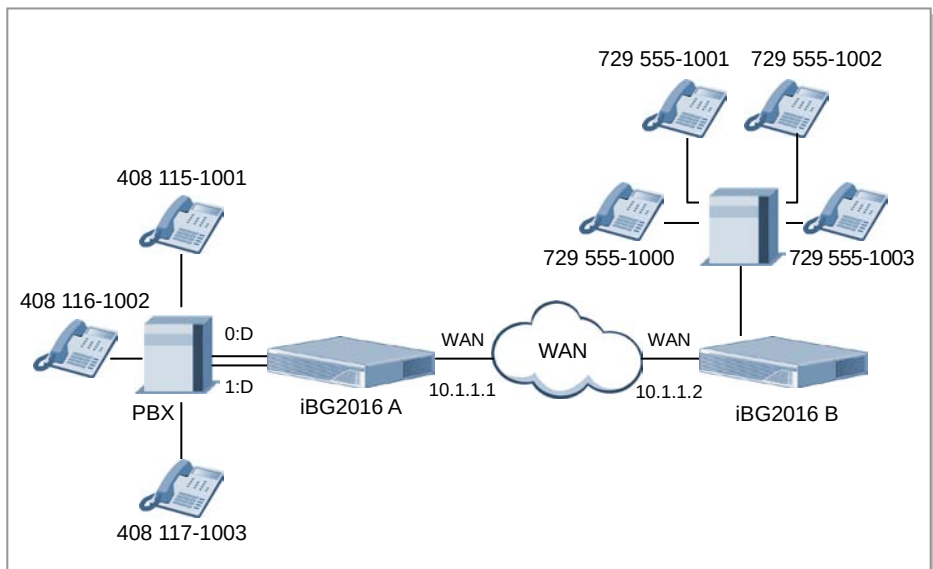


Figure 8.9 VoIP Example for Number Expansion

In the above case, the configuration table for applying number expansion is the same as the following:

Table 8.2 Number Expansion Commands

Extension	Destination Pattern	Num-exp Command
5....	408115....	numexp 5.... 408115....
6....	408116....	numexp 6.... 408116....
7....	408117....	numexp 7.... 408117....
1....	729555....	numexp 1.... 729555....

The Num-exp rule of the above table 8.2 should be applied to both Ubigate iBG router A and B.

Command	Purpose
sbm/dialplan# num-exp extension-number expanded-number	Configures number expansion globally to all dial peers. The <i>extension-number</i> means the extension number to be expanded with the value of <i>expanded-number</i>. The <i>expanded-number</i> argument means the telephone number that the full telephone number or extension number is likely to be expanded to.

Digit Translation Rule

The digit translation rule is used for changing digits of calling number or called number and numbering type, numbering plan.

For example, when the user's call is dialed with only five extension digits to other employees at other sites in company, change to the ten digit type which is capable of showing that switching should be done in the central office system. In this case, use the digit translation rule.

For example, users may dial only the five extension digits to other employees at another sites in the company. If the call is routed through the PSTN to reach the other site, the iBG router must use the translation rules to convert the five digit extension into the 10-digit format which is recognized by the central office switch.

The translation rule set can be configured with the translation-rule for up to 15 sets.

The kind of rule includes both the match & replace rule and the reject rule. The pattern expression in each rule uses the SED type expression characteristic.

By designating the translation rule set against the called number and the calling number, you can configure the translation profile.

The translation profile and the translation rule set can be applied to the various points such as the following.

- Trunk Group - The two different translation profiles can be applied to incoming and outgoing POTS calls. Two different translation rule sets can be designated for the called number and the calling number.
- Access Group - It is possible to designate a translation profile and rule set to apply translation to the Incoming VoIP call.
- Dial-peer.
- Voice-port.
- Incoming VoIP.

Configuring Translation Rule Set

By using the '**voice translation-rule**' global command, it is possible to create a rule set. Using the '**rule-match-replace**' voice translation-rule command, it is possible to designate match & replace rules in the rule set. Likewise, users can designate the reject rule using '**rule-reject**' voice translation-rule.

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters global configuration mode.
2	voice translation-rule <i>ruleset-id</i> Example) sbm/configure# voice translation-rule 1	Configuring translation rule set. Creates a translation rule set. Rule set ID can have a single value ranging from 1 to 10000.
3-1	rule-match-replace <i>precedence</i> /match-pattern/ /replace-pattern/ [match-type <i>type</i>] [replace-type <i>type</i>] [match-plan <i>plan</i>] [replace-plan <i>plan</i>] sbm/configure/.../rule 1# rule-match-replace 0 /111/ /333/	Configuring Reject Rule Precedence value can have a value ranging from 0 to 14.
3-2	rule-reject <i>precedence</i> /reject-pattern/ [reject-type <i>type</i>] [reject-plan <i>plan</i>] sbm/configure/.../rule 1# rule-reject 0 /111/	Configuring the Reject Rule Precedence value can have the value ranging from 0 to 14.

Voice translation rule uses a similar letter like Regular Expression Syntax. An example is found in the following Table 8.3.

Table 8.3 Characters of Translation Rule

Character	Description
^	Match the expression at the start of a line.
\$	Match the expression at the end of the line.
/	Delimiter that marks the start and end of both the matching and replacement strings.
\	Escape the special meaning of the next character.
-	Indicates a range when not in the first/last position. Used with the '[' and ']'.
[list]	Match a single character in a list.
[^list]	Do not match a single character specified in the list.
.	Match any single character.
*	Repeat the previous regexp zero or more times.
+	Repeat the previous regexp zero or more times.
?	Repeat the previous regular expression zero or one time. (use CTRL-V in order to enter).
()	Groups regular expressions.

Configuring Translation Profile

Creating a translation profile is possible by using '**voice translation-profile**' global configuration command. Designating the rule set in the called number and calling number is possible by using the '**translate**' voice translation-profile command.

Step	Command	Purpose
1	voice translation-profile <i>prof-name</i> Example) sbm/configure # voice translation-profile prof1	Configuring translation profile. Creating translation profile is possible by designating the single profile name.
2	translate {called calling} <i>rule-set-id</i> Example) sbm/.../translation-profile prof1# translate called 1	Configuring Translation Rule Set in Profile. Designates rule-set-id against called and calling number.

Applying Translation in Dial Peer

Command	Purpose
translation-profile {incoming outgoing} <i>trans-prof-name</i> Example) sbm/.../pots 1# translation-profile incoming prof1	Applying Translation Profile in Dial Peer.
translation-rule {called calling} <i>rule-set-id</i> Example) sbm/.../pots 1# translation-rule called 1	Applying Translation Rule in Dial Peer.

Applying Call Block in Dial Peer

Command	Purpose
call-block translation-profile incoming <i>trans-prof-name</i> Example) sbm/.../pots 1# call-block translation- profile incoming <i>trans-prof-name</i>	Configuring Call Block Translation Profile in Dial Peer. Translation profile is used for designating call block. In this case, designating reject-rule in rule-set should be done. Designates call block translation-profile against incoming call.

Applying Translation in Voice Port

Command	Purpose
translation-profile {incoming outgoing} <i>trans-prof-name</i> Example) sbm/.../voice-port 0/1/0# translation- profile incoming <i>prof1</i>	Applies Translation Profile in Voice Port.
translate {called-number calling-number} <i>rule-set-id</i> Example) sbm/.../voice-port 0/1/0# translate called-number 1	Applies Translation Rule in Voice Port.

Applying Translation in Trunk Group

Command	Purpose
translation-profile {incoming outgoing} <i>trans-prof-name</i> Example) sbm/.../trunk-group 1# translation-profile outgoing <i>prof1</i>	Applies Translation Profile in Trunk Group.

Applying Translation in Access Group

Command	Purpose
translation-profile {incoming outgoing} <i>trans-prof-name</i> Example) sbm/.../access-group ag1# translation-profile incoming <i>prof1</i>	Applies Translation Profile in Access Group.

Applying Translation in VoIP Incoming Calls

Command	Purpose
translation-profile <i>trans-prof-name</i> Example) sbm/.../voip-incoming# translation-profile <i>prof1</i>	Applies Translation Profile in VoIP incoming calls.
translation-rule {called calling} <i>rule-set-id</i> Example) sbm/.../voip-incoming# translation-rule called 1	Applies Translation Rule in VoIP Incoming Calls.

Verifying Translation Rule

To verify translation rules, perform the following steps.

1. Show voice translation-rule number.
2. Test voice translation-rule number input-test-string [type match-type [plan match-type]].

```
Router/configure# show voice translation-rule all
Translation-rule set id : 1
  Rule 0:
    Rule type : match & replace
    Match pattern : /^33/
    Replace pattern : //
    Match type: none      Replace type: none
    Match plan: none      Replace plan: none

Router/configure# test voice translation-rule 1 332795000

  Matched with Rule 1
  Original Number : 332795000
  Translated Number : 2795000
  Original Number Type : none   Translated Number Type : none
  Original Number Plan : none   Translated Number Plan : none
```

Verifying and Troubleshooting commands

Router# show voice translation-rule all

Router# test voice translation-rule <rule-id> <num>

Access Group Management

Introduction

Applying the call block function determines whether it permits the call or not based on the IP address before the inbound dial peer is matched against the VoIP incoming call. Executing the classification function is possible by setting Permit and Deny. By managing list groups with the IP address, authentication and call block function can be done.

Configuring Access Group

See the below table for the method for setting the access group and access list.

- Configuration Steps
 - configure terminal
 - voice access-group
 - access-list
 - access-list-permit
 - access-list-deny (optional)
 - description (optional)
 - disconnect-cause (optional)
 - translation-profile (optional)
 - exit
- Detailed Steps

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters global configuration mode.
2	voice access-group Example) sbm/configure# voice access-group <i>accgrp1</i>	Creates access group. The name of group must be less than 31 letters.
3	access-list <i>num</i> Example) sbm/... /access-group <i>name</i> # access-list 0	Creates access list. Users can create 8 lists ranging from 0 to 7.

(Continued)

Step	Command	Purpose
4	access-list-permit access-list-number { ipv4:ipv4-address[/subnet mask] [host] ipv6:ipv6-address[/subnet mask] [host] Example) sbm/... /access-group <i>name</i> # access-list-permit 0 ipv4:10.10.20.40	Designates permit IP within the list. If the permit IP is not designated, permit ip against the entire call. The range of permit ip depends on the subnet mask. For example, 10.10.10.1/32 means host but 10.10.10.1/24 means 10.10.10.0~10.10.10.254.
5	access-list-deny access-list-number {ipv4:ipv4-address[/subnet mask] ipv6:ipv6-address[/subnet mask]} Example) sbm/... /access-group <i>name</i> # access-list-deny 0 <i>ipv4-address</i>	Designates deny IP in (optional) list. IP users designated as deny member is possible only in IPs belonging to permit member. When there is no permit member, it is impossible to input. For example, if permit IP member is designated with 10.10.10.1/24, it is possible to designate 10.10.10.10 as deny ip member.
6	description <i>string</i> Example) sbm/... /access-group <i>name</i> # description ' <i>description for access group</i> '	Inputs description. on (optional) Access group. Uses Quotation mark ('').
7	disconnect-cause { invalid-number unassigned-number user-busy call-rejected } Example) sbm/... /access-group <i>name</i> # disconnect-cause invalid-number	When call is blocked by limiting (optional) Access list, select the returnable disconnect cause. The default value is no-service.
8	translation-profile <i>prof-name</i> Example) sbm/... /access-group <i>name</i> # translation-profile <i>profname1</i>	Translating access group in terms of passing call by designating (optional) translation profile.

Verifying Access Group

By using the **'test voice access-group *ip-address*'** command, you can check whether the call from the pertinent IP-address is allowed or not based on the access-group setting.

To verify the voice access-group, perform the following steps.

1. show voice access-group all
2. test voice access-group IP-address

```
Router/configure# show voice access-group all

    Access Group : agg1
      Description :

        Access List : 0
          PERMIT: ipv4:172.19.30.1/32 host

Router/configure# test voice access-group ipv4:172.19.30.1

A access group is found with ip address ipv4:172.19.30.1

    Source Group: agg1
  description: ""
  access-list: 0
disconnect-cause: "No Service"
translation profile: ""
```

Verifying and Troubleshooting commands

Router# show voice access-group all

Router# test voice access-group <ip-address>

Trunk Group Management

Introduction

The trunk group is the logical group of the interface having the same signal type. Thus, even though a single channel is in operation or in failure, the call can be made through other channels. The signal type is as follows.

- T1/E1 DS-0 Group (FXS, FXO, E & M, DID, R2 digital/pulse/analog)
- FXS, FXO, E & M, and DID analog voice ports:

Trunk group can be designated with the target of POTS outgoing dial peer and it is possible to designate it up to 12. It is possible to create a trunk group up to 100.

By using the '**translation-profile**' trunk group command in the trunk group, changing the calling and called number is possible by designating translation profile.

By designating the '**Max-calls**' trunk group command, users can limit the number of call made possible with the pertinent trunk group in terms of in and out.

By using the '**Block**' trunk group command, it is possible to prevent calls to the pertinent trunk group.

Multiple Trunk Group

It is possible to by designating the trunk group as the target up to 12 in the POTS dial peer.

The dial peer decreases the number of dial-peers desired to configure by having more than a single target.

Find the empty channel among the various trunk groups when the call request set against the outbound call is being made. The trunk group is searched in sequence according to the priority. If finding the empty channel in the trunk group with priority is impossible, it is possible to find it in the trunk group of following sequence. When the empty channel is found, the pertinent trunk group is used for the outbound call.

The following example shows how the trunk group is selected.

Example 1

```
dial-peer voice pots 1
trunk-group 101 1
trunk-group 102 2
trunk-group 103 3
```

Since trunk group 101 in the above example has priority with a preference value of 1, it is selected first. Then the trunk group 102 and trunk group 103.

Example 2

```
dial-peer voice pots 2
trunk-group 101
trunk-group 102
trunk-group 103 1
```

In the above example, trunk groups 101 and 102 are not designated in terms of the preference number. When the preference number is not designated, 13 is taken, which is the lowest value. Thus, selecting trunk group 103 comes first and then the sequence of 101 and 102.

Hunt Scheme

The hunt scheme is the selection method for selecting voice port or channel. The trunk group with various members uses the hunt scheme to find an idle channel for routing the outgoing call. The hunt scheme provided in Ubigate iBG router is random, round-robin or sequential.

Assume the three trunk groups. A has the smallest preference value. Let's assume that C has the biggest value and B has a value larger than A.

Optional parameters can modify the search to look in either ascending or descending order for an even-numbered channel, an odd-numbered channel, or either type.

Random

The trunk group finds an idle channel in random sequence. This method does not involve how call distribution is made between channels or whether the single channel is used more than other channels. Select the channel regardless of the standard of ascending series, descending series or odd, even channel.

Round-Robin

The trunk group finds idle channels in sequence. By remembering the previously selected channel, the channel can be found later following the same sequence.

This method meets the channel load balance between trunk group elements. With the optional parameter, it is possible to change to finding all channels or just the even or odd channel in either ascending or descending order.

Suppose '**hunt-scheme round-robin both up**' is enabled. Trunk group A is searched first because it has the highest preference. The search looks for an either-numbered idle channel in ascending series in A. If one is available, that channel is used for the call routing. A new idle channel request would start with B, which has the next highest precedence value.

If A does not have an available both-numbered channel, the search tries to find a channel in the next highest trunk group member, which is B. If successful, that channel is used for call routing. A new idle channel request would start with C.

If B does not have any available both-numbered channel, the search tries to find a channel in the next highest trunk group member, which is C. If successful, that channel is used for call routing. A new idle channel request would start with A.

Sequential

Regardless of the previously selected channel, Sequential is similar to the round-robin method except that it finds the first empty channel.

Suppose '**hunt-scheme sequential even down**' is enabled. Trunk group member A is searched first because it has the highest precedence value. The search checks A's channels in descending order looking for an even-numbered available channel. If successful, that channel is used for the call routing. The next idle channel request starts its search with A.

If A does not have an available even-numbered channel, the search tries to find an even-numbered channel in the next highest trunk group member, which is B. If successful, that channel is used for the call routing. A new idle channel request would start with A.

If B does not have any available even-numbered channels, the search tries to find an even-numbered channel in the next highest trunk group member, which is C. If successful, that channel is used for the call routing. A new idle channel request would start with A.

If C has no available even-numbered channels, the search repeats the process to find an odd-numbered channel. In this instance, the search would start again with A.

PLAR

PLAR Overview

PLAR (Private-line Automatic Ringdown) is an autodialing mechanism forming the perpetual connection between the voice interface of the opposite PBX and voice interface without dialing. It permits call completion with either the particular telephone number or PBX.

If the origination call is hooked off, the already defined network dial peer automatically matches and the call is made to the termination telephone or PBX.

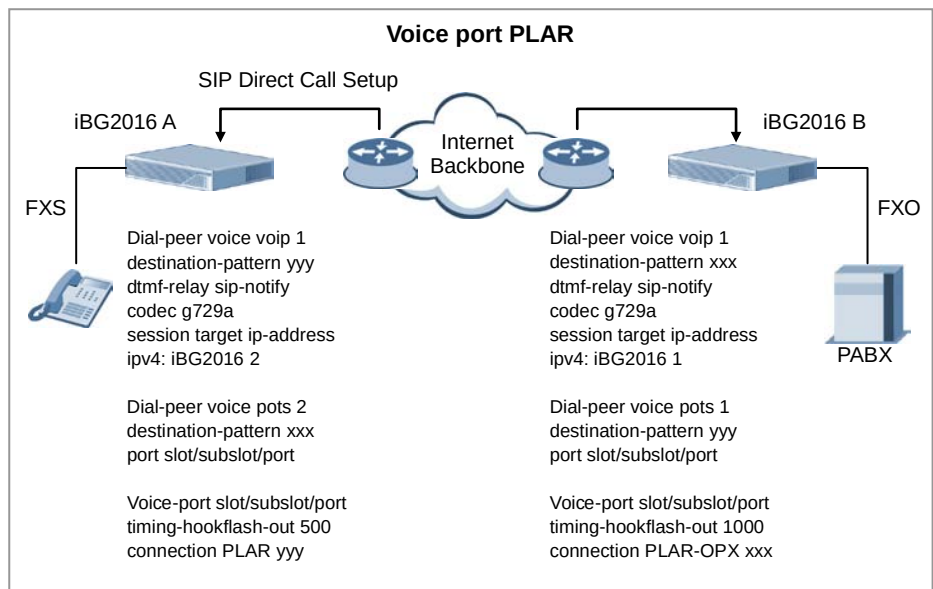


Figure 8.10 Example of PLAR configuration

How to Configure PLAR

- Configuration Steps
 - configure terminal
 - voice-port
 - connection plar
 - exit
- Detailed Steps

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters global configuration mode.
2	voice-port <i>slot/subslot/port</i> Example) /configure# voice-port 0/0/0	Enters voice-port configuration mode.
3	connection plar <i>digit-string</i> Example) /configure/voice-port(<i>slot/subslot/port</i>)# connection plar 01034381234	Enters connection mode for voice port.
4	exit Example) /configure/voice-port(<i>slot/subslot/port</i>)# exit	Exits the current mode.

PLAR-OPX

PLAR-OPX (Private-line Automatic Ringdown Off-Premises eXtension) enables the user of the remote FXS port to see the central PBX in the physically expanded way.

By using this option, the local voice port provides the local response before the remote voice port receives answer.

The PLAR-OPX connection makes the call possible before the user dials. The Ubigate iBG router uses the digits that follow the command internally to send to a dial peer.

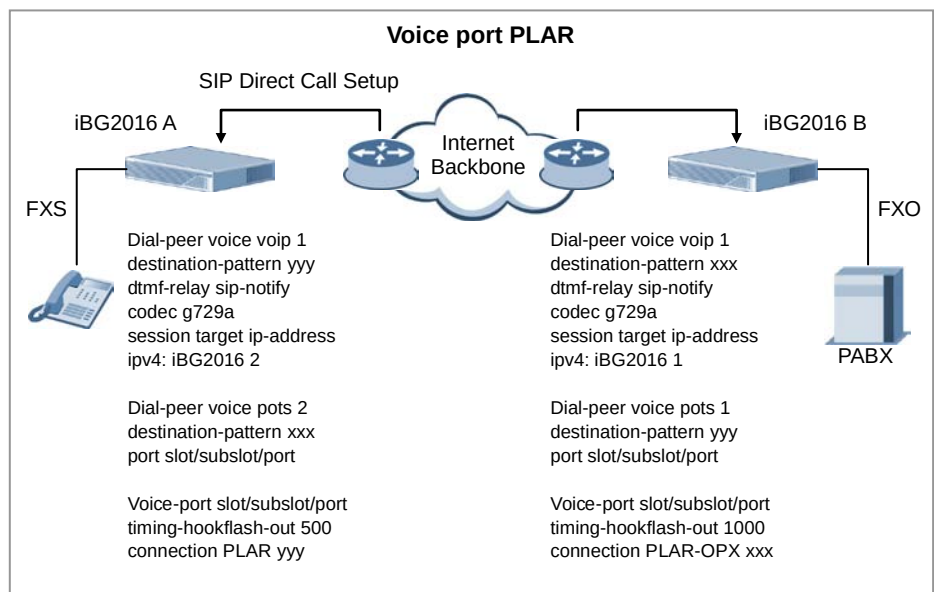


Figure 8.11 Example of PLAR-OPX configuration

How to Configure PLAR OPX

- Configuration Steps
 - configure terminal
 - voice-port
 - connection plar-opx
 - exit
- Detailed Steps

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters global configuration mode.
2	voice-port <i>slot/subslot/port</i> Example) /configure# voice-port 0/0/0	Enters voice-port configuration mode.
3	connection plar-opx <i>digit-string</i> Example) /configure/voice-port(<i>slot/subslot/port</i>)# connection plar-opx 01034381234	Enters connection mode for voice port.
4	exit Example) /configure/voice-port(<i>slot/subslot/port</i>)# exit	Exits the current mode.

PLAR and PLAR-OPX can be configured in Ubigate iPX interworking mode. When PLAR and PLAR-OPX were configured in Ubigate iPX interworking mode, you don't need to set up the VoIP dial-peer.

COR

Introduction

This is the function that decides call admission on the basis of the incoming, outgoing COR list designated in the inbound, outbound dial peer.

This function provides flexibility when planning the network, and enables a user to block a call, and limits distinctively between different callers.

COR (Class Of Restriction) is used for defining which incoming dial peer will be connected to which outgoing dial peer. Each dial peer can be designated as incoming or outgoing COR list. The incoming COR list shows the capacity of initialization of a chain of call attempts.

Configuring COR

Generally to apply the COR, define the COR names to as many outgoing dial peers as provided. Define the configured list of COR names. Allocate the list as an outgoing COR list of the outgoing dial peer. The names are the values of any string so a user can define it easily.

The next stage defines how many call admission groups are needed. Each group defines the COR list. Designating the COR list to a dial peer means defining the number of calls that an incoming dial peer can make.

Number	Description
dial-peer cor custom name 2a name 6a name 060b	# outgoing dialpeer 10, 20, 30 dial-peer voice pots 10 destination-pattern 2..T corlist outgoing list2a dial-peer voice pots 20 destination-pattern 6..T corlist outgoing list6a dial-peer voice pots 30 destination-pattern 060T corlist outgoing list060b
dial-peer cor list listA member 2a member 6a	# incoming dialpeer 80, 90 dial-peer voice voip 80 answer-address 590.... corlist incoming listA dial-peer voice voip 90
dial-peer cor list listB member 2a member 6a member 060b	answer-address 060T corlist incoming listB
dial-peer cor list list2a member 2a	
dial-peer cor list list6a member 6a	
dial-peer cor list list060b member 060b	

To set up the COR, use commands on the bottom of global configuration mode.

- Configuration Steps
 - configure terminal
 - dial-peer cor custom
 - name
 - exit
 - dial-peer cor list
 - member
 - exit
 - dial-peer voice {pots|voip}
 - corlist {incoming|outgoing}
 - exit
- Detailed Steps

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters global configuration mode.
2	dial-peer cor custom Example) sbm/configure# dial-peer cor custom	Enters COR configuration mode.
3	name <i>cor-name</i> Example) sbm/configure/.../custom# name <i>corname1</i>	Defines COR name. This step should be repeated as many as COR names.
4	exit Example) sbm/configure/.../custom# exit	Exits COR configuration mode.
5	dial-peer cor list <i>cor-list-name</i> Example) sbm/configure# dial-peer cor list <i>corlist1</i>	Defines COR list.

(Continued)

Step	Command	Purpose
6	member <i>cor-name</i> Example) sbm/configure/.../list <i>list-name</i> # member <i>corname1</i>	Designates member included in COR list. This step should be repeated under the necessity. <i>cor-name</i> should be the cor-name created in step 2.
7	exit Example) sbm/configure/.../list <i>list-name</i> # exit	Exits COR list configuration mode.
8	dial-peer voice {pots voip} <i>num</i> Example) Sbm/configure# dial-peer voice {pots voip} 10	Creates dial-peer.
9	corlist incoming <i>cor-list-name</i> Example) Sbm/configure/.../pots <i>num</i> # corlist incoming <i>corlist1</i>	When the appropriate dial-peer is used as incoming, set up a cor list.
10	corlist outgoing <i>cor-list-name</i> Example) Sbm/configure/.../pots <i>num</i> # corlist outgoing <i>corlist2</i>	When the appropriate dial-peer is used as outgoing, set up a cor list. From step7 to step9 should be repeated under the necessity, and designates cor list in dial-peer.

Verifying Classes of Restrictions

To check the COR configuration, follow the procedures below.

- To check the configured COR and list, use the **'show dial-peer cor'** command.

```
<<< Class of Restriction >>>
  < COR Custom NAME >
    name: corname1
    name: corname2
    name: corname3
  < COR list: list1 >
    member: corname1
    member: corname2
  < COR list: list2 >
    member: corname2
    member: corname3
```

- To check the COR list in which dial peer is set, use the **'show dial-peer voice'** command.

```
VoiceEncapPeer1
  <<< Dial Peer Common Info >>>
  id = 1, type = pots,
  description = ``,
  admin state = 'up', operation state = 'up',
  destination-pattern = `1001`, answer-address = ``,
  preference = 0, numbering type = 'none',
  incoming called-number = ``, connections/maximum = 0/
unlimited,
  decision limit number = '3',
  huntstop = `disabled`,
  incoming COR list = `list1`,
  outgoing COR list = `list2`,
  ...
```



CHAPTER 9. Extended VoIP Services

This chapter provides an overview of Voice over IP (VoIP) services. The chapter contains the following sections:

Fax Relay with VoIP
Supplementary services for Call Manager Interworking mode
Supplementary services for Survivable telephony mode
Supplementary services for Stand Alone mode

Fax Relay with VoIP

Introduction to Fax Relay with VoIP

To support fax transmission in a VoIP environment, the following methods are supported:

- pass-through (High-bandwidth codec)
- T.38

The method using Pass-through (High-bandwidth codec) transmits the fax through the use of G.711-alaw or G.711-ulaw voice stream; and the method using T.38 exchanges the T.38 Internet Fax Protocol (IFP) packets to transmit real-time Group 3 fax documents, which is the ITU-T recommendation. Regardless of the method specified for fax relay in the VoIP gateway, the VoIP gateway detects the fax tone, and codec negotiation is done before fax transmission if the codec needs to be changed.

This section describes how to configure each one to support fax relay under VoIP environment.

Configuring Fax Relay with VoIP

Restrictions for Configuring Fax Relay with VoIP

The following constraints exist for the fax relay in the VoIP environment.

- The codec (G.711-alaw or G.711-ulaw) specified in Pass-through (High-bandwidth codec) should also exist in the codec list of the relevant VoIP dial-peer.
- T.38 fallback function is supported only in H.323.

How to use high-bandwidth codec as Fax Relay with VoIP

There are 2 methods of setting the fax relay using the High-bandwidth codec (G.711-alaw or G.711-ulaw). The setting in 'VoIP dial-peer configuration' mode has a priority over the setting in 'voice-service configuration' mode.

1. 'fax protocol pass-through' command in 'VoIP dial-peer configuration' mode

- Configuration Steps
 - configure terminal
 - dial-peer voice voip
 - fax protocol pass-through
 - exit
- Detailed Steps

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters global configuration mode.
2	dial-peer voice voip Example) /configure#dial-peer voice voip 1000	Enters VoIP dial-peer configuration mode.
3	fax protocol pass-through Example) /configure/dial-peer/voice/voip 1000#fax protocol pass-through g711alaw	Specifies a high-bandwidth codec for fax relay with VoIP.
4	exit Example) /configure/dial-peer/voice/voip 1000#exit	Exits the current mode.

2. 'fax protocol pass-through' command in 'voice-service configuration' mode

- Configuration Steps
 - configure terminal
 - voice service voip
 - fax protocol pass-through
 - exit
- Detailed Steps

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters global configuration mode.
2	voice service voip Example) /configure#voice service voip	Enters voice-service configuration mode.
3	fax protocol pass-through Example) /configure/voice/service/voip#fax protocol pass-through g711alaw	Specifies a high-bandwidth codec for fax relay with VoIP.
4	exit Example) /configure/voice/service/voip#exit	Exits the current mode.

How to use T.38 as Fax Relay with VoIP

There are 2 methods of setting the fax relay using T.38. The setting in 'VoIP dial-peer configuration' mode has priority over the setting in 'voice-service configuration' mode. The fallback function enables the used of the high-bandwidth codec specified in fallback when T.38 cannot be used during the negotiation for fax transmission.

3. 'fax protocol t38' command in 'VoIP dial-peer configuration' mode

- Configuration Steps
 - configure terminal
 - dial-peer voice voip
 - fax protocol t38
 - fax rate
 - fax error-correction-mode
 - exit
- Detailed Steps

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters global configuration mode.
2	dial-peer voice voip Example) /configure#dial-peer voice voip 1000	Enters VoIP dial-peer configuration mode.
3	fax protocol t38 Example) /configure/dial-peer/voice/voip 1000#fax protocol t38 redundancy 0 fallback pass- through-g711ulaw	Specifies T.38 for fax relay with VoIP. - redundancy: specifies the number of redundant T.38 fax packets to be sent - fallback: {none pass-through-g711alaw pass-through-g711ulaw }
4	fax rate Example) /configure/dial-peer/voice/voip 1000#fax rate 14400	Specifies fax transmission speed.
5	fax error-correction-mode Example) /configure/dial-peer/voice/voip 1000#fax error-correction-mode	Enables fax-relay Error Correction Mode (ECM). To disable ECM, use 'no fax error-correction-mode' command.
6	exit Example) /configure/dial-peer/voice/voip 1000#exit	Exits the current mode.

4. 'fax protocol t38' command in 'voice-service configuration' mode

- Configuration Steps
 - configure terminal
 - voice service voip
 - fax protocol t38
 - fax rate
 - fax error-correction-mode
 - exit
- Detailed Steps

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters global configuration mode.
2	voice service voip Example) /configure#voice service voip	Enters voice-service configuration mode.
3	fax protocol t38 Example) /configure/voice/service/voip#fax protocol t38 redundancy 0 fallback pass-through-g711ulaw	Specifies T.38 for fax relay with VoIP. - redundancy: specifies the number of redundant T.38 fax packets to be sent - fallback: {none pass-through-g711alaw pass-through-g711ulaw }
4	fax rate Example) /configure/voice/service/voip#fax rate 14400	Specifies fax transmission speed.
5	fax error-correction-mode Example) /configure/voice/service/voip#fax error-correction-mode	Enables fax-relay Error Correction Mode (ECM). To disable ECM, use 'no fax error-correction-mode' command.
6	exit Example) /configure/voice/service/voip#exit	Exits the current mode.

Supplementary Services for Call Manager Interworking Mode

Service Descriptions

Ubigate iBG router provides supplementary services like Table 9.1 through control of Call Manager in the Call Manager interworking mode. For the methods for using services not mentioned in this document, see the Call Manager Operation Manual.

Table 9.1 Supplementary services for Call Manager Interworking mode

Service	Description
CLID	Calling Line Identification (CLID) function displays a calling party's phone number on a terminal of a called party.
Call Forward-All	This function forwards automatically all the calls incoming to a subscriber toward the pre-designated number inside or outside the system.
Call Forward-Busy	This function, when a called party is engaged, forwards automatically all the calls incoming to a subscriber toward the pre-designated number inside or outside the system.
Call Forward-NoAnswer	This function, when a called party does not reply, forwards automatically all the calls incoming to a subscriber toward the pre-designated number inside or outside the system.
Call Hold and Retrieve	This function allows you to place a call on hold, try a new call, and retrieve the call.
Call Park	The Call Park feature allows you to place a call on hold, so it can be retrieved from another phone in the Call Manager system. When talking on the phone, and hearing the dial tone after placing a call on hold, you can park a call by pressing the call park feature code and call park extension. Someone on another phone in your system can then dial the call park extension to retrieve the call.
Call Pickup Group	With this function another subscriber can answer the phone when a call is terminated to an extension subscriber and rings. With this function one picks up the call by dialing the group call pickup feature code only.
Call Pickup Direct	With this function another subscriber can answer the phone when a call is terminated to an extension subscriber and rings. Call Pickup direct is the function that picks up the call by directly dialing the ringing number followed by direct call pickup feature code.

Table 9.1 Supplementary services for Call Manager Interworking mode (Continued)

Service	Description
Call Pickup Universal	With this function another subscriber can answer the phone when a call is terminated to an extension subscriber and rings. With this function when a call is terminated to a subscriber of a group the call is picked up by dialing the number of the group followed by group call pickup feature code.
Call Restriction by User	Apart from the Call Restriction by Operator, Call Restriction by User function enables a subscriber to restrict origination from his own number at the request of a subscriber. This function does not affect termination.
Call Waiting and Retrieve	Call waiting lets users receive a second incoming call on the same line without disconnecting the first call. When the second call arrives, the user receives a brief call waiting indicator tone. If a subscriber responds to the second call by pressing Hook flash, the first call is held.
Call Transfer- Blind	Call Transfer holds a call in conversation and originates a new call to an extension number where you want to transfer your call. It is the function to transfer a call by hooking on a phone when a ring tone is given to a target extension subscriber to transfer. If the target does not reply, the call is re-terminated toward the transferring subscriber.
Call Transfer- Consultative	Call Transfer holds a call in conversation and originates a new call to an extension number you want to transfer your call. After an extension subscriber to where you want to transfer your call answers the call, Consultative Call Transfer transfers the call by hooking on.
Call Forwarding to VMS-All	This is the function that transfers the incoming call to the voice mail device, so an extension subscriber can leave a voice message in the voice message box when the subscriber does not answer the phone.
Call Forwarding to VMS-Busy	This is the function that transfers the incoming call to the voice mail device, so an extension subscriber can leave a voice message in the voice message box when the subscriber cannot answer the phone. Call forward to VMS- busy transfers the incoming call to the voice mail device, so an extension subscriber can leave a voice message in the voice message box when the appropriate subscriber is in conversation.

Table 9.1 Supplementary services for Call Manager Interworking mode (Continued)

Service	Description
Call Forwarding to VMS - NoAnswer	This is the function that transfers the incoming call to the voice mail device, so an extension subscriber can leave a voice message in the voice message box when the subscriber cannot answer the phone. Call forward to VMS- busy transfers the incoming call to the voice mail device, so an extension subscriber can leave a voice message in the voice message box when the appropriate subscriber does not answer.
Call Back Busy Subscriber	When the called party is busy, if the calling party has made a call reservation, Call Manager will originate a call from the calling party to the called party when the called party is idle.
Call Override	With the call override function, when a subscriber A and B registered with this function are busy in an emergency status, if A or B are called and they are busy; if a subscriber presses the number of A or B followed by the feature code, the call between A and B are held, such subscriber can make a call with A or B.
Call Intrusion	With the call override function, when a subscriber A and B registered with this function are busy in an emergency status, if A or B are called and they are busy; if a subscriber presses the number of A or B followed by the feature code, the conference call is established between A, B and said subscriber.
Privacy	If a subscriber does not want to interruption the call with another subscriber, activate this function. Then the subscriber will be not interrupted by Call Intrusion and Call Override function of other subscribers. This function is available only for the subscribers that an operator registered a privacy function.
Wake-up Call	If a subscriber has set a time and when the time is up, WKP transmits a paging signal to the subscriber. When the subscriber answers he will hear an announcement that the time is up.
Do Not Disturb (DND)	If Do Not Disturb (DND) is enabled, any incoming call from an internal/external subscriber is not terminated, but the originating party will hear an announcement that the called party does not want to answer the call.
Absentee Service (ABS)	If absentee service is enabled, any incoming call from an internal/external subscriber is not terminated, but the originating party will hear an announcement that the called party is absent.

Table 9.1 Supplementary services for Call Manager Interworking mode (Continued)

Service	Description
Conference calls (ad-hoc conference)	Ad-hoc Conferencing is the function that calls other subscribers when one subscriber is talking to another subscriber, and has a conversation with many subscribers at the same time, using conference bridge. Making other subscribers participate in the conversation while talking on the phone is available only for the promoter. The call is terminated when the promoter ends the call or all the participants end the call.
Group Call	This is the function that makes a specific group call number, and dials the appropriate group call number after registering the Call Manager subscribers as the member of a group call, all the members can talk over the phone at the same time.
Distinctive Ring	This function is to transmit distinctively designated rings accordingly as the terminating call of a subscriber is on-net or off-net.
Music On Hold Service	Music On Hold Service enables the call held party to listen to music designated in the Call Manager when the subscriber place the current call on hold.
Malicious Call	The function enables a subscriber who receives a unwanted call to leave the call record in the Call Manager operation terminal. To do so, pick up a receiver again, and dial the Malicious Call Feature code.
Follow Me	This function allows a subscriber to dial a Follow Me feature code and his own telephone number from a phone to which call forwarding will be done to forward a call to a desired phone.

Configuring Feature Codes

To support a smooth provision of services, the following feature codes should be set in a Ubigate iBG router. The feature codes regarding Call Pickup and Call Waiting are commonly used regardless of the operation mode. For more information on feature code settings, see the Command Reference.

How to download the feature codes from Call Manger

To download the feature codes from Call Manager follow the steps below:

- Configuration Steps
 - configure terminal
 - voip-gateway
 - call-server
 - exit

Although the feature codes have already been configured in the case of standalone mode using the commands below, you can automatically download the feature-codes administered in Call Manager to be deployed network wide to synchronize the usage of feature codes.

No	Command	Purpose
1	activate-call-conference	It is the feature code to dial prior to a phone number to call a third party or another for the conference call. During a generic call between A and B, do a hook flash, and then dial 'active-call-conference feature + C number' When the call between A and C is placed, do the hook flash again to proceed with the conference call among A, B, and C. In the same way, up to 6 parties can participate in a conference call. This feature code is valid only in a Call Manager Interworking mode.
2	drop-last-joined-party	It is a feature code to terminate the call with the last-joined subscriber during a conference call. When A,B,C,D are participating in a conference call, for example, and D is the last joined subscriber, if 'A' does hook flash and dial the drop-last-joined-party feature code, D is excluded from the conference. This feature code is valid only in a Call Manager Interworking mode.

(Continued)

No	Command	Purpose
3	group-call-pickup	This feature code is used for Group call pickup or Universal call pickup. Dial the group-call-pickup feature code to pick up the call terminating toward the subscriber in the pickup group which is the same as yours. To pick up the call terminating toward the group being different from yours, dial a group number together with a feature code.
4	direct-call-pickup	If you dial a Direct-call-pickup feature code together with a phone number, you can pick up the call terminating toward such number.
5	disable-call-waiting-for-current-call	This function disables the Call-waiting service during the period of the current call. If you do hook flash during a busy status and dial the disable-call-waiting-for-current-call feature code, the Call-waiting service is disabled for the duration of such call. If such call is released, the service is enabled again.
6	disable-call-waiting-for-next-call	This function disables the Call-waiting service for a new call. If you dial the disable-call-waiting-for-next-call feature code in front of the number to call, the Call-waiting service is disabled for the duration of such call.

Configuring Services

All the configuring services of the Call Manager Interworking mode are done in the Call Manager. But, for CLID Service enable the function that transfers a Caller ID to an FXS phone in FXS voice-port.

How to Configure Voice-Port for CLID

To enable the Caller Id function at FXS voice-port follow the procedures below:

- Configuration Steps
 - configure terminal
 - voice-port
 - caller-id enable
 - exit
- Detailed Steps

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters global configuration mode.
2	voice-port <i>slot/subslot/port</i> Example) /configure# voice-port 0/1/2	Enters Voice-Port configuration mode.
3	[no] caller-id enable [type1 type2] Example) /configure/voice-port(0/1/2)# caller-id enable type1	Enables or Disables caller-id feature.
4	Exit Example) /configure/voice-port(0/1/2)# exit	Exits the current mode.

How to Configure a Mixer for Conference (external)

In iPX interworking mode, the conference service is provided with iPX software resources (internal) or Ubigate iBG's DSP (external).

To utilize the iBG's DSP resource for a conference, follow the steps below:

- Configuration Steps
 - configure terminal
 - voice service voip conf
 - feature-code <string>
 - main-number <digit string>
 - room-number <base> <range>
 - max-participants <0-32> {default 16}
 - exit
- Detailed Steps

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters global configuration mode.
2	Voice service voip conf Example) /configure# voice service voip conf	Enters voice service voip conference configuration mode.
3	feature-code	This feature code is automatically updated and synchronized with the 'conference start' feature code
4	main-number <extension> Example) /configure# voice/service/voip/conf/ main-number 9000	The main (representative) number for a conference service. In iPX, EXT_NUM value
5	room-number <base> <range> Example) /configure# voice/service/voip/conf/ main-number 9001 10	Specify the starting number used to identify conference rooms and the range of rooms. The range is between 1 and 32. In iPX, START_CHANNEL, END_CHANNEL.

(Continued)

Step	Command	Purpose
6	max-participants <0-32> Example) /configure# voice/service/voip/conf/ max-participants 16	Total number of conference participants allowed by the system, considering provided DSP resources. Default: 16
7	exit Example) /configure# voice/service/voip/conf/ exit	Exits the current mode.

Open Ubigate iPX-DM, select CONFIG menu → Application Server → Create/Change, select a USER_GRP_NAME which conference attendee's user group.

EXT_NUM is 'main-number' in iBG, 'START_CHANNEL' is room-number in iBG and the range between START_CHANNEL and END_CHANNEL is 'room-number range' in iBG

[DIALOG] Application-Server - Change

USER_GRP_NAME	vgw-ug	NAME	DUT152_CONF
APP_TYPE	CONF_EXTERN	LOCATION_NAME	LOC_vgw
EXT_NUM	9811	START_CHANNEL	9812
END_CHANNEL	9820	SIP_URI	ibg152_conf@sec.com
REG_TYPE	APP_REG_N	IP_ADDR	172.19.30.152
PORT	5060	VMS_SVC_CODE	
URL_TYPE	SIP	PROTOCOL	UDP
TTL		UNAME	
PASSWORD			

Change Clear

Verifying configuration of Supplementary services

After configuring the service class for each subscribers in one iBG, you should verify that the configuration of each services are well configured and the profiles of each subscriber are downloaded.

How to Verify the subscribers profiles

To verify the subscribers profile follow, the procedures below.

- Verifying Steps
 - show sip-ua registration
 - show voip profiles
 - show voip profiles <extension number>
 - show voip sip-service-list
 - show voip feature-codes
 - show voice service voip

```

router# show voip profiles
      Id  Public Number      Extension  VMS
-----
SIP   1  2792700             2700
SIP   2  2792701             2701
-----
FXS   1  2792130             2130
FXS   2  2792131             2131
-----
Total 4, SIP 2, FXS 2
iBG_03#
iBG_03#
iBG_03#
router# show voip profiles 2130
FXS SUBSCRIBER : 2130
Public number   = 2792130
Extension number = 2130
Host domain     = sec01.com
Dual home       = no
User ID         =
Password        =
VMS URI         =
Used Services   = CTR CWT CPU GPU CID LCR MOH PARK TWC CC
GRC CINT OVRD
      CTR      : Call Transfer
      CWT      : Call Waiting
      CPU      : Call Pickup
      GPU      : Group Call Pickup
      CID      : Calling Line Identification
  
```

```

LCR          : Last Call Redial
MOH          : Music On Hold
PARK         : Call Park
TWC          : Three Way Call
CC           : Conference Call
GRC          : Group Call
CINT         : Call Intrusion
OVRD         : Call Override
Call forward any      =
Call forward busy     =
Call forward no answer =
Group pickup number   = 20003
iBG_03# show voip profiles 2700
IP PHONE SUBSCRIBER   : 2700
Public number         = 2792700
Extension number      = 2700
Host domain           = sec01.com
Dual home             = yes
VMS URI               =
Used Services         = CTR CWT CPU GPU CID
    CTR : Call Transfer
    CWT : Call Waiting
    CPU : Call Pickup
    GPU : Group Call Pickup
    CID : Calling Line Identification
Call forward any      =
Call forward busy     =
Call forward no answer =
Group pickup number   = 20003
Auth User ID          =
Auth Password         = 2700
Algorithm(global)     = MD5
Realm(global)         =
qop auth-int(global)  = no

```

router# show voip sip-service-list

ID	EXT	CFA	CFB	CFN	CTR	CWT	CPU	GPU	CID	CGD	LCR	MOH	PRK
TWC	CC	HLN	GRC	CB	PRI	CIN	OVR						
F 1	2130	-	-	-	use	use	use	use	use	-	use	use	use
use	use	-	use	-	use	use							
F 2	2131	-	-	-	use	use	use	use	use	-	use	use	use
use	use	-	use	-	use	use							
S 1	2700	-	-	-	use	use	use	use	use	-			
S 2	2701	-	-	-	use	use	use	use	use	-			

router# show voip feature-codes

[F CODE] [MIN] [MAX] [SVC NAME]

```

-----
*17      3      10  group_call_pickup
*77      3      10  direct_call_pickup
*22      3      10  active_call_conference
*70      3      10  drop_last_joined_party
*50      6      14  call_forward_all_registration
*51      0      0   call_forward_all_cancel
*52      6      14  call_forward_busy_registration
*53      0      0   call_forward_busy_cancel
*54      6      14  call_forward_no_answer_registration
*55      0      0   call_forward_no_answer_cancel
*21                               conference_start

```

<<< Downloaded feature codes >>>

```

-----
*17      3      10  group_call_pickup
*77      3      10  direct_call_pickup
*22      3      10  active_call_conference
*70      3      10  drop_last_joined_party
*21                               conference_start

```

router# show voice service voip

VoIP Service Feature

Codec List: System Default

Preference 1: G.711 a-law 64 kbps 20 ms

Preference 2: G.711 u-law 64 kbps 20 ms

Preference 3: G.729 8 kbps 20 ms

Conference

Feature code: *21

Main number: 9000

Max participants: 16

Room number: 9001 - 9010

Digital Gain

Input: 0.0 dB

Output: 0.0 dB

FAX Protocol: NONE

ECM: ENABEL

Rate: 14400 bps

Playout Delay: Adaptive Mode

Nominal Delay: 80 ms

Minimum Delay: 20 ms

Maximum Delay: 200 ms

Timer

Media inactivity detection: DISABLE

VAD: DISABLE

Supplementary services for Survivable Telephony Mode

Service Descriptions

Even in Survivable telephony mode, Ubigate iBG router independently provides some supplementary services provided by Call Manager control in Call Manager interworking mode. The services provided in survivable telephony mode are like Table 9.2 below.

Table 9.2 Supplementary services for Survivable telephony mode

Service	Description
CLID	Calling Line Identification (CLID) function displays a calling party's phone number on a terminal of a called party.
Call Forward-All	It is the function to forward automatically all the calls incoming to a subscriber toward the pre-designated number inside or outside the system.
Call Forward-Busy	It is the function, when a called party is engaged, to forward automatically all the calls incoming to a subscriber toward the pre-designated number inside or outside the system.
Call Forward-NoAnswer	It is the function, when a called party does not reply, to forward automatically all the calls incoming to a subscriber toward the pre-designated number inside or outside the system.
Call Hold and Retrieve	This function allows you to place a call on hold, try a new call, and retrieve the call.
Call Pickup Group	With this function another subscriber can answer the phone when a call is terminated to an extension subscriber and rings. It is the function that when a call is terminated to a subscriber from the same group who picks up the call by dialing a specific feature code.
Call Pickup Direct	It is the function that another subscriber can answer the phone when a call is terminated to an extension subscriber and rings. Call Pickup direct is the function that picks up the call by directly dialing the ringing number.
Call Pickup Universal	It is the function that another subscriber can answer the phone when a call is terminated to an extension subscriber and rings. With this function a call is terminated to a subscriber of a group who picks up the call by dialing the number of the group.

Table 34.2 Supplementary services for Survivable telephony mode (Continued)

Service	Description
Call Waiting and Retrieve	Call waiting lets users receive a second incoming call on the same line without disconnecting the first call. When the second call arrives, the user receives a brief call waiting indicator tone. If a subscriber responds to the second call by pressing Hook flash, the first call is held.
Call Transfer-Blind	Call Transfer holds a call in conversation and originates a new call to an extension number where you want to transfer your call. It is the function to transfer a call by hooking on a phone when a ring tone is given to a target extension subscriber to transfer. If the target does not reply, the call is re-terminated toward the transferring subscriber.
Call Transfer-Consultative	Call Transfer holds a call in conversation and originates a new call to an extension number where you want to transfer your call. After an extension subscriber where you want to transfer your call answers the call, Consultative Call Transfer transfers the call by hooking on.
Distinctive Ring	This function is to transmit distinctively designated rings accordingly as the terminating call of a subscriber is on-net or off-net.

Configuring Services

Ubigate iBG router does not require a user to set up separately for survivable telephony mode services. In the Call Manager Interworking mode, it controls services on the basis of subscriber profiles downloaded from Call Manager. But, as in Call Manager Interworking mode, CLID Service enables the function that transfers a Caller Id to a FXS phone in FXS voice-port.

How to Configure Voice-Port for CLID

To enable the Caller Id function in FXS voice-port follow the below procedures.

- Configuration Steps
 - configure terminal
 - voice-port
 - caller-id enable
 - exit
- Detailed Steps

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters global configuration mode.
2	voice-port <i>slot/subslot/port</i> Example) /configure# voice-port 0/1/2	Enters Voice-Port configuration mode.
3	[no] caller-id enable [type1 type2] Example) /configure/voice-port(0/1/2)# caller-id enable type1	Enables or Disables caller-id feature.
4	Exit Example) /configure/voice-port(0/1/2)# exit	Exits the current mode.

Supplementary Services for Stand Alone Mode

Service Descriptions

Ubigate iBG router independently provides services in Stand Alone mode as Table 9.3 below.

Table 9.3 Supplementary services for Stand Alone mode

Service	Description
CLID	Calling Line Identification (CLID) function displays a calling party's phone number on the terminal of a called party.
Call Hold and Retrieve	This function allows you to place a call on hold, try a new call, and retrieve the call.
Call Pickup Group	With this function another subscriber can answer the phone when a call is terminated to an extension subscriber and rings. It is the function that when a call is terminated to a subscriber from the same group picks up the call by dialing a specific feature code.
all Pickup Direct	With this function another subscriber can answer the phone when a call is terminated to an extension subscriber and rings. Call Pickup direct is the function that picks up the call by directly dialing the ringing number.

Table 9.3 Supplementary services for Stand Alone mode (Continued)

Service	Description
Call Pickup Universal	With this function another subscriber can answer the phone when a call is terminated to an extension subscriber and rings. With this function, when a call is terminated to a subscriber of a group, picks up the call by dialing the number of the group.
Call Waiting and Retrieve	Call waiting lets users receive a second incoming call on the same line without disconnecting the first call. When the second call arrives, the user receives a brief call waiting indicator tone. If a subscriber responds to the second call by pressing Hook flash, the first call is held.
Call Transfer-Blind	Call Transfer holds a call in conversation and originates a new call to an extension number where you want to transfer your call. It is the function to transfer a call by hooking on a phone when a ring tone is given to a target extension subscriber to transfer. If the target does not reply, the call is re-terminated toward the transferring subscriber.
Call Transfer-Consultative	Call Transfer holds a call in conversation and originates a new call to an extension number where you want to transfer your call. After an extension subscriber where you want to transfer your call answers the call, Consultative Call Transfer transfers the call by hooking on.
Distinctive Ring	This function is to transmit distinctively designated rings accordingly as the terminating call of a subscriber is on-net or off-net.

Configuring Services

To provide supplementary services for FXS phone, configure service by service in FXS voice-port.

How to Configure Voice-Port for CLID

To enable the Caller ID function in FXS voice-port follow the below procedures.

- Configuration Steps
 - configure terminal
 - voice-port
 - caller-id enable
 - exit
- Detailed Steps

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters global configuration mode.
2	voice-port <i>slot/subslot/port</i> Example) /configure# voice-port 0/1/2	Enters Voice-Port configuration mode.
3	[no] caller-id enable [type1 type2] Example) /configure/voice-port(0/1/2)# caller-id enable type1	Enables or Disables caller-id feature.
4	Exit Example) /configure/voice-port(0/1/2)# exit	Exits the current mode.

How to Configure Voice-Port for CLIDB

To block Caller ID in an originating call of an FXS phone, follow the procedures as below.

- Configuration Steps
 - configure terminal
 - voice-port
 - caller-id block
 - exit
- Detailed Steps

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters global configuration mode.
2	voice-port <i>slot/subslot/port</i> Example) /configure# voice-port 0/1/2	Enters Voice-Port configuration mode.

(Continued)

Step	Command	Purpose
3	[no] caller-id block Example) /configure/voice-port(0/1/2)# caller-id block	Blocks or re-enables the caller id of the calls made from this port.
4	Exit Example) /configure/voice-port(0/1/2)# exit	Exits the current mode.

How to Configure for Call Hold

The Call Hold and Retrieve service is available for all FXS subscribers by default. There is no way to enable or disable.

How to Configure Dial-Peer for Call Forwarding

To enable Call Forwarding service, enable the services and assign a forwarding number in the dial-peer according to the procedures below:

- Configuration Steps
 - configure terminal
 - dial-peer voice pots
 - call-forwarding enable
 - call-forwarding all-number <digit>
 - call-forwarding busy-number <digit>
 - call-forwarding no-answer-number <digit>
 - exit
- Detailed Steps

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters global configuration mode.
2	dial-peer voice pots <i>tag</i> Example) /configure# dial-peer voice pots 11	Enters POTS Dial-peer configuration mode.

(Continued)

Step	Command	Purpose
3	[no] call-forwarding enable Example) /configure/ dial-peer/voice/pots 11# call-forwarding enable call-forwarding { all-number busy-number no-answer-number } <string> Example) /configure/dial-peer/voice/pots 11# call-forwarding busy-number 031279333	Enable Call forwarding service. Specifies call forwarding number for each service type. All: always forwarding to this number busy: forwarding this number when busy no-answer: forwarding this number when there is no answer during 30 seconds.
4	Exit Example) /configure/ dial-peer/voice/pots 11# exit	Exits the current mode.

How to Configure Dial-Peer for Call Pickup

To enable Call Pickup service, allocate the pickup group number in the dial-peer according to the procedures below.

- Configuration Steps
 - configure terminal
 - dial-peer voice pots
 - call-pickup-group
 - exit
- Detailed Steps

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters global configuration mode.
2	dial-peer voice pots <i>tag</i> Example) /configure# dial-peer voice pots 11	Enters POTS Dial-peer configuration mode.

(Continued)

Step	Command	Purpose
3	[no] call-pickup-group <i>group-number</i> Example) /configure/ dial-peer/voice/pots 11# call-pickup-group 8400	Specifies call pickup group number for Call Pickup service.
4	Exit Example) /configure/ dial-peer/voice/pots 11# exit	Exits the current mode.

How to Configure Dial-Peer for Call Waiting

To enable Call Waiting and Retrieve service, follow the procedures as below.

- Configuration Steps
 - configure terminal
 - dial-peer voice pots
 - call-waiting
 - exit
- Detailed Steps

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters global configuration mode.
2	dial-peer voice pots <i>tag</i> Example) /configure# dial-peer voice pots 11	Enters POTS Dial-peer configuration mode.
3	[no] call-waiting Example) /configure/ dial-peer/voice/pots 11# call-waiting	Enables or Disables Call waiting and retrieve service.
4	Exit Example) /configure/ dial-peer/voice/pots 11# exit	Exits the current mode.

How to Configure Call Transfer

The Call Transfer service is available for all FXS subscribers by default. There is no way to enable or disable this service.

How to Configure Voice-Port for Distinctive Ring

To enable Distinctive Ring service, follow the procedures as below.

- Configuration Steps
 - configure terminal
 - voice-port
 - ring cadence on-net
 - ring cadence off-net
 - exit
- Detailed Steps

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters global configuration mode.
2	voice-port <i>slot/subslot/port</i> Example) /configure# voice-port 0/1/2	Enters Voice-Port configuration mode.
3	ring cadence on-net <i>ring-type</i> Example) /configure/voice-port(0/1/2)# ring cadence on-net bellcore01	Specifies On-Net Ring type for the voice port.
3	ring cadence off-net <i>ring-type</i> Example) /configure/voice-port(0/1/2)# ring cadence off-net bellcore01	Specifies Off-Net Ring type for the voice port.
4	Exit Example) /configure/voice-port(0/1/2)# exit	Exits the current mode.



CHAPTER 10. Call Admission Control

CAC is an important technology for maintaining reliable voice quality. Unlike general data packet, voice is sensitive to packet delay. If traffic is transmitted in real time, it is more effective to reject its session connection in advance than to establish a session when it is an anticipated packet. A user should check whether network resources are available using the Voice CAC that maintains voice quality and admits a new voice call.

Local CAC

Local CAC is applied to a VoIP system and its network interfaces on which VoIP traffic is transmitted and limits VoIP calls according to the maximum number of calls allowed on a system-wide basis and a dial-peer basis. For example, Local CAC provides a function to cut off calls when there are more than 10 calls in excess of the bandwidth allocated in the network interface, since it is set to have less than 10 calls in a WAN network interface.

Max call for system

Max call for system is the function to set the max limitation for calls in the Ubigate iBG router, and limit new calls until the number of calls has fallen when it reaches the maximum. This function does not operate when applied to the whole Ubigate iBG router. This is because the call limitation function that permits max calls is used in the Call Manager.

A user is able to set max calls using call-admission max-calls and change it to the initial value using the no form of the command.

The initial value is the maximum value which the Ubigate iBG router admits.

call-admission max-calls *value*

value: Designates max calls that are admitted and a number of 1~20,000 can be used.

If you want to check the information set, use 'show running-config'.

Configuration procedure

- Configuration Steps
 - configure terminal
 - call-admission max-call
 - exit
- Detailed Steps

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters global configuration mode.
6	Call-admission max-call Example) configure # call-admission max-call	Configures max call.
7	Exit Example) configure # exit	Exits the current mode.

```
call-admission max-calls 2000
```



NOTE

In Call Manager interworking mode the mechanism of the Max call for the system is not used.

DS0 Limitation

DS0 Limitation limits available physical interface. To limit a certain amount of max calls coming through PBX, it blocks a part of the channels in E1/T1 trunk, which is connected to PBX, in order to decrease DS0 in the system.

It is possible to avoid heavy traffic that is more than the planned bandwidth in the network by using the Physical DS0 timeslot. It is also possible to not generate CPU overhead, and provide additional service in toll by pass. Using this kind of method, it is available to cope with busy-hour of heavy traffic.

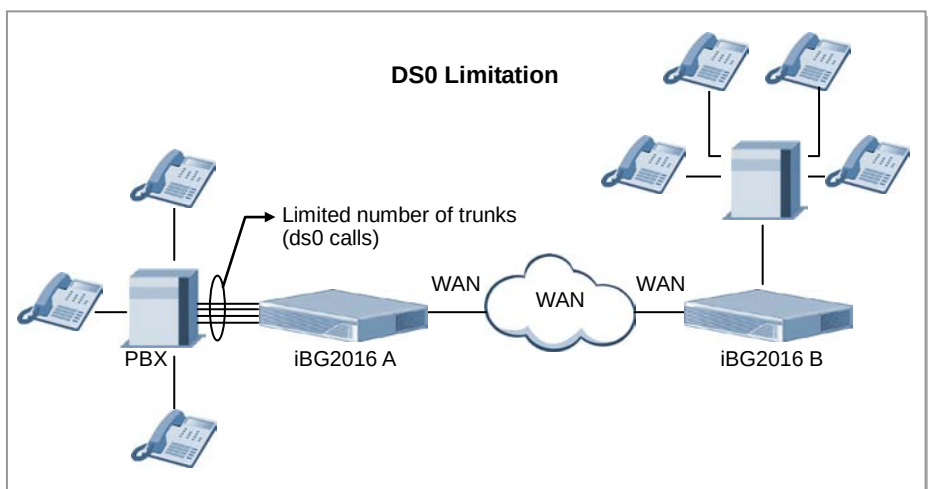


Figure 10.1 DS0 Limitation

Max call per dial-peer

Provides a way to limit the number of max connections of the Dial-peer. A user is able to set this using 'max-conn' command in dial-peer configuration mode.

This is a way to control the connection number available at the same time in the Dial-peer for Outbound, in order that the current connection does not exceed the connection number set.

This tool is easy to use but limited in the scope of the network design problems it can solve. Because it is applied per dial peer, it is not possible to limit the total number of calls the outgoing gateway can have active simultaneously unless you have a limited number of dial peers and you use the max-call command on each one.

The max-connections feature can also be used on the POTS dial peer to limit the number of calls that can be active on a T1/E1 to a PBX/PSTN if one wishes to provision all time slots on that connection but limit the number of calls to a lesser number than the physical number of time slots.

Although this feature is useful in many scenarios, it has the following drawbacks:

- Although it provides some protection for the voice gateway egress WAN link, it provides little or no protection for links in the network backbone.
- It does not work for IP telephony applications that do not use dial peers.
- It is limited to simple topologies.
- It does not react to link failures or changing network conditions.

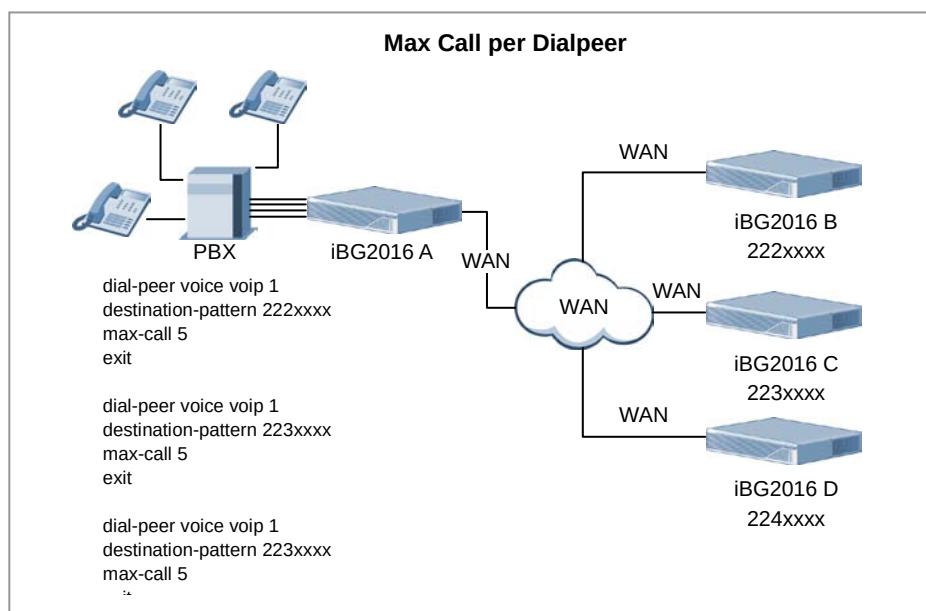


Figure 10.2 max call per dialpeer



NOTE

In Call Manager interworking mode the Max call per dial-peer mechanism is not used.

Voice Bandwidth

When WAN link is used for processing the VoIP call, this is the function to calculate the media bandwidth used as WAN link by using the set up voice bandwidth, and control in order that the bandwidth that is more than the permitted bandwidth may not be used in VoIP media. In Voice Bandwidth, payload for voice, not for signal bandwidth, is available.

Table 10.1 Bandwidth per Codec

Codec	Bandwidth
G.711 (a-law and -law)	80 kbps
G.723.1 and G.723.1A (5.3 kbps)	22 kbps
G.723.1 and G.723.1A (6.3 kbps)	23 kbps
G.726 (16 kbps)	32 kbps
G.726 (24 kbps)	40 kbps
G.726 (32 kbps)	48 kbps
G.728	32 kbps
G.729 (all versions)	24 kbps



NOTE

In Call Manager interworking mode, mechanism of Voice Bandwidth is not used.

Local voice busyout

Local voice busyout monitors the status of Ethernet/WAN etc. and sets a certain port or Digital trunk timeslot to busyout. An operator is also able to set voice-port, DS0-group voice-port, BRI port, and Digital trunk timeslots to busyout.

The objects of busyout monitoring can monitor the gatekeeper, sip-server, Ethernet interface, WAN interface (bundle interface), and SIP Peer.

The busyout monitoring objects can be classified. A user is able to gather monitoring lists, create a class, and add the class to the monitoring objects, in order to include the class objects defined in the monitoring list in the monitoring objects.

A user is able to create a busyout class by using 'voice class busyout <tag>', the available tag is from 1 to 31, and add the busyout monitoring list used in the busyout class in voice class busyout configuration mode.

LVBO allows you to take a PBX trunk connection to the attached gateway completely out of service when WAN conditions are considered unsuitable to carry voice traffic.

This technique has the following advantages:

- Not every call must be rejected individually and incur a postdial delay.
- Prevents the need for hairpinning rejected calls back to the originating PBX, using up multiple DS0 slots for a single call.
- Works well to redirect rejected calls with PBXs that either do not have the intelligence or are not configured appropriately.
- Solves the hairpinning problem of the PBX putting the call back onto a third DS0 on the same T1/E1 line to the gateway that has already rejected the call and hairpinned it. CCS trunk types manage this hairpinning problem because cause code information can be returned to the PBX that triggers rerouting logic. However on CAS trunks the PBX does not know what went wrong, and unless digits are manipulated in the gateway, the PBX cannot easily make a decision to reroute the call over a different trunk group.

LVBO provides the outgoing gateway with the ability to monitor the state of various network interfaces, both LAN and WAN, and busy back the trunk to the PBX if any of the monitored links should fail. Up to 32 interfaces can be monitored; if either one of or all of the interfaces change state, the gateway can be configured to busy back the trunk to the PBX. The reason this feature is called local voice busyout is because only local links can be monitored. This feature has no visibility into the network beyond the link of the local gateway.

How to set LVBO

Convert Voice-port to busyout state by force (busyout forced).

Convert time slots on E1/T1 trunk to busyout state by force (ds0 busyout).

With specific conditions things can be converted to busyout by monitoring (busyout monitor).

If you want to check the current busyout monitor list, use the 'show voice busyout monitor' command.

Using the show voice busyout port, a user is able to check the voice port list currently set to busyout and information on the reason why voice port is busyout.

Busyout forced

To handle voice-port to busyout by force, use the 'busyout forced' command in voice port configuration mode. In this case, away from busyout handling by monitoring, it is possible to handle the voice-port in a busyout status.

busyout forced
no busyout forced

Gatekeeper monitoring

This is a method to check out the status of the Gatekeeper by the RRQ message with Gatekeeper, and provides the method used in busyout monitoring. Gateway monitoring works upon down.

To configure a voice port to enter the busyout state if connectivity to the gatekeeper is lost, use the **busyout monitor gatekeeper** command in voice-port configuration mode. To disable, use the **no** form of this command.

busyout monitor gatekeeper
no busyout monitor gatekeeper

SIP-server monitoring

This can check out the status of the server using OPTIONS/REGISTER message for SIP with SIP-Server/Call-Server, this method provides the way that can use sip-server status in the busyout monitoring. Gateway monitoring works up/down.

To configure a voice port to enter the busyout state if SIP options message with the sip-server is no answer, use the **busyout monitor sip-server** command in the voice-port configuration mode. To disable, use the **no** form of this command.

busyout monitor sip-server
no busyout monitor sip-server

Ethernet monitoring

Detects the status of Ethernet Link Layer, and provides busyout monitoring using Ethernet link in order to set up/release the busyout according to Down/Up of Ethernet link, and supports to set up busyout state according to UP/Down.

To place a voice port into the busyout monitor Ethernet state, enter the **busyout monitor ethernet** command in voice-port configuration mode. To remove the busyout monitor Ethernet state from the voice port, use the **no** form of this command.

busyout monitor ethernet *interface-number* [**in-service**]
no busyout monitor ethernet *interface-number*

interface-number Identifies an interface to be monitored for the voice port busyout function.

in-service (Optional) Configures the voice port to be busied out when any monitored interface comes into service (its state changes to up). If the keyword is not entered, the voice port is busied out when all monitored interfaces go out of service (their state changes to down).

WAN link monitoring

WAN link monitoring detects the links of interfaces configured as WAN and provides busyout monitoring that used the WAN link in order to set up/release busyout according to down/up of the WAN link, and supports to set up/release busyout state according to Up/Down of the WAN link.

To set up busyout monitoring of the WAN link, a desired WAN interface should be created in advance.

To place a voice port into the busyout monitor WAN state, enter the **busyout monitor** command in voice-port configuration mode. To remove the busyout monitor WAN state from the voice port, use the **no** form of this command.

busyout monitor *interface-name interface-number* [**in-service**]
no busyout monitor *interface-name interface-number*

interface-name Identifies an interface name to be monitored for the voice port busyout function.

These are bundle, and loopback that can be used as the interface name.

interface-number Identifies an interface to be monitored for the voice port busyout function.

in-service (Optional) Configures the voice port to be busied out when any monitored interface comes into service (its state changes to up). If the keyword is not entered, the voice port is busied out when all monitored interfaces go out of service (their state changes to down).

IP address monitoring

To turn on Peer (by IP address) busyout monitoring of a voice port, use the **busyout monitor ip-address** command in voice-port configuration mode. To remove Peer (by IP address) busyout monitoring, use the no command. Check out the state of the peer if the SIP-stack is working normally, using the SIP OPTIONS message for the system designated to the IP address.

busyout monitor ip-address *ip-address*
no busyout monitor ip-address *ip-address*

Class monitoring

To turn on busyout monitoring of the busyout class of a voice port, use the **busyout monitor class** command in the voice-port configuration mode. To remove busyout monitoring of the busyout class, use no command.

Refer to 'voice class busyout' section for more information about busyout class.

This sets up resources information to be monitored using busyout in which items are collected.

busyout monitor class *<tag>*
no busyout monitor class *<tag>*

<tag>: From 1 to 31 can be used. Designates Voice class tag

Use 'busyout monitor <interface type> <interface name>' for the Busyout monitor command used in Voice class busyout configuration mode, and use bundle and Ethernet for interface type.

To check set up and status information on voice class busyout a user is able to use 'show voice busyout class' command.

DS0 busyout

When E1/T1 Digital Trunk is used, provides a method to set up the busyout status of specific timeslots.

In the case of an Analog port, use the ‘busyout forced’ command in the Voice-port configuration mode of the appropriate voice-port in order to set up busyout.

In case of Digital trunk, use the ‘busyout forced’ command in the Voice-port configuration mode of the appropriate voice-port in order to set up busyout at a DS0-Group unit. It provides a set up method in case of setting up busyout at a unit of a specific timeslot.

To force a DS0 timeslot on a controller into the busyout state, use the **ds0 busyout command** in Voice-port configuration mode. To remove the DS0 time slot from the busyout state, use the **no** form of this command.

ds0 busyout *ds0-time-slot*
no ds0 busyout *ds0-time-slot*

ds0-time-slot DS0 time slots to be forced into the busyout state. Range is from 1 to 24 and can include any combination of time slots.

voice class busyout

This sets up resources information to be monitored using busyout in which items are collected.

voice class busyout <tag>
no voice class busyout <tag>

<tag>: From 1 to 31 can be used. designates Voice class tag.

Use ‘busyout monitor <interface type> <interface name>’ for Busyout monitor command used in Voice class busyout configuration mode, and use bundle and Ethernet for interface type.

The following are busyout monitor commands used in voice class busyout configuration mode.

busyout monitor ethernet *interface-number* [**in-service**]
no busyout monitor ethernet *interface-number*
busyout monitor bundle *interface-name* [**in-service**]
no busyout monitor bundle *interface-name*
busyout monitor sip-server
no busyout monitor sip-server
busyout monitor gatekeeper
no busyout monitor sgatekeeper
busyout monitor ip-address *dest-ip-address*
no busyout monitor ip-address *dest-ip-address*

busyout monitor ethernet:

- add Ethernet interface to busyout monitoring class

busyout monitor bundle:

- add WAN (bundle) interface to busyout monitoring class

busyout monitor sip-server:

- add sip server or call server status to busyout monitoring class

busyout monitor gatekeeper:

- add gatekeeper status to busyout monitoring class

busyout monitor ip-address:

- add SIP UA (by ip address) status to busyout monitoring class

To check set up and status information on voice class busyout a user is able to use 'show voice busyout class' command.

show voice busyout class

To configure busyout voice port class monitoring, use busyout monitor class command.

busyout monitor class *<tag>*
no busyout monitor class *<tag>*

Resource-based CAC

System resource-based Call Admission Control uses two kinds of resources on the basis of requested and used quantity of the resource, reserving the resources necessary for processing a call. One method processes according to CPU power and utilization of memory, and the other processes according to utilization of DSP.

CPU/Memory sets up a threshold, on the basis of a pre-set percentage, and starts controlling when the value is more than the designated high value, and terminates when less than the designated low value.

CPU utilization

This is the function that checks utilization at 5 second-intervals and checks the average at 30 second-intervals. It processes busyout or treatment when utilization is more than the designated high value, and operates normally when it is less than the low value.

Monitoring utilization which is the global resource of Ubigate iBG router. A user can set it up using 'call-admission threshold global' command that is the global CAC configuration, and release it using the 'no' command. A user is able to use call-admission control, monitor utilization by using `cpu-5sec`, `cpu-avg` trigger of call-admission threshold global.

```
call-admission threshold global trigger-name low value high value  
[busyout] [treatment]  
no call-admission threshold global trigger-name low 1 high 1  
show call-admission threshold config
```

Trigger-name is the value of `cpu-5sec` and `cpu-avg` against CPU utilization. One of the following can be used.

- **cpu-5sec**-CPU utilization in the last 5 seconds.
- **cpu-avg**-Average CPU utilization.
- **total-calls**-Total number of calls.
- **total-mem**-Total memory utilization.

low value Value of low threshold: Range is from 1 to 100% for the utilization triggers; 1 to 10000 calls for **total-calls**

high value Value of high threshold: Range is from 1 to 100% for the utilization triggers; 1 to 10000 calls for **total-calls**.

busyout (Optional) Busyout the T1/E1 channels if the resource is not available.

treatment (Optional) Applies call treatment from the session application if the resource is not available.

The default is **busyout** and **treatment** for global resource triggers.

Memory consumption

This is the function that checks total utilization of memory at 5 second-intervals, and processes busyout or treatment when utilization is more than the designated high value, and operates normally when it is less than the low value.

To monitor memory which is the global resource of the Ubigate iBG router.

A user can set it up using 'call-admission threshold global' command which is the global CAC configuration, and release it using the 'no' command.

A user is able to use call-admission control, monitor utilization by using the total-mem trigger of the global call-admission threshold.

Call-admission threshold global *trigger-name* **low value high value**
[busyout] [treatment]

no call-admission threshold global *trigger-name* **low 0 high 0**
show call-admission threshold config

Trigger-name is the value of total-mem against memory utilization. One of the followings can be used.

- **cpu-5sec**-CPU utilization in the last 5 seconds.
- **cpu-avg**-Average CPU utilization.
- **total-calls**-Total number of calls.
- **total-mem**-Total memory utilization.

low value Value of low threshold: Range is from 1 to 100% for the utilization triggers; 1 to 10000 calls for **total-calls**

high value Value of high threshold: Range is from 1 to 100% for the utilization triggers; 1 to 10000 calls for **total-calls**.

busyout (Optional) Busyout the T1/E1 channels if the resource is not available.

treatment (Optional) Applies call treatment from the session application if the resource is not available.

The default is **busyout** and **treatment** for global resource triggers.

DSP resource

When there is no DSP resource available, this is the function that cuts calls until the DSP resource is returned. When DSP utilization is more than the designated value the Minor/Major Alarm goes on.

Set up the threshold according to utilization of the DSP chip mounted in the system, not to utilization of the DSP resource, use call-admission threshold alarm max-dsp, and change the initial value using the 'no' command. The initially set min value is 70 and max value is 80.

The initial min value is 70, and max value is 80.

call-admission threshold alarm max-dsp [min <value>] [maj <value>]
no call-admission threshold alarm max-dsp

min value: Is the value of DSP utilization that Minor Alarm would RAISE/CLEAR, a user can designate it from 1% TO 100%. The initial value is 70.

maj value: Is the value of DSP utilization that Major Alarm would RAISE/CLEAR, a user can designate from 1% to 100%. The initial value is 80.

Call-admission Spike

This is the function that cuts calls by monitoring when incoming calls reach their peak in a certain period. To set up this function, use 'call-admission spike' which is a global CAC configuration command, to release it use the 'no' command.

call-admission spike <call-number> [**steps** <number-of-steps> **size** <milliseconds>]
no call-admission spike <call-number>

- **call-number**-The number of incoming calls to set as the spike threshold. The range is from 1 to 2, 147, 483, 647.
- **steps**-The number of steps in a sliding window. The range is from 3 to 10.
- **size**-The size of the step in milliseconds. The range is from 100 to 2000.

A user is able to limit incoming calls in intervals of size time using the call-admission spike command. Size and step make windows, the windows are made by size intervals. The size of a window is $\text{size} \times \text{step}$. The relationship between size and step is shown in the figure below.

The Call-admission spike command is a command that limits incoming calls available in a window. Information on windows is created every size time, and there are as many windows as steps.

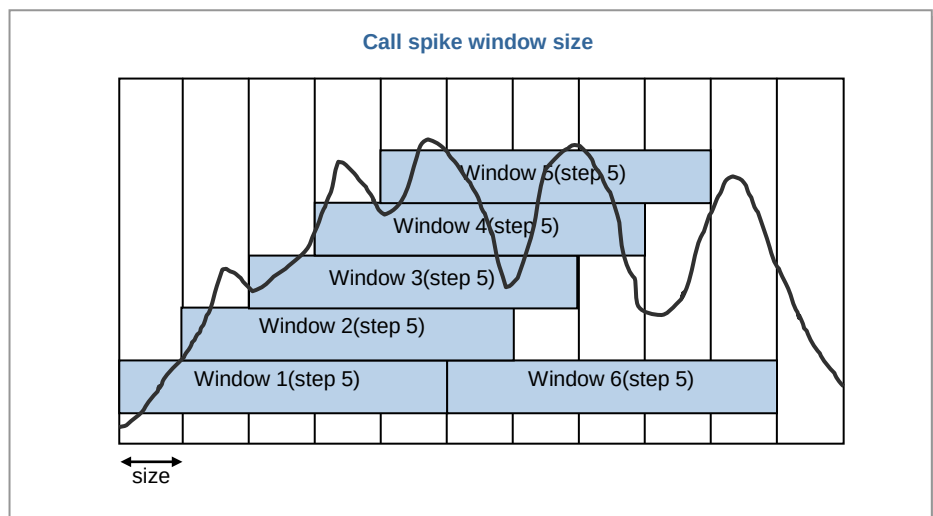


Figure 10.3 Call-admission spike window size

Call admission Treatment

enable treatment

Use the call-admission treatment on command in a global configuration mode to enable call treatment; and use the no call-admission treatment on command to disable it.

call-admission treatment on
no call-admission treatment on

treatment action

When the call treatment is enabled, use the call-admission treatment action command in a global configuration mode to select the action necessary for call-admission control; use 'no' command to release it.

call-admission treatment action { reject | hairpin }
no call-admission treatment action {reject | hairpin }

cause-code

When call treatment is enabled and the call-treatment is 'reject', use the call-admission treatment causecode command in a global configuration mode to select the error code to be used for rejection; use 'no' command to release it.

call-admission treatment causecode *<busy|no-resource >*
no call-admission treatment causecode *<busy|no-resource>*

isdn reject code

When call treatment is enabled, the call-treatment is 'reject', and the Inbound signal upon rejection is ISDN; use the call-admission treatment isdn-reject command in a global configuration mode to select the error code to be used for rejection; use 'no' command to release it.

call-admission treatment causecode *<cause-code>*
no call-admission treatment causecode *<cause-code>*
<cause-code>: From 34 to 47 can be used.



CHAPTER 11. Management

Alarm

There are 7 alarms and 2 faults relating to voice from Ubigate iBG router.

Alarm

There are mainly 5 types of alarms relating to voice. The alarms are in relation to Call Count, DSP channel, SIP entity, H323 gatekeeper, and FXS port.

The detailed alarm list is described in Table 11.1 below.

Each alarm is created automatically and is cleared automatically when it is restored.

A user can check logging about RAISE/CLEAR of the alarm using 'show system logging buffered'.

Table 11.1 Alarm List

Alarm Name	Level	Description
MaximumCallLimitMaj	Major	Exceeding a threshold of the system maximum call limit (Major thresholds)
MaximumCallLimitMin	Minor	Exceeding a threshold of the system maximum call limit (Minor thresholds)
DSPChannelLimitMaj	Major	Exceeding a threshold of the DSP channel capacity limit (Major thresholds)
DSPChannelLimitMin	Minor	Exceeding a threshold of the DSP channel capacity limit (Minor thresholds)
SIPEntityFail	Major	Connection fails between iBG and SIP entity
gwgkFailAlarm	Major	Connection fails between H.323 entity
FXOConnect	Minor	Notify that FXO port is connected when using Loop-Start ONLY

To display the screen on alarm, set up using system logging. Since the default configuration is 'system logging console critical', check the terminal screen logged by setting up as 'system logging all_terminal informational'. If you cannot check the alarm information with the terminal, check it with 'show system logging buffered', and check the information on system logging buffer with 'show system logging syslog'.

Maximum Call Limit

This is an alarm created when a certain percentage is reached on the basis of pre-set max call. Default value is Minor 70%, Major 80%. To change it, use 'call-admission threshold alarm max-call' command in Global configuration command mode, and to initialize the default value, use the 'no' command.

```
call-admission threshold alarm max-call min <value> maj <value>
no call-admission threshold alarm max-call
```

min <value>: Is the percentage of current call count of the max call count that would create a minor alarm

maj <value>: Is the percentage of current call count of the max call count that would create a major alarm.

Set up max call used as the basis, using 'call-admission max-calls' command in global configuration command mode.

A user is able to check the current value set with the show running-config command.

DSP Channel Limit

It is an alarm created when a certain percentage is reached on the basis of pre-set max DSP channel usage. Default value is Minor 70%, Major 80%. To change it, use the 'call-admission threshold alarm max-dsp' command in the Global configuration command mode, and to initialize the default value, use the 'no' command.

```
call-admission threshold alarm max-dsp min <value> maj <value>
no call-admission threshold alarm max-dsp
```

min <value>: Is the percentage of current used dsp channel compared with the max dsp channel that would create a minor alarm.

maj <value>: Is the percentage of current used dsp channel compared with the max dsp channel that would create a major alarm.

It is impossible to set up the max value of the DSP channel used as the basis; the system decides automatically according to the type of the mounted DSP card.

A user can check the current value set with show running-config command.

SIPEntityFail

This is an alarm created when REGIST fails after periodically trying registering the gateway using the SIP REGISTER message in call-server or SIP proxy.

GW GK Fail Alarm

This is an alarm created when the communication with the H.323 Gatekeeper through RRQ message has failed.

FXOConnect

This is an alarm to notify whether ports are connected or not in analog channels of the FXS card using loop start.

Fault

The fault, which may have occurred, relating to the Voice Feature of Ubigate iBG router is a fault related to DSP and Voice Task.

When a fault has occurred, a user has to restore it by resetting the system.

Table 11.2 Fault List

Fault Name	Description
DSP init fail	Fail to Initialize DSP resource
Voice task fail	Voice task killed

DSP init fail

This fault occurs when there is an error in the process of initializing the DSP card, it might occur in the initiation of the system. When a fault occurs the system cannot be used as the voice gateway.

Voice task fail

When operating the Ubigate iBG router, this fault occurs in case the task related to voice processing suspends. In this case, the Ubigate iBG router cannot be used as a voice gateway.

Statistics

Ubigate iBG router statistics displays the numerical value of accumulation after booting up the system. The objects of Ubigate iBG router statistics are as follows.

- Call statistics-whole call statistics, POTS call statistics, VoIP call statistics.
- Protocol statistics-SIP, H323 protocol statistics.
- Dial peer statistics.

Call statistics.

It displays the statistics of both POTS and VoIP call.

Call Statistics Command

Table 11.3 Call Statistics command

Command	Explanation
show statistics { call pots-call voip-call }	Checks statistics of whole call, POTS call, and VoIP call.
clear statistics { all call }	Initializes statistics of whole call, call

Call Statistics Item

Table 11.4 Call Statistics Item

Item	Object	explanation
Inbound Total Calls Num	POTS, VoIP, Call	Incoming call number
Outbound Total Callse Num	POTS, VoIP, Call	Outgoing call number
Inbound Success Calls Num	POTS, VoIP, Call	Incoming successful calls - number of incoming calls that received answers

Table 36.4 Call Statistics Item (Continued)

Item	Object	explanation
Outbound Success Calls Num	POTS, VoIP, Call	Outgoing successful calls - number of outgoing calls that received answers
Inbound Failed Calls Num	POTS, VoIP, Call	Incoming failed calls - number of incoming calls that failed
Outbound Failed Calls Num	POTS, VoIP, Call	Outgoing failed calls - number of outgoing calls that failed
Inbound Abnormal Terminated Calls Num	Call	Incoming abnormal terminated calls - number of incoming answered calls terminated with any cause code other than 'normal'
Outbound Abnormal Terminated Calls Num	Call	Outgoing abnormal terminated calls - number of incoming answered calls terminated with any cause code other than 'normal'
Inbound Abandon Calls Num	POTS, VoIP, Call	Incoming abandon call - number of incoming not-answered calls with normal cause.
Outbound Abandon Calls Num	POTS, VoIP, Call	Outgoing abandon call - number of outgoing not-answered calls with normal cause.
Canceled Calls Num	Call	Cancelled calls - number of calls encountering the originating side having been disconnected before the outgoing calls were connected
Excess Loss Packet Calls Num	VoIP, Call	Excess loss packet calls - number of calls losing packets
Excess Latency Calls Num	VoIP, Call	Excess latency calls - number of calls encountering more than the configured amount of latency
Excess Jitter Buffer Calls Num	VoIP, Call	Excess jitter buffer calls - number of calls encountering more than the configured amount of jitter

SIP protocol statistics.

Displays the statistics of SIP protocol. The statistics of SIP protocol takes statistics of send, resend, receive, and receive in each item.

SIP protocol command

Table 11.5 SIP protocol Statistics command

Command	Explanation
show statistics sip-protocol	checks statistics of sip protocol
clear statistics sip-protocol	initializes statistics of sip protocol

Call Statistics Item

Table 11.6 SIP protocol Statistics command

Item	Explanation
Req Bye Num	Terminated the session
Req Cancel Num	Terminated the pending request
Req Info Num	Number of information messages the gateway have been received (inbound) and how many have been transmitted (outbound)
Req Invite Num	Number of Call Initiations
Req Notify Num	Number of Notify requests
Req Options Num	Number of Option requests
Req Prack Num	Number of PRACK request
Req Register Num	Number of Register requests
Req Subscriber Num	Number of Subscribe requests
Req Refer Num	Number of Refer requests
Req Update Num	Number of Update requests
Req Message Num	Number of Message requests
Ack Num	A confirmed final response sent
Ok Bye Num	Terminated the session
Ok Cancel Num	Terminated the pending request
Ok Info Num	Number of information messages the gateway has received (inbound) and how many have been transmitted (outbound)

Table 36.6 SIP protocol Statistics command (Continued)

Item	Explanation
Ok Invite Num	Number of call initiations
Ok Notify Num	200 Successful response to a Notify request
Ok Options Num	200 Successful response to an Options request
Ok Prack Num	200 Successful response to a PRACK request
Ok Register Num	200 Successful response to a Register request
Ok Subscribe Num	200 Successful response to a SUBSCRIBE request
Ok Update Num	200 Successful response to a Update request
Ok Message Num	200 Successful response to a Message request
Trying Num	100 Action is being taken with no resolution
Ringing Num	180 Called party has been located and is being notified of the call
Call Is Being Forwarded Num	181 Call is being forwarded to a different set of destinations
Queued Num	182 Until the called party is available, the message is queued
Session Progress Num	183 Indicates in-band alerting
Accepted Num	202 A successful response to a Refer request received
Multiple Choices Num	300 The address resolved several choices. UA can select preferred communication
Moved Permanently Num	301 User is no longer available at this location
Moved Temporarily Num	302 User is temporarily unavailable
Use Proxy Num	305 Caller must use a proxy to contact called party
Alternative Service Num	380 Unsuccessful call; however, an alternate service is available
Bad Request Num	400 Bad Request (includes the malformed Via header)
Unauthorized Num	401 The request requires user authentication
Payment Required Num	402 Payment is required to complete the call
Forbidden Num	403 The SIP server has the request, but cannot provide service
Not Found Num	404 Called party does not exist in the specified domain
Method Not Allowed Num	405 Method specified in the request is not allowed
Not Acceptable Num	406 Call was contacted, but some aspect of the session description was unacceptable

Table 36.6 SIP protocol Statistics command (Continued)

Item	Explanation
Proxy Authentication Required Num	The request requires user authentication by proxy
Request Timeout Num	408 Server could not produce a response before the Expires time-out
Gone Num	410 Resource is no longer available at the server, and no forwarding address is known
Request Entity Too Large Num	413 Server refuses to process request because the request is larger than is acceptable
Request URI Too Long Num	414 Server refuses to process, because the URI (URL) request is larger than is acceptable
Unsupported Media Type Num	415 Server refuses to process a request because the service option is not available on the destination endpoint
Unsupported URI Scheme Num	416 Server refuses to process, because the scheme of the URI is unknown to the server
Bad Extension Num	420 Server could not understand the protocol extension in the Require header
Extension Required Num	421 The UAS needs a particular extension to process the request, but this extension is not listed in a Supported header field in the request
Session Interval Too Small Num	422 The request contains a Session-Expires header field with a duration below the minimum timer for server
Interval Too Brief Num	423 Server reject the request, because the expiration time of the resource is too short
Temporarily Unavailable Num	480 The callee's end system was contacted successfully but the callee is currently unavailable
Call Transaction Dose Not Exist Num	481 The request does not match the existing dialog or transaction
Loop Detection Num	482 A loop server received a request that included itself in the path
Too Many Hops Num	483 A server received a request that required more hops than is allowed by the Max-Forward header
Address Imcomplete Num	484 Address supplied is incomplete
Ambiguous Num	485 Address supplied is ambiguous
Busy Here Num	486 Called party is busy
Request Terminated Num	487 The request is canceled

Table 36.6 SIP protocol Statistics command (Continued)

Item	Explanation
Not Acceptable Here Num	488 Call was contacted, but some aspect of the session description was unacceptable
Bad Event Num	489 Bad Event response indicates a Subscribe request has an event type that the server could not understand
Request Pending Num	491 UAS have a pending request within the same dialog
Undeipherable Num	493 UAS received encrypted MIME body, but does not process
Security Agreement Required Num	494 The request needs security agreement
Server Internal Error Num	500 The server or gateway encountered an unexpected error that prevented it from processing the request
Not Implemented Num	501 Service or option not implemented in the server or gateway
Bad Gateway Num	502 Network is out of order
Service Unavailable Num	503 Server is temporarily unable to process the request due to a temporary overloading or maintenance of their server
Server Timeout Num	504 Server could not produce a response before the Expires time- out
Version Not Supported Num	505 The SIP protocol version that was used in the request is not supported
Message Too Large Num	513 The message length exceeded capabilities
Precondition Failure Num	580 The session could not be established because of failure to meet required preconditions
Busy Everyshere Num	600 Called party is busy
Decline Num	603 Call rejected
Does Exist Anywhere Num	604 Server has authoritative information that the called party does not exist in the network
Not Acceptable Num	606 Call was contacted, but some aspect of the session description was unacceptable

H323 protocol statistics.

H323 protocol command

Table 11.7 Call Statistics command

Command	Explanation
show statistics h323-protocol	Checks statistics of h323 protocol (H.225.0 CS, H.225.0 RAS, H.245, Release-Cause).
clear statistics h323-protocol	Initializes statistics of h323 protocol.

Call Statistics Item

The statistics items of H.225.0 CS, H.225.0 RAS, and H.245 Message are as below, and the statistics item of the Release-Cause is same as the cause value defined in Q.850.

Table 11.8 H.225.0 CS Statistics command

Item	Explanation
Setup	Number of Setup messages the gateway has received and transmitted
Setup Acknowledge	Number of SetupAcknowledge messages the gateway has received and transmitted
Call Proceeding	Number of Call Proceeding messages the gateway has received and transmitted
Progress	Number of Progress messages the gateway has received and transmitted
Alerting	Number of Alerting messages the gateway has received and transmitted
Connect	Number of Connect messages the gateway has received and transmitted
Release Complete	Number of Release Complete messages the gateway has received and transmitted
Facility	Number of Facility messages the gateway has received and transmitted
Information	Number of Information messages the gateway has received and transmitted
UserInformation	Number of UserInformation messages the gateway has received and transmitted

Table 36.8 H.225.0 CS Statistics command (Continued)

Item	Explanation
Notify	Number of Notify messages the gateway has received and transmitted
Status	Number of Status messages the gateway has received and transmitted
Status Inquiry	Number of Status Inquiry messages the gateway has received and transmitted
Unknown	Number of unknown messages the gateway has received and transmitted

Table 11.9 H.225.0 RAS Statistics command

Item	Explanation
GatekeeperRequest	Number of GRQ messages the gateway has received and transmitted
GatekeeperConfirm	Number of GCF messages the gateway has received and transmitted
GatekeeperReject	Number of GRJ messages the gateway has received and transmitted
RegistrationRequest	Number of RRQ messages the gateway has received and transmitted
RegistrationConfirm	Number of RCF messages the gateway has received and transmitted
RegistrationReject	Number of RRJ messages the gateway has received and transmitted
UnregistrationRequest	Number of URQ messages the gateway has received and transmitted
UnregistrationConfirm	Number of UCF messages the gateway has received and transmitted
UnregistrationReject	Number of URJ messages the gateway has received and transmitted
AdmissionRequest	Number of ARQ messages the gateway has received and transmitted
AdmissionConfirm	Number of ACF messages the gateway has received and transmitted
AdmissionReject	Number of ARJ messages the gateway has received and transmitted

Table 36.9 H.225.0 RAS Statistics command (Continued)

Item	Explanation
BandwidthRequest	Number of BRQ messages the gateway has received and transmitted
BandwidthConfirm	Number of BCF messages the gateway has received and transmitted
BandwidthReject	Number of BRJ messages the gateway has received and transmitted
DisengageRequest	Number of DRQ messages the gateway has received and transmitted
DisengageConfirm	Number of DCF messages the gateway has received and transmitted
DisengageReject	Number of DRJ messages the gateway has received and transmitted
LocationRequest	Number of LRQ messages the gateway has received and transmitted
LocationConfirm	Number of LCF messages the gateway has received and transmitted
LocationReject	Number of LRJ messages the gateway has received and transmitted
InfoRequest	Number of IRQ messages the gateway has received and transmitted
InfoRequestResponse	Number of IRR messages the gateway has received and transmitted
NonStandardMessage	Number of Non-Standard message the gateway has received and transmitted
UnknownMessageResponse	Number of XRS messages the gateway has received and transmitted
RequestInProgress	Number of RIP messages the gateway has received and transmitted
ResourceAvailableIndicate	Number of RAI messages the gateway has received and transmitted
ResourceAvailableConfirm	Number of RAC messages the gateway has received and transmitted
InfoRequestAck	Number of IACK messages the gateway has received and transmitted
InfoRequestNak	Number of INAK messages the gateway has received and transmitted

Table 36.9 H.225.0 RAS Statistics command (Continued)

Item	Explanation
ServiceControlIndication	Number of SCI messages the gateway has received and transmitted
ServiceControlResponse	Number of SCR messages the gateway has received and transmitted
Unknown	Number of unknown messages the gateway has received and transmitted

Table 11.10 H.245Statistics command

Item	Explanation
MasterSlaveDetermination	Number of MasterSlaveDetermination messages the gateway has received and transmitted
MasterSlaveDeterminationAck	Number of MasterSlaveDeterminationAck messages the gateway has received and transmitted
MasterSlaveDeterminationReject	Number of MasterSlaveDeterminationReject messages the gateway has received and transmitted
MasterSlaveDeterminationRelease	Number of MasterSlaveDeterminationRelease messages the gateway has received and transmitted
TerminalCapabilitySet	Number of TerminalCapabilitySet messages the gateway has received and transmitted
TerminalCapabilitySetAck	Number of TerminalCapabilitySetAck messages the gateway has received and transmitted
TerminalCapabilitySetReject	Number of TerminalCapabilitySetReject messages the gateway has received and transmitted
TerminalCapabilitySetRelease	Number of TerminalCapabilitySetRelease messages the gateway has received and transmitted
OpenLogicalChannel	Number of OpenLogicalChannel messages the gateway has received and transmitted
OpenLogicalChannelAck	Number of OpenLogicalChannelAck messages the gateway has received and transmitted
OpenLogicalChannelReject	Number of OpenLogicalChannelReject messages the gateway has received and transmitted
OpenLogicalChannelConfirm	Number of OpenLogicalChannelConfirm messages the gateway has received and transmitted
CloseLogicalChannel	Number of CloseLogicalChannel messages the gateway has received and transmitted

Table 36.10 H.245Statistics command (Continued)

Item	Explanation
CloseLogicalChannelAck	Number of CloseLogicalChannelAck messages the gateway has received and transmitted
RequestChannelClose	Number of RequestChannelClose messages the gateway has received and transmitted
RequestChannelCloseAck	Number of RequestChannelCloseAck messages the gateway has received and transmitted
RequestChannelCloseReject	Number of RequestChannelCloseReject messages the gateway has received and transmitted
RequestChannelCloseRelease	Number of RequestChannelCloseRelease messages the gateway has received and transmitted
RequestMode	Number of RequestMode messages the gateway has received and transmitted
RequestModeAck	Number of RequestModeAck messages the gateway has received and transmitted
RequestModeReject	Number of RequestModeReject messages the gateway has received and transmitted
RequestModeRelease	Number of RequestModeRelease messages the gateway has received and transmitted
EndSessionCommand	Number of EndSessionCommand messages the gateway has received and transmitted
UserInputIndication	Number of UserInputIndication messages the gateway has received and transmitted
Unknown	Number of unknown messages the gateway has received and transmitted

Debug Management

This section describes commands that show Debug related to voice.
The following contents are displayed:

- Voice Call Control Debug.
- Voice Protocol Module Debug.
- H323 Debug.
- SIP Debug.
- Voice Debug.
- Voice Call log Debug

Voice Call Control Debug Mode

This is the function that shows an appropriate call log after a voice call.
There are parameters of in/out/all that set up Incoming/Outgoing, and
deb0/deb1/info/all that set up levels.

Especially set up log commands when displaying debug Messages of a specific port.

Table 11.11 Voice Call Control Debug

Command	Purpose
Debug vcc ascc	Analog Signal Call Control debug
Debug vcc ccac	CCAC debug
Debug vcc iscc	ISDN Call Control Debug
Debug vcc tkcc	Trunk Call Control Debug
Debug vcc port	Use a specific port when debugging

Voice Protocol Module debug mode

This is the function that shows debug messages of the layer close to a device on ports side.

There are parameters of in/out/all that set up Incoming/Outgoing, and deb0/deb1/info/all that set up levels.

Table 11.12 Voice Protocol Module Debug

Command	Purpose
Debug vpm asi	Analog Sub Interface debug
Debug vpm ati	Analog Trunk Interface debug
Debug vpm dti	Digital Trunk Interface debug
Debug vpm ssi	Signal Interface

H323 debug mode

This is the function that shows an H323 debug message, and shows the contents of stack and call-control.

Log displays an appropriate calling number and called number, All displays a debug message regardless of the calling/called number.

Table 11.13 H323 Debug

Command	Purpose
Debug h323 stack	h323 stack related command
Debug h323 vcc	h323 Voice Call Control related command
Debug h323 log	h323 calling or called number log related command

SIP debug mode

This is the function that shows a SIP debug message, and shows the contents of stack and call-control.

Dump is the function that shows a SIP message.

Log displays an appropriate calling number and called number, All displays a debug message regardless of the calling/called number.

Table 11.14 SIP Debug

Command	Purpose
Debug sip stack	SIP stack related command
Debug sip vcc	SIP Voice Call Control related command
Debug sip log	SIP calling or called number log related command
Debug sip dump	Trace SIP msg

Voice debug mode

This is a debug command related to other voice, a user is able to set up the levels (deb0, deb1, info, all) of the displayed message.

Especially the debug voice off command is to turn off all the debugs related to voice.

Table 11.15 Voice Debug

Command	Purpose
Debug voice base	BASE LIB debug
Debug voice bcc	Basc Call Control LIB debug
Debug voie cac	Call Admin Control debug
Debug voice log	LOG class debug
Debug voice nrc	Number Resource Control debug
Debug voice off	debug voice off
Debug voice rmdh	Resource Manager Data Handler debug

Voice Call log Debug

This is a command that displays the call log after starting a voice call.

Table 11.16 Voice Call log Debug

Command	Purpose
Debug call-log	Call log on

CDR Management

Ubigate iBG router transmits the CDR made by processing a call to RADIUS server.

This section describes the method of configuration to manage the CDR and CDR attributes.

Configuration

Restrictions for CDR Management

Works only when an Authentication, Authorization, and Accounting (AAA) RADIUS server is enabled for VoIP calls.

Supports VSA parsing only on those universal gateways that are configured for AAA.

How to Configure RADIUS server

Set up AAA configuration first, and then set up gw-accounting.

- Configuration Steps
 - configure terminal
 - aaa authentication login
 - aaa radius
 - voip-gateway
 - gw-accounting
 - exit
- Detailed Steps

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters global configuration mode.
2	aaa authentication login Example) /configure# aaa authentication login default radius	Configures authentication login information.

(Continued)

Step	Command	Purpose
3	aaa authentication protocol Example) configure #aaa authentication protocol default pap	Configures protocol.
4	aaa radius Example) configure # aaa radius primary 10.254.167.244 configure # aaa radius shared testing123	Configures RADIUS.
5	voip-gateway Example) configure #voip-gateway	Enters voip-gateway configuration mode.
6	gw-accounting Example) configure/voip-gateway# ga-accounting	Configures gw-accounting enable.
7	Exit Example) configure/voip-gateway# exit	Exits the current mode.

CDR Attributes

The CDR in the Ubigate iBG router transmits accounting request packets according to the RADIUS specification described in RFC2865, RFC2866. The attributes described in Table 11.1 below is used and numerous Vendor Specific Attributes are included.

Table 11.17 Attribute List

Attribute type	Length	Attribute Name
30	>=3	Called Station ID
31	>=3	Calling Station ID

Table 11.17 Attribute List (Continued)

Attribute type	Length	Attribute Name
40	6	Account Status Type
44	≥ 3	Account Session ID
26	≥ 7	Vendor Specific Attribute

Standard Attribute

Called Station ID

Attribute type: 30

Length: ≥ 3

This Attribute allows the NAS to send in the Access-Request packet the phone number that the user called, using Dialed Number Identification (DNIS) or similar technology. Note that this may be different from the phone number the call comes in on. It is only used in Access-Request packets.

Calling Station ID

Attribute type: 31

Length ≥ 3

This Attribute allows the NAS to send in the Access-Request packet the phone number that the call came from, using Automatic Number Identification (ANI) or similar technology. It is only used in Access-Request packets.

Account Status type

Attribute type: 40

Length: 6

This attribute indicates whether this Accounting-Request marks the beginning of the user service (Start) or the end (Stop).

It MAY be used by the client to mark the start of accounting (for example, upon booting) by specifying Accounting-On and to mark the end of accounting (for example, just before a scheduled reboot) by specifying Accounting-Off.

Account Session ID

Attribute type: 44

Length: ≥ 3

This attribute is a unique Accounting ID to make it easy to match start and stop records in a log file. The start and stop records for a given session **MUST** have the same Acct-Session-Id. An Accounting-Request packet **MUST** have an Acct-Session-Id.

An Access-Request packet **MAY** have an Acct-Session-Id; if it does, then the NAS **MUST** use the same Acct-Session-Id in the Accounting-Request packets for that session.

vendor specific attribute

Vendor specific attributes used in the Ubigate iBG router are arranged in the following table and the values of VSA attribute field are as follows.

- Type field = 26
- Length field ≥ 7 byte (vendor-string field has to be more than 1byte)
- Vendor-ID field = 70
- String Field is configured as below.
- vendor-type = the VSA number that Samsung has designated
- vendor-length ≤ 247 byte
- vendor-string = the value expressed as ASCII text messages

Table 11.18 Vendor Specific Attribute List

VSA No	Length	VSA Name
4	32	System ID
3	12	Call ID
22	4	Calling Party Type
15	40	Setup Time
16	40	Connect Time
17	40	Disconnect Time
18	12	Disconnect Cause

System ID

VSA No: 4

Length: 32

Ubigate iBG system ip address or domain-name

Call ID

VSA No: 3

Length: 12

Call ID

Calling party type

VSA No: 22

Length: 4

Calling party category. Information on a category of calling party.

Setup time

VSA No: 15

Length: 40

Calling setup time and time format is 'YYYYmmddHHMMSS'. For example, at 08: 09: 10 on the 2nd of January in 2000, input '20000102080910'.

Connect time

VSA No: 16

Length: 40

Calling setup time and time format is 'YYYYmmddHHMMSS'. For example, at 08: 09: 10 on the 2nd of January in 2000, input '20000102080910'.

Disconnect time

VSA No: 17

Length: 40

Calling disconnect time and time format is 'YYYYmmddHHMMSS'. For example, at 08: 09: 10 on the 2nd of January in 2000, input '20000102080910'.

Disconnect cause

VSA No: 18

Length: 12

Calling disconnect cause code. Use Q.850 cause code for disconnect cause code.



CHAPTER 12. Survivable Telephony

This section describes additionally necessary set up for survivable Telephony mode. Survivable Telephony mode is a status where the system cannot be controlled by Call Manager because there are problems in Call Manager interworking such as down or network trouble etc. In this status, Ubigate iBG router independently provides service not only for the calls of POTS ports connected to Ubigate iBG router, but also for the calls of SIP phones allocated in Ubigate iBG router.

To provide secure service in Survivable Telephony mode, set up the additional functions described in this section.

Configuring Call Forward for Survivable Telephony

This section describes how to set up the Call-Forwarding Feature in Survivable Telephony mode. Generally Call Forwarding in Survivable Telephony mode progresses according to the situation of the Call Manager interworking. That is, it operates as a subscriber set up in the Call Manager interworking mode. Besides, in case a subscriber does not set up Ubigate iBG router, it generally provides a method to set up Call-Forwarding Service. That is, in the situation that a call is terminated to a specific FXS port in Survivable Telephony mode, and that port is busy or no answer, if there is no call forwarding set up in Call Manager interworking mode, try call forwarding with the number using the commands as follows.

How to Configure Call Forward-Busy

Configure Call Forward-Busy function for Survivable Telephony mode as in the following procedures.

- Summary Steps
 - configure terminal
 - voip-fallback
 - call-forward busy
 - exit
- Detailed Steps

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters global configuration mode.
2	voip-fallback Example) /configure# voip-fallback	Enters VOIP Fallback configuration mode.
3	call-forward busy <i>forward-number</i> Example) /configure/voip-fallback# call-forward busy 4400	Specifies Call-forward Number for Call Forward-Busy in Survivable Telephony mode.
4	Exit Example) /configure/voip-fallback# exit	Exits the current mode.

How to Configure Call Forward-NoAnswer

Configure Call Forward-NoAnswer function for Survivable Telephony mode as in the following procedures.

- Summary Steps
 - configure terminal
 - voip-fallback
 - call-forward noan
 - exit
- Detailed Steps

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters global configuration mode.
2	voip-fallback Example) /configure# voip-fallback	Enters VOIP Fallback configuration mode.
3	call-forward noan <i>forward-number</i> timeout <i>timeout</i> Example) /configure/voip-fallback# call-forward noan 4400 timeout 30	Specifies Call-forward Number and no answer timeout duration for Call Forward-NoAnswer in Survivable Telephony mode.
4	Exit Example) /configure/voip-fallback# exit	Exits the current mode.

**NOTE**

If a call forwarding number is configured in the subscriber's profile, it uses that forwarding number first and the timeout value is 30 seconds. After 30 seconds, if still there is no answer, the call-forwarding number is configured in voip-fallback mode and timeout is more than 30 seconds, the call will be forwarded to this forwarding number (voip-fallback mode) globally.

If there is no call forwarding number in the subscriber's profile and a call-forwarding number is configured in voip-fallback mode, the call is forwarded to the number in voip-fallback mode.

Configuring System Message for Survivable Telephony

When Ubigate iBG router is converting between Call Manager interworking mode and Survivable Telephony mode, to inform the user that the mode is converting, it sends designated messages through MESSAGE method with a SIP phone.

This section describes how to send the messages.

How to Configure System Message for Survivable Telephony mode

When the Call Manager interworking mode is converted to Survivable Telephony mode, it sets up the message that would be sent to SIP phone as in the following procedures. The default message is 'Survivable Mode'.

- Summary Steps
 - configure terminal
 - voip-fallback
 - system-message survivable
 - exit
- Detailed Steps

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters global configuration mode.
2	voip-fallback Example) /configure# voip-fallback	Enters VOIP Fallback configuration mode.
3	system-message survivable <i>system-message</i> Example) /configure/voip-fallback# system-message survivable 'Survivable Mode'	Specifies message context to inform mode transition from Ubigate iPX interworking to survivable telephony.
4	Exit Example) /configure/voip-fallback# exit	Exits the current mode.

How to Configure System Message for Call Manager interworking mode

When Survivable Telephony mode is converted to Call Manager interworking mode, it sets up the message that would be sent to SIP phone as in the following procedures. The default message is 'Normal Mode'.

- Summary Steps
 - configure terminal
 - voip-fallback
 - system-message normal
 - exit
- Detailed Steps

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters global configuration mode.
2	voip-fallback Example) /configure# voip-fallback	Enters VOIP Fallback configuration mode.
3	system-message normal <i>system-message</i> Example) /configure/voip-fallback# system-message normal 'Normal Mode'	Specifies message context to inform mode transition from survivable telephony to Ubigate iPX interworking.
4	Exit Example) /configure/voip-fallback# exit	Exits the current mode.

Configuring COR List for Survivable Telephony

The Class of Restriction (COR) function enables some calls to be rejected according to the standard of incoming, outgoing COR set in the dial peer. This function provides flexibility in planning the network, and enables a user to block some calls. It is possible to apply call restriction according to a caller's class.

The incoming dial peer COR list is prior to the COR list of outgoing dial peer. In case that there is no COR list in the incoming dial peer, a call is processed regardless of the outgoing COR list (or with regards to). In case that both COR lists are registered, a call is restricted when the incoming COR list is the same as the outgoing COR list, or less than the outgoing COR list.

How to Configure COR list

When the Call Manager interworking mode is converted to Survivable Telephony mode, a user is able to register up to 20 COR lists to be applied.

- Summary Steps
 - configure terminal
 - voip-fallback
 - cor {incoming|outgoing} cor-list-name cor-list-number starting-number ending-number
 - exit
- Detailed Steps

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters global configuration mode.
2	voip-fallback Example) /configure# voip-fallback	Enters VOIP Fallback configuration mode.
3	cor {incoming outgoing} cor-list-name cor-list-number starting-number ending-number Example) /configure/voip-fallback# cor incoming corlist1 1 1001 1005	Configures a COR on dial peers associated with directory numbers.

(Continued)

Step	Command	Purpose
4	Exit Example) /configure/voip-fallback# exit	Exits the current mode.

Verifying COR list

To verify the COR list, perform the following steps.

1. show dial-peer cor.

```
Router# show dial-peer cor

<<< Class of Restriction >>>
  < COR Custom NAME >
    name : corname1
    name : corname2
    name : corname3
  < COR list : corlist1 >
    member : corname1
  < COR list : corlist2 >
    member : corname2
    member : corname3
```

2. show running-config

```
Router# show running-config
.
.
.
voip-fallback
  corlist incoming corlist1 1 6000 6002
  exit voip-fallback
.
.
.
```

Verifying and Troubleshooting commands

Router# show dial-peer cor

Router# show running-config

Configuring Translation for Survivable Telephony

Digit translation is also applicable in Survivable telephony mode. This is a mechanism that handles numbers, automatically modifying or adding area codes or prefixes of the calling and called number. It is applicable not only to the translation rule but also the translation profile. The translation rule is prior to the profile.

How to Configure Translation Rule

- Summary Steps
 - configure terminal
 - voice translation-rule *rule-set-id*
 - rule *precedence* /*match-pattern*/ /*replace-pattern*/
 - exit
- Detailed Steps

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters global configuration mode.
2	voice translation-rule <i>rule-set-id</i> Example) /configure# voice translation-rule <i>rule-set-id</i>	Defines a translation rule for voice calls and enters voice translation-rule configuration mode.
3	rule-match-replace <i>num</i> / <i>match-pattern</i> / / <i>replace-pattern</i> / [<i>match-type type</i>] [<i>replace-type type</i>] [<i>match-plan plan</i>] [<i>replace-plan plan</i>] Example) /configure/voice/translation-rule <i>rule-set-id</i> # rule-match-replace <i>num</i> / <i>match-pattern</i> / / <i>replace-pattern</i> /	Defines a translation rule.
4	Exit Example) /configure/voice/translation-rule <i>rule-set-id</i> # exit	Exits the current mode.

How to Configure Translation Profile

- Summary Steps
 - configure terminal
 - voice translation-profile *prof-name*
 - translate *ruleset-id*
 - exit
- Detailed Steps

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters global configuration mode.
2	voice translation-profile <i>prof-name</i> Example) /configure# voice translation-profile <i>name1</i>	Defines a translation profile for voice calls.
3	translate { called calling } <i>rule-set-id</i> Example) /configure/voice/translation-profile <i>prof-name</i> # translate called 11	Associates a voice translation rule with a voice translation profile.
4	Exit Example) /configure/voice/translation-rule <i>rule-set-id</i> # exit	Exits the current mode.

How to Configure Translation Rule in Fallback Mode

- Summary Steps
 - configure terminal
 - voip-fallback
 - translate { called | calling } ruleset-id
 - exit
- Detailed Steps

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters global configuration mode.
2	voip-fallback Example) /configure# voip-fallback	Enters VOIP Fallback configuration mode.
3	translate { called calling } <i>rule-set-id</i> Example) /configure/voip-fallback# translate called 11	Applies a translation rule to modify the phone number dialed or received by IP phone user while fallback is active.
4	Exit Example) /configure/voip-fallback# exit	Exits the current mode.

How to Configure Translation Profile in Fallback Mode

- Summary Steps
 - configure terminal
 - voip-fallback
 - translation-profile {incoming|outgoing} prof-name
 - exit
- Detailed Steps

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters global configuration mode.
2	voip-fallback Example) /configure# voip-fallback	Enters VOIP Fallback configuration mode.
3	translation-profile {incoming outgoing} <i>prof-name</i> Example) /configure/voip-fallback# translation-profile incoming prof1	Applies a translation profile to modify the phone number dialed or received by IP phone user while fallback is active.
4	Exit Example) /configure/voip-fallback# exit	Exits the current mode.

Verifying Translation Rule

To verify translation rules, perform the following steps.

1. show voice translation-rule number
2. test voice translation-rule number input-test-string [type match-type [plan match-type]]

```

Router/configure# show voice translation-rule all
Translation-rule set id : 1
  Rule 0:
    Rule type : match & replace
    Match pattern : /^33/
    Replace pattern : //
    Match type: none      Replace type: none
    Match plan: none      Replace plan: none

Router/configure# test voice translation-rule 1 332795000

Matched with Rule 1
Original Number : 332795000
Translated Number : 2795000
Original Number Type : none Translated Number Type : none
Original Number Plan : none Translated Number Plan : none

```

3. show running-config

```

Router/configure# show running-config
.
.
voip-fallback
  translate called 1
  exit voip-fallback
.
.

```

Verifying and Troubleshooting commands

```

Router# show voice translation-rule all
Router# test voice translation-rule <rule-id> <num>
Router# show running-config

```



NOTE

If the translation rule or translation profile is configured in voip-fallback mode, when iBG voice gateway turns to survivable mode, no other translation rules and profiles are applied. Only translation rules and profiles of the voip-fallback mode are applied.



CHAPTER 13. Integrated Communication Manager

This chapter provides configuration guidance of Integrated Communication Manager (ICM) features.

Introduction to Integrated Communication Manager Features

Voice Station

Voice Station indicates the subscriber that are managed by Ubigate when SIP Relay server feature is enabled or when Integrated Communication Manager mode is enabled.

Time-based service

Time-based service is a function that accepts, rejects, or forwards a incoming call by schedules. The schedule divides time into three kinds of part. Those are DAY, NIGHT, and HOLIDAY. DAY means business time, and NIGHT means out-of-business time. DAY and NIGHT are defined by time-schedule. HOLIDAY is defined by holiday-schedule and this takes a priority over time-schedule.

Hunt Parallel

Hunt Parallel is a kind of hunt-scheme of Hunt Group. The incoming calls alert all idle stations in the group. The call is connected to the first user to answer the call.

Executive/Secretary service

This is named “shared-group service” in Ubigate and it’s combination of intercom, hold call pickup and Shared-group multi-ring. Refer to shared-group service scenarios.

Intercom

This service allows a users to connect the destination with automatic answer by force by dialing the intercom feature code with an extension.

There is option of ring type and alerting count at destination to notice that intercom call is arrived.

Hold Call Pickup

This service allows a users to pickup the held call which was hold by another user by dialing hold call pickup feature code with hold user’s station umber (not held user’s station number). For example, 1000 hold 2000, 3000 dialing hold-call-pickup fac + 1000 to pickup hold call.

This is useful when a user is hold and another user is retrieve.

Phone Provison

Phone Provisioning is a propriotorily implemented feature in the standard firmware of all snom3xx VoIP phone.

It allows remote administration (configuration and maintenance) of unlimited number of distinct snom phone types and can be used to provide general and specific configuration parameters to the phones.

Automatic Callback

An Automatic Callback feature is computer telephony calling feature that permits a user, when encountering a busy condition or other condition(no-answer) where the called individual is unavailable, to instruct the system to retain the called number and to establish the call when the called number is no longer busy.

Multi-ring

This service enables a user to have multiple destinations ring simultaneously when any calls are received on their phone number. The first destination to be answered is connected.

This service is a user “find-me” service that alerts multiple terminating locations simultaneously. A user can provision up to 3 fineme-number (for example, cell phone, home phone, etc.).

Transfer Recall

Call Transfer Recall, allows for a transferred call to be reconnected to the transferring party if it reaches a failure or no-answer condition after transfer.

Call Override

Override allows a user A to dial a feature access code (FAC) followed by an extension of user B to override the call which was already in talking with user C . When a override occurs, A is talk with B, and C was held by B.

Group Call - Paging

The Group Call service allows a user to call the pilot-number of group-call, whereby the system alerts all members in the group. As the members answer, they are joined into a multi-way conference.

The Group Call service allows an administrator to define a group composed of a list of member users. These members can be part of station number or reachable numbers.

There two type of group call, diapatch is two-way conference call among all members, all members can join this group call by answered by themselves. paging is one-way broadcast call and automatically answered at once. All members are hear the originator's broadcast speech.

The Group Call service is a group service created and operated by a system or service provider administrator.

Note: The total number of members are configurable up to 16, but it recommends that do not configure over 8 parties because of conferece voice quality. New dsp images will be released later.

Ring Group

This system service is to providing a local ringback from Ubigate system regardless of next remote system's behaviour.

The ring groups are administered by operator. The ring group can be made up to 64 and each ring-group include up to 64 patters with one ring id.

When a call coming, search patterns with the called number, if there is matched ring-group, then use the ring-id for that ring-group to ringback.

The "0123456789+*.%^\$\"?[]()T-#" characters can be used for ring pattern in ring-group.

Barge-In with/without warning tone

Barge-in allows a user A to dial a feature access code (FAC) followed by an extension of user B to barge in on the call which was already in talking with user C . When a barge-in occurs, a three-way call is established between B, C and A.

The configurable option for this service is the barge-in warning tone. This option controls whether a warning tone is given to all barge-in participants when a barge-in occurs.

The warning tone option is only configurable by administrators.

Mixer warning tone

This service providing some warning tone to all conference participants when joining to or leaving from the conference mixer. Join and drop tones are different.

Convert COR - Transfer/Forwarding

When user A make a call to user B then, user B try to transfer the call to outside trunk. The COR of the second call through trunk will be judged depends on this option. if this option is set to 'diveter', the cor of this call will be decided upon the user B's station cor, if this option is set to 'oroginator', the cor will be determined on the user A's station cor.

Forwarding is the same as transfer.

The transfer target number and forwarding destination number must be pre-configured at the number-plan with COR type.

Call Forwarding Unreachable

This service allows users to redirect incoming calls to a configurable destination when the user's device is unreachable or unregistered.

This service is activated when user assign the forwarding number by feature code and service will be invoked when the device associated with the called user is not accessible by ICM engine and the service redirects the call to the specified forwarding destination.

Call Forwarding DND

This service allows users to redirect incoming calls to a configurable destination when the user set DND to server. This service is automatically activated when the device associated with the called user is not accessible by BroadWorks, and the service redirects the call to the specified forwarding destination.

Call Forwarding No Answer to VMS

Forwarding a call to VMS depending on its conditions. This service allows users to redirect incoming calls to the VMS system when a configurable destination for each service does not exist. When the forwarding busy conditions are met, if there is no call forwarding busy number on its station and call forwarding busy to VMS is enabled, call will be redirected to VMS system.

Media Connection Point

This feature provides a media proxy which represents obligatory crossroads for media streams in the communications between the terminals – SIP phones – attested to Ubigate Integrated Communication Manager and the networks itself.

The signaling and the RTP stream between the terminals and the networks – SIP trunking networks i.e. ITSP – is always established and managed by MCP.

B-ACD

This feature provides an automatic answering of outside calls with interactive menus that allow callers to select the appropriate department or to dial known extension numbers.

Personal web pages

Personal web pages (PWP) is used only for snomxxx phone. Through web, each station setting and function confirmation are available. Setting is possible only individual phonebook function at the present.

Configuring Integrated Communication Manager

Enable Integrated Communication Manager Features

This section describes how to enable the Integrated Communication Manager features which include features for voice station management.

How to Enable Integrated Communication Manager Features

Enable Integrated Communication Manager.

Step	Command	Purpose
1	configure terminal	Enters global configuration mode.
2	voip-intserver	Enters voip-intserver configuration mode.
3	call-manager	Enable call-manager When the call-manager is set, manage-station is enabled automatically.

Configuring Voice Stations

This section describes how to configure voice stations that is associated with the SIP Phones or Analog FXS phones.

Voice stations indicates the subscribers which is managed by Ubigate. i.e. SIP phones or Analog FXS phones – reside on the local network and Ubigate will manage the devices with this configuration.

If there is no voice stations for SIP phones, Ubigate won't accept SIP phones to be used in the local network.

In the Integrated Communication Manager Mode, all the subscriber should be created and configured in the voice station configuration mode

The primary features of voice stations include:

- A station number for a extension
- Secondary numbers
- Creating dial-peer for call routing.
- Configuring call features to activate or deactivate a specific call feature and numbers such as call forwarding number, pick-up group number, ans so on.

Figure 13.1 shows that voice station 1000 is associated with the pots dial-peer that has the destination-pattern 1000 and the port 0/0/0. Figure 13.2 shows that voice station 2000 is associated with the voip dial-peer that has the destination-pattern 2000. The dial-peers are used for call-routing purposes for incoming or outgoing calls.

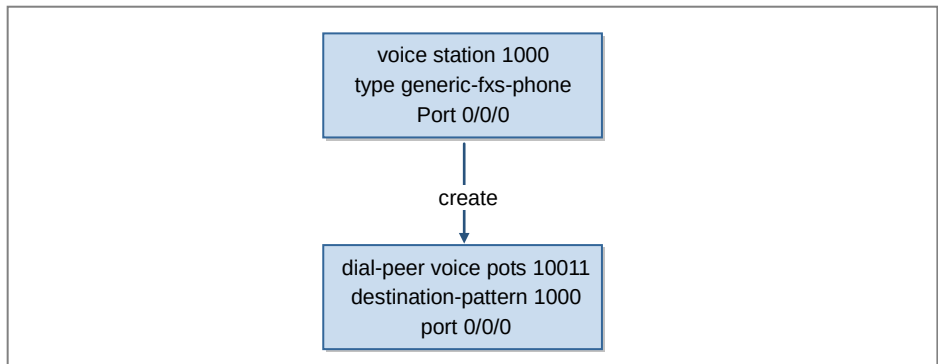


Figure 13.1 Relation of voice station 1000 and pots dial-peer

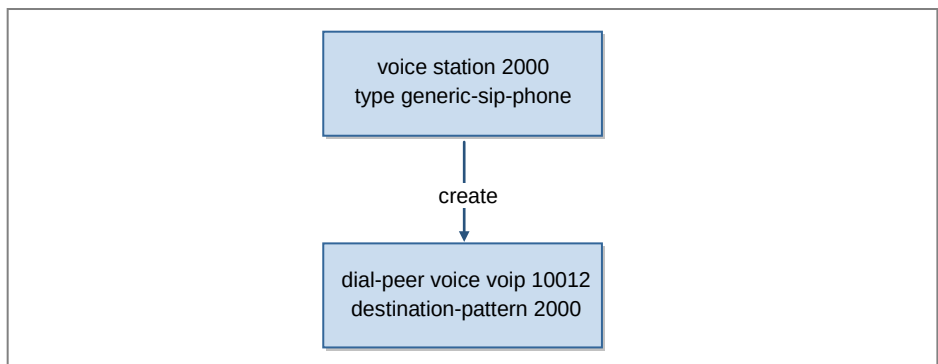


Figure 13.2 Relation of voice station 2000 and voip dial-peer

For example, when the voice station with the number 1000 was defined and type is set to generic-fxs-phone, the following POTS dial peer was automatically created for it : dial-peer voice pots 10011. When the voice station with the number 2000 was defined and type is set to generic-sip-phone, the following VOIP dial peer was automatically created for it : dial-peer voice voip 10012.

How to Configure Voice Stations

Step	Command	Purpose
1	configure terminal	Enters global configuration mode.
2	voice station <number> Example) /configure# voice station 3801	Creates or Modifies a specific voice station.
3	number Example) /configure/voice station 3801# number 2413333801 number 2413333801 2413333802 number 2413333801 2413333802 2413333803	[Optional] Define a secondary telephone number in E.164 format. - Changed to secondary-number
4	type Example) /configure/voice station 3801# type generic-sip-phone /configure/voice station 3801# type generic-fxs-phone	Define type of a station - generic sip phone - generic fxs phone To create dial-peer corresponding to the voice station, 'type' should be set. when 'type' is set, dial-peer is created automatically in the Integrated Communication Manager mode.
5	port Example) /configure/voice station 3801# port 0/0/0	Set the voice port When the type is only generic-fxs-phone, port can be set.
6	routing	Set the configuration mode related to call-routing

(continued)

Step	Command	Purpose
7	huntstop Example) <pre>/configure/voice station 3801/routing# huntstop</pre>	[Optional] Set huntstop To discontinue call hunting behavior for an extension, use the huntstop command in voice station routing configuration mode. To disable huntstop, use the no form of this command.
8	preference <0 – 10> Example) <pre>/configure/voice station 3801/routing# preference 1</pre>	[Optional] Set the preference To order the dial-peers(or voice stations) when multiple dial-peers are matched for a dial string A low preference number is high priority
9	station-cor Example) <pre>/configure/voice station 3801/routing# station-cor emergency</pre>	[Optional] Set the station-cor(class of restriction) To apply the class of restriction in the voice station. The station-cor functionality provides the ability to deny certain call attempts on the basis of the class of restrictions provisioned on the number plan.
10	translation-rule {called calling} <rule-id> Example) <pre>/configure/voice station 3801/routing# translation-rule called 100 /configure/voice station 3801/routing# translation-rule calling 200</pre>	[Optional] Set the translation-rule. To apply a translation rule in order to manipulate the digits.

(continued)

Step	Command	Purpose
11	translation-profile {incoming outgoing} <profile-name> Example) /configure/voice station 3801/routing# translation-profile incoming in_test /configure/voice station 3801/routing# translation-profile outgoing out_test	[Optional] Set the translation-profile. To apply a translation profile in order to manipulate the digits.
12	call-forwarding Example) /configure/voice station 3801# call-forwarding	Enable call forwarding service of a station
13	call-forwarding all <number> Example) /configure/voice station 3801# call-forwarding all 2433332203	Set call-forwarding all number
14	call-forwarding busy <number> Example) /configure/voice station 3801# call-forwarding busy 2433332203	Set call-forwarding busy number
15	call-forwarding no-answer <number> Example) /configure/voice station 3801# call-forwarding no-answer 2433332203	Set call-forwarding no-answer number
16	call-waiting Example) /configure/voice station 3801# call-waiting	Enable call-waiting service of a station

(continued)

Step	Command	Purpose
17	call-pickup-group Example) /configure/voice station 3801# call-pickup-group <number>	Set call pick-up-group number of a station
18	call-3-way-calling	Set 3-way calling service of a Analog station only
19	call-n-way-conference	Set N-way conference service of a station
20	call-park	Set call park service of a station
21	call-return	Set call return service of a station
22	call-screening {disconnect-cause screening-profile outgoing <profile-name>} Example) /configure/voice station 3801# call-screening disconnect-cause no-service /configure/voice station 3801# call-screening screening-profile outgoing profile-test	[Optional] Configure outgoing call screening. 'outgoing' means that station calls to someone. In other words, direction 'outgoing' is not outgoing call but incoming call on the ubigate.. call-screening disconnect-cause <cause> To set the disconnect cause to return when the call is blocked by the Call-block function call-screening screening-profile outgoing <profile-name> To activate the Call-block function by applying the Translation-profile.
23	codec codec-val [<i>interval-time</i>] Example) /configure/voice station 3801# codec g711alaw 20	[Optional] Configure the codec To set the codec type and sampling interval of each codec
24	Description Example) /configure/voice station 3801# description "test station"	[Optional] Set station specific description

(continued)

Step	Command	Purpose
25	do-not-disturb	Set do-not-disturb service of a station
26	find-me-number	Configure find-me-number to set number for PSTN, Mobile..etc
27	follow-me	Set follow-me service of a station
28	last-number-redial	Set last-number-redial service of a station
29	music-on-hold	Set music-on-hold service of a station
30	rtp payload-type { comfort-noise nte <val> } Example) /configure/voice station 3801# rtp payload-type comfort-noise /configure/voice station 3801# rtp payload-type nte 101	[Optional] Set rtp payload-type. This CLI can be set when the type of voice station is only sip. rtp payload-type comfort-noise - to set payload type of RTP (Realtime Transport Protocol) packet to comfort noise type (PT13) in voice station configuration mode. rtp payload-type nte <val> - to set the payload type of the RTP NTE packet to specific value val : A named telephone event. (NTE). number. 0, 96~127. Default value : 101
31	automatic-callback	Set automatic callback service of a station
32	time-base-service	Set time-based-service of a station
33	holiday-service	Configure holiday-service of a station
34	night-service	Configure night-service of a station

(continued)

Step	Command	Purpose
35	shared-service mode {executive secretary} shared-service ring-type {bellCore1 bellCore2 bellCore3 bellCore4 bellCore5 silent} Example) /configure/voice station 1000#shared-service mode secretary /configure/voice station 1000#shared-service ring-type bellCore5	Configure shared service mode and ring-type
36	secondary-number Example) /configure/voice station 3801# secondary-number 1 2413333801 secondary-number 2 2413333801 secondary-number 3 2413333801	[Optional] Define a secondary telephone number in E.164 format.

How to Show Voice Stations

Step	Command	Purpose
-	show voice station summary	Show voice station summary information
-	show show station number <station-number>	Show detailed voice station information for a station

Configure Automatic Callback service

An Automatic Callback feature is invoked when an Ubigate user (A) calls another Ubigate user (B) who is busy or no answer. User A is played an audio prompt indicating the busy condition and is asked whether or not this user would like to call back user B when user B becomes available. If Automatic Callback is confirmed by user A, user B's call status is monitored for a configurable amount of time by **Ubigate ICM Call Engine**. When user B becomes available, Ubigate **Callback Engine** (Automatic Callback Control) initiates a recall toward user A. When user A answers, the call is redirected toward user B.

The system administrator can configure the attributes such below by CLI,

- **Monitor Minutes:** The amount of time to camp out on the busy line, waiting for it to become idle. (Default 30 minutes – Range 5 -180)
- **Max Originator Sessions:** The total number of outstanding Automatic Callback sessions that can be initiated by one subscriber. (Default 2 – Range 1 - 5)
- **Max Terminator Sessions:** The total number of outstanding Automatic Callback sessions that can be initiated toward the same subscriber. (Default 5 – Range 1 – 30)
- **Max Ringing Time:** The maximum amount of ringing time when alerting the originator that the terminator is available. (Default 10 sec – Range 5 – 30 sec)
- **Idle Guard Timer:** Total amount of time from when the B-party becomes available to postpone a callback alert to allow the B-party to make other calls. (Default 10 seconds – Range 5 – 300)
- **Language:** Language code of audio files that used for prompts of automatic callback service.
 - gb: United kingdom
 - it: Italy
 - kr: Korea
 - us: United States

Enable automatic callback Features

This section describes how to enable automatic callback feature.

How to assign a service

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters configuration mode.
2	Voice station xxxx Example) /configure# voice station xxxx	Enters voice station number xxxx
3	automatic-callback Example) /configure/voice/station/1000# automatic-callback	Enable automatic-callbackservice

configure Idle guard timer

```

Ubigate/configure# voip-intserver
Ubigate /configure/voip-intserver# feature-options
Ubigate /configure/voip-intserver/feature-options#
automatic-callback
Ubigate /configure/voip-intserver/feature-options/automatic-
callback# idle-guard-time ?
5 - 300                idle guard time(default : 10
seconds) : 5 ~ 300 seconds

Ubigate /configure/voip-intserver/feature-options/automatic-
callback# idle-guard-time 30
Ubigate /configure/voip-intserver/feature-options/automatic-
callback#

```

configure maximum originator session number

```
Ubigate/configure# voip-intserver
Ubigate /configure/voip-intserver# feature-options
Ubigate /configure/voip-intserver/feature-options#
automatic-callback
Ubigate/configure/voip-intserver/feature-options/automatic-
callback# max-orig-session ?
1 - 5                                max originator sessions(default :
2) : 1 ~ 5

Ubigate /configure/voip-intserver/feature-options/automatic-
callback# max-orig-session 4
Ubigate /configure/voip-intserver/feature-options/automatic-
callback#
```

configure maximum terminator session number

```
Ubigate/configure# voip-intserver
Ubigate /configure/voip-intserver# feature-options
Ubigate /configure/voip-intserver/feature-options#
automatic-callback
Ubigate /configure/voip-intserver/feature-options/automatic-
callback# max-term-session ?
1 - 30                               max terminator sessions(default :
5) : 1 ~ 30

Ubigate /configure/voip-intserver/feature-options/automatic-
callback# max-term-session 6
Ubigate /configure/voip-intserver/feature-options/automatic-
callback#
```

configure maximum ringing time

```
Ubigate/configure# voip-intserver
Ubigate /configure/voip-intserver# feature-options
Ubigate /configure/voip-intserver/feature-options#
automatic-callback
Ubigate /configure/voip-intserver/feature-options/automatic-
callback# max-ringing-time ?
5 - 30                      max ringing time(default : 10
seconds) : 5 ~ 30 seconds

Ubigate /configure/voip-intserver/feature-options/automatic-
callback# max-ringing-time 30
Ubigate /configure/voip-intserver/feature-options/automatic-
callback#
```

configure monitor minutes

```
Ubigate/configure# voip-intserver
Ubigate /configure/voip-intserver# feature-options
Ubigate /configure/voip-intserver/feature-options#
automatic-callback
Ubigate /configure/voip-intserver/feature-options/automatic-
callback# monitor-minutes ?
5 - 180                     monitor minutes(default : 30
mininues) : 5 ~ 180 minutes

Ubigate /configure/voip-intserver/feature-options/automatic-
callback# monitor-minutes 15
Ubigate /configure/voip-intserver/feature-options/automatic-
callback#
```

Show Automatic Callback session information

```
Ubigate/configure# show voice call automatic-callback
-----
Index      Type      Calling Party Number
Called Party Number
-----
0          Busy      1001
1003
-----
Total number of callbacks : 1
-----
Ubigate/configure#
```

Configuring Number-Plan

This section describes how to configure the number-plan to check class of restriction and to reduce the post dial delay. The timeout for the post dial delay can be set using ‘timeout interdigit-short’ command in the voice service pots configuration mode

The Number-Plan is made up of the following components : the pattern, minimum value of the pattern length, maximum value of the pattern length, pattern-type for class of restriction.

- pattern – The called number is matched with this pattern
- min – The minimum length of called number for matching the pattern.
- max – The maximum length of called number for matching the pattern.
- type – pattern type for class of restriction.

The following table describes the permission between class of restriction type in the voice station and pattern type.

Emergency < Internal < Local < Toll < International < premium < superpremium < Unrestricted

For example, If the station is set to “Emergency”, the only calls that are allowed are those which have an “emergency” type identified in the Number-Plan.

If the station is set to “Local”, the only calls that are allowed are those which have an “Emergency” and “Internal” type identified in the Number-Plan.

How to Configure Number-Plan

Step	Command	Purpose
1	configure terminal	Enters global configuration mode.
2	dial-plan Example) /configure# dial-plan	Enter the dial-plan configuration mode to set the number-plan.
3	Number-plan <list-id> Example) /configure/dial-plan# number-plan 1	Enter the number-plan configuration mode.
3-1	pattern <pattern> min <min> max <max> Example) /configure/dial-plan/number-plan 1# pattern 911 min 3 max 3	Set the pattern of number-plan. The number of list is 127,
3-2	type Example) /configure/dial-plan/number-plan 1# type emergency	Set the pattern type for class of restriction. The kinds of type are emergency, internal, local, toll, international, premium, superpremium, unrestricted.

How to Show Number-Plan

Step	Command	Purpose
-	show dial-plan cfg	Show the number-plan
-	show show dial-peer voice summary	Show the dial-peers and number-plan

Hunt Group service

Introduction

The Hunt group service allows incoming calls to a representative number (pilot number) of a hunt group, this forwards the call to a member of the hunt group who can answer the phone using hunting methods including Sequential, Round-robin, Uniform, and Random method. This feature doesn't work in sip-server interworking mode.

Hunt Scheme

The hunt scheme is the selection method for selecting hunt group member. The hunt group with various members uses the hunt scheme to find an idle member for routing the outgoing call. The hunt scheme provided in Ubigate is sequential, round-robin, uniform, random.

Random

The hunt group finds an idle member in random sequence. This method does not involve how call distribution is made between members or whether the single member is used more than other members. Select the member randomly.

Round-Robin

The hunt group finds idle member in sequence. By remembering the previously selected member, the member can be found later following the same sequence.
This method meets the member load balance between hunt group members.

Sequential

Regardless of the previously selected member, Sequential is similar to the round-robin method except that it finds the first idle member.

Uniform

Uniform is similar to the round-robin. This method selects member that has been idle for the longest time.

Parallel

All idle member in the hunt-group are alerted. The incoming call to the hunt-group is connected to the first member to answer the call.

Schedule

Time Schedule

This is to define business hours for the hunt group. When calls is incoming to the group, the group accept or reject or redirect the calls based on time schedule.

Holiday Schedule

This is to define holiday schedule for the hunt group. When calls is incoming to the group, the group accept or reject or redirect the calls based on holiday schedule. This precedes time schedule.

Call Forwarding

Call Forwarding All always

For all of incoming calls to the hunt group, the group always forwards calls to specific number.

Call Forwarding All selective

For all of incoming calls to the hunt group, the group forwards calls to specific number instead of rejecting calls based on holiday and time schedule.

Call Forwarding Busy

The hunt group forwards call to the specific number if all members in the group are busy or not answer.

Call Forwarding No-answer

The hunt group forwards call to the specific number if nobody answer to the incoming call until the wating time expired.

Configuring Hunt Group

See the below table for the method for setting the hunt group.

- Configuration Steps
 - configure terminal
 - holiday-schedule (optional)
 - time-schedule (optional)
 - hunt-group
 - member-number
 - hunt-scheme
 - holiday-schedule (optional)
 - time-schedule (optional)
 - skip-to-next (optional)
 - call-forwarding (optional)
 - exit
- Detailed Steps

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters global configuration mode.
2	voice holiday-schedule <name> example) # configure voice holiday-schedule holiday	Creates holiday schedule for hunt group
3	schedule example) # configure/voice/holiday-schedule holiday# schedule 0 start-date 8 15 2008 end-date 8 17 2008	Set holiday schedule(start, end date)
4	exit	Exits holiday-schedule mode
5	voice time-schedule <name> example) # configure/voice/holiday-schedule time	Creates time schedule for hunt group

(Continued)

Step	Command	Purpose
6	schedule example) # configure/voice/time-schedule time# schedule 0 start-day wednesday start-time 8 0 end- day friday end-time 17 0	Set time schedule(start, end time)
7	exit	Exits time-schedule mode
8	hunt-group <number> Example) sbm/configure# hunt-group 15881000	Creates hunt group. The group's number must be less than 31 letters.
9	Member-numebr <i>precedence</i> number Example) sbm/configure/hunt-group 15881000# member-number 0 3803	Configuring the member-number Precedence value can have the value ranging from 0 to 63.
10	hunt-scheme {random round- robin sequential uniform} Example) sbm/configure/hunt-group 15881000# hunt-scheme sequential	Configuring the hunt-scheme
11	holiday-schedule <name> Example) sbm/configure/hunt-group 15881000# holiday-schedule holiday	Set the holiday schedule name
12	time-schedule <name> Example) sbm/configure/hunt-group 15881000# time-schedule <i>time</i>	Set the holiday schedule name

(Continued)

Step	Command	Purpose
13	skip-to-next <value> Example) sbm/configure/hunt-group 15881000# skip-to-next 20	Configuring the timeout value for skipping to next member
14	call-forwarding all <i>number</i> [all selective] Example) sbm/configure/hunt-group 15881000# call-forwarding all 3001	Configuring call-forwarding all number
15	call-forwarding busy <i>numbe</i> Example) sbm/configure/hunt-group 15881000# call-forwarding busy 3001	Configuring call-forwarding busy number
16	call-forwarding no-answer <i>number</i> [timeout <i>value</i>] Example) sbm/configure/hunt-group 15881000# call-forwarding no- answer 3001 timeout 300	Configuring call-forwarding no-answer number
17	exit	Exits hunt-group mode

Verifying Hunt Group

To check the hunt-group configuration, perform the following steps.

1. `show hunt-group {all | id | sort}`

```
Router/configure# show hunt-group all
Hunt Group Number : 15881000
  member-number 0 38086
  member-number 1 38084
  member-number 2 38085
  member-number 3 38087

  hunt-scheme      : sequential

  holiday-schedule :
  time-schedule    : (Acceptance)

  skipping to next member after 10 sec
  call-forwarding all      :
  call-forwarding busy     :
  call-forwarding no-answer :
```

Verifying and Troubleshooting commands

Router# show hunt-group all

Station Group service

Introduction

The station group is the group of stations. Configuring the station group in the voice-station or in the trunk-group or in the outbound dial-peer determines whether it permits the call or not based on the station group in the voice-station or in the trunk-group or outbound dial-peer. If the voice-station or the trunk-group or the dial-peer is dedicated to the station group, the voice-station or the trunk-group or the dial-peer can only be used for station in the station group.

Configuring Station Group

See the below table for the method for setting the station group.

- Configuration Steps
 - configure terminal
 - voice station-group
 - station-number
 - exit
- Detailed Steps

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters global configuration mode.
2	voice station-group <i>id</i> Example) sbm/configure# voice station-group 1	Create station group. Station group ID can have a single value ranging form 1 to 10000. The number of the station group is 32
3	Station-number <i>number</i> Example) sbm/... /voice/station-group <i>id</i> # station-number 3000	Configure the station-number. Users can configure 64 lists.

Applying Station Group in Dial Peer

Command	Purpose
Station-group <i>num</i> dedication {enable disable} Example) sbm/.../dial-peer/voice/pots 1# station-group 1 dedication enable	Applying Station Group in Dial Peer.

Applying Station Group in Trunk Group

Command	Purpose
Station-group <i>num</i> dedication {enable disable} Example) sbm/.../trunk-group 1# # station-group 1 dedication enable	Applies Station Group in Trunk Group.

Applying Station Group in Voice Station

Command	Purpose
Station-group <i>num</i> dedication {enable disable} Example) sbm/.../voice station 1000# station-group 1 dedication enable	Applies Station Group in Voice Station.

Verifying Station Group

To check the voice station-group configuration, perform the following steps.

1. show voice station-group {all | num | sort}

```
Router/configure# show voice station-group all
Station Group Id : 1
    station-number 3785
    station-number 3786
```

2. show dial-peer voice num id

```
Router/configure# show dial-peer voice num 1
VoiceEncapPeer1
    <<< Dial Peer Common Info >>>
    id = 1, type = pots,
    description = '',
    admin state = 'up', operation state = 'up',
    destination-pattern = `9T`, answer-address = '',
    preference = 2, numbering type = 'none',
    incoming called-number = '',
    connections/maximum = 0/ unlimited,
    decision limit number = '3',
    station-group id = '1 enabled',
    huntstop = `disabled`,
    incoming COR list = `maximum capability`,
    outgoing COR list = `minimum requirement`,
    called translation ruleset id = `0`,
    calling translation ruleset id = `0`,
    incoming translation profile = `none`,
    outgoing translation profile = `none`,
    CLID restrict = 'disabled', CLID remove = 'disabled',
    CLID remove name = 'disabled',
    CLID network number = '', CLID override RDNIS =
    'disabled',
    call block translation-profile = '',
    call block disconnect-cause = 'No Service',
    call local routing = 'enabled',

    <<< Dial Peer POTS Info >>>
    prefix = '',
    forward digits = 'default',
    direct-inward-dial = 'enabled',
```

```

digit strip = 'enabled',
port = '0/2/0:D',
authentication name = '', passwd = '',
sip registration = 'disable',
trunk group = '0 trunk group is registered'
smime = 'disable',
auto-alert = '0',
progress-ind :
    alert = '0', call proceed = '0', connect = '0',
    disconnect = '0', progress = '0',
    setup = '0', setup ack = '0',
progress-ind-locate = 'disable',

<<< Dial Peer Service Info >>>
call waiting = 'disabled',
call pickup group id = ''
call forwarding = 'disabled'
    all-number = '',
    busy-number = '',
    no-answer-number = ''
follow-me = 'disabled', number = ''

service-password = '',
conference: 3-Way Calling = 'disabled',
    N-Way Conference = 'disabled',
music-on-hold: 'disabled', id 0
do-not-disturb: 'disabled'
last number redial: 'disabled', number = ''
call return: 'disabled', number = ''

<<< Dial Peer Statistics Info >>>
Connect Time = 4 seconds,
In Calls = 7, Out Calls = 4
In Ans Num = 3, Out Ans Num = 3
In Fail Num = 4, Out Fail Num = 0
In Abnormal Term Num = 0, Out Abnormal Term Num = 0
In Abandon Num = 0, Out Abandon Num = 1
Last Disconnect Cause is 'CS_UNALLOCATED_NUMBER',
Last Setup Time = 08/21/2008-20:50:57-550 .

```

3. show trunk-group all

```
TRUNK GROUP : tg1
  Type : DS0 Group
  Description :

  Translation profile (incoming) :
  Translation profile (outgoing) :

  Station Group (Dedication : enable) : 1

  Trunk group is Unblocked
  Hunt Scheme is round-robin both up
  Current Calls (incoming): 0
  Current Calls (outgoing): 0
  Max Calls (incoming): unlimited
  Max Calls (outgoing): unlimited

  TG Member : 0/2/0:D(isdn-pri)
    Channel(1) is free
    Channel(2) is free
    Channel(3) is free
    Channel(4) is free
    Channel(5) is free
    Channel(6) is free
  Total available channel : 6 , used: 0 , free: 6
```

Verifying and Troubleshooting commands

```
Router# show voice station-group all
Router# show dial-peer voice num <id>
Router# show trunk-group all
```

Configuring Time-based Service

Configuring Time and Holiday schedules

This section describes how to configure time and holiday schedules for time-based service. Time-schedule is used for defining the office hour. Holiday-schedule has priority over time-schedule.

Warning! These commands are changed the position of CLI tree and modified format in this SNOS version. If these commands are used in old SNOS version, you must re-configure these.

How to configure a time-schedule

Step	Command	Purpose
1	configure terminal	Enters global configuration mode.
2	voice service time-schedule <i>name</i> example) voice service time-schedule time1	Creates a time-schedule with proper name and enters time-schedule configuration mode.
3	schedule <i>num day-of-week start-hour start-min end-hour end-min</i> example) schedule 0 monday 8 30 17 30 schedule 1 tuesday 9 00 18 00	Set time schedules (start, end of the office hour)
4	exit	Exits time-schedule mode.

How to configure a holiday-schedule

Step	Command	Purpose
1	configure terminal	Enters global configuration mode.
2	voice service holiday-schedule <i>name</i> example) voice service holiday-schedule ho1	Creates a holiday-schedule with proper name and enters time-schedule configuration mode.

(continued)

Step	Command	Purpose
3	weekend <i>day-of-week</i> example) weekend saturday weekend sunday	Set the weekend.
4	schedule <i>num</i> start-date <i>month day year</i> [end-date <i>month day year</i>] example) schedule 0 start-date 12 25 2009 schedule 1 start-date 1 1 2010 end-date 1 3 2010	Set holiday schedules (start, end date)
5	exit	Exits holiday-schedule mode.

How to display the configured schedules

Step	Command	Purpose
-	show voice service time-schedule all	Show the time-schedules
-	show voice service holiday-schedule all	Show the holiday-schedules

Configuring Time-based service

This section describes how to configure time-based service. The configuration on the station has priority over system-wide configuration.

How to configure system-wide time-based service

Step	Command	Purpose
1	configure terminal	Enters global configuration mode.
2	voice service timebased-service	Enters time-based service configuration mode.
3	time-schedule <i>name</i>	Set the time schedule.
4	holiday-schedule <i>name</i>	Set the holiday schedule.
5	day-service find-me <i>findme-num</i> example) night-service find-me find-me1	Set the find-me service for office hour.
6	night-service <i>type</i> example) night-service forwarding 3000	Set the service type for out of office hour.
7	holiday-service <i>type</i> example) holiday-service reject	Set the service type for holiday.
8	wait-time-before-fwd night <i>time</i>	Set the waiting time before call is forwarded by night-service. (optional)
9	wait-time-before-fwd holiday <i>time</i>	Set the waiting time before call is forwarded by holiday-service. (optional)
10	enable	Enables system-wide time-based service.
11	exit	Exits time-schedule mode.

How to configure time-based service on the station

Step	Command	Purpose
1	configure terminal	Enters global configuration mode.
2	voice station <i>number</i>	Enters time-based service configuration mode.
3	night-service <i>type</i> example) night-service forwarding 3000	Set the service type for out of office hour. (optional)
4	holiday-service <i>type</i> example) holiday-service none	Set the service type for holiday. (optional)
5	timebased-service	Authorizes time-based service to the station.

How to display the time-based service configuration

Step	Command	Purpose
-	show voice service timebased-service	Show the system-wide time-based service configuration

Configuring Phone Provisioning Service

Prerequisites

First of all, snom-general.template and snom-mac.template shall exist within the CF (/cf0/tftpboot/) which are used to generate the provision files. (both files are released together with SNOS Image)

Configuring Server (TFTP, DHCP)

This section explains how to set up TFTP, DHCP server configuration for phone provision.

TFTP server acts as a provisioning server used to provide the provision files with tftp protocol to snom3xx phone when phone boots.

DHCP server supplies dynamic IP address and informs location of files(snom3xx.htm, snom3xx-<mac>.htm) as tftp server address. And these files are accessed when the phone reboots newly for the first time.

If DHCP server is not a iBG, contact the DHCP server administrator and configure option 66 field with the address of iBG's tftp server.

How to configure

Step	Command	Purpose
1	configure terminal	Enters global configuration mode.
2	tftp_server	Enable tftp server
3	<pre>ip dhcp pool <pool_name> tftpserver tftp://<iBG address> commit example) ip dhcp pool snom360 tftpserver tftp://90.90.13.60 hwaddr 00:04:13:29:08:56 host 90.90.13.176 255.255.0.0 default_router 90.90.13.60 commit exit pool</pre>	Set tftp server address

Generation of global provisioning file

This section explains how to generate general.xml file used for all types of snom phone.

First of all, check if operation status is “Stand-alone ICM mode” because phone provision feature can be used only in case iBG is ICM mode.

File is produced as voip-gateway becomes DOWN to UP.

(Gateway must establish bind information, host domain information to become UP status certainly.)

How to configure

Step	Command	Purpose
1	configure terminal	Enters global configuration mode.
2	voip-gateway shutdown exit	Do gateway so as to do shutdown before converting to ICM mode.
3	voip-intserver call-manager	Change to ICM mode
4	voip-gateway no shutdown exit	Do gateway so as to do no shutdown.

Generation of specific provisioning files

This section explains about creation of snom3xx-<mac>.htm file and snom3xx.htm file including phone specific configuration information by each type.

Creation condition of snom3xx-<mac>.htm is that phone type must be snom3xx certainly. And must set it up to station to the value reading MAC address at phone backside if there is no MAC information.

In case of there is a remote station that want to be monitored, do additionally BLF(Busy Lamp Field) setting.

Files are created when performing save local command.

How to configure

Step	Command	Purpose
1	configure terminal	Enters global configuration mode.
2	voice station <i>number</i>	Enters station configuration mode
3	type <i>type</i> example) type snom320	Set the phone type
4	authentication username <i>username</i> password <i>password</i> example) authentication username 5611 password 5611	Set the user number and password for registration.
5	phone-profile	Enters phone provision configuration mode
6	mac-address <mac_address>	Set the mac address of the phone
7	blfext <i>tag number</i> example) blfext 6 2000	Set the blf info to monitor the remote station. tag: location index of free keys number : station to monitor
8	speed <i>tag number</i> example) speed 7 3000	Set the speed dial configuration. tag: location index of free keys number : destination number
9	save local	Generate or update the provision files(snom3xx.htm, snom3xx-<mac>.htm)

Connect or reboot the phone

Confirm file list in CF(/cf0/tftpboot/) whether general.xml, snom3xx.htm and snom3xx-<mac>.htm are created.

Next, connect the phone to the network or reboot newly if was already linked.

If the phone was linked normally, it receives IP address from DHCP server.

And it receives provision files from TFTP server and configure phone setting with those.

How to verify and reboot

Step	Command	Purpose
1	file	access file commands
2	cd tftpboot ls	List files on /cf0/tftpboot/ device
3	voice reboot station <i>number</i> example) voice reboot station 5611	Reboot a SIP station

Configure Shared-Group Services

Prerequisites

It includes intercom and hold call pickup service. Phone provisioning must be understood.

It is Boss (Executive)/Secretary Service.

Service Scenarios

This configuration is based upon SNOM xxx phones.

1. First of all, make a new shared-group and assign a representative number which is used to external secretary and executive number.
2. Assign an member on that shared-group.
3. At each station which a member of shared-group, assign a mode or ring type depends on it's role.

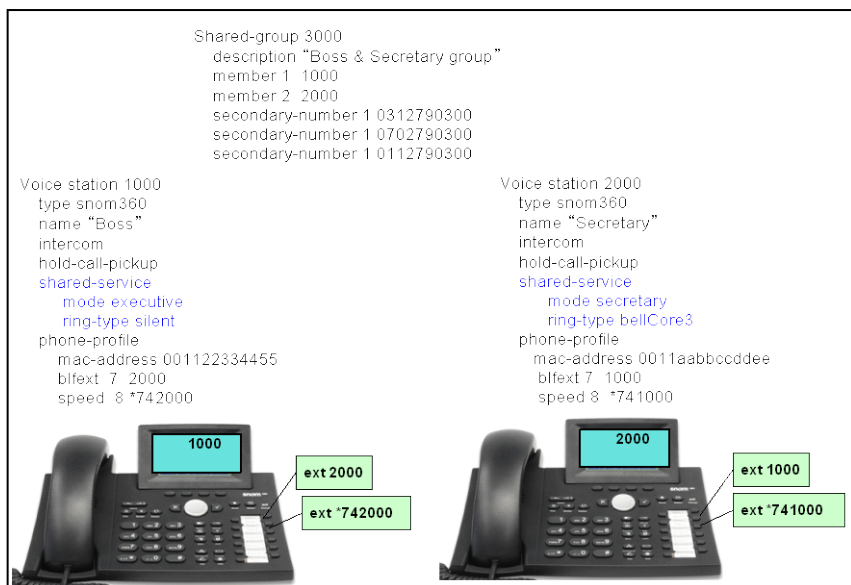


Figure 13.3 Device configuration example for shared-service

Incoming call to shared-group

1. When call is coming to shared-group number 3000, both station 1000 and 2000 are ringing, according to figure1.1, executive 1000 has no ringing, secretary 2000 has ring type bellcore-dr3
2. Secretary got answered.
3. Secretary holds this call. Executive's secretary monitoring blf button is blinking.
4. Secretary push speed dial BLF button to make intercom call to executive.
5. Executive auto-answer and talk with secretary.
6. Secretary let boss know push blinking BLF button to pick up the call which was hold by secretary.
 - 6.a or secretary can attended transfer by pushing "X" button in SNOM phone)
7. Executive push blinking BLF button to pickup hold call. At this time, secretary's intercom call will be held by executive.
 - 7.a secretary's intercom call should be released by secretary side when executive is on line with X.
 - 7.b When executive is on line with X. if executive push "X" button, call is re-transfer between secretary and X if secretary is still didn't released.
 - 7.c if executive select the secretary's intercom hold line (blink), and push "X", then THE call will be cleared.
8. Secretary release the intercom call.
9. Both executive and external caller are on line.
10. The name of shared group member is not shown to external caller.

Making a call from shared-group

1. When executive or secretary making a call to external PTSN or subscriber, the caller is changed to shared-group's representative number 3000
 - It is depends on configuration of "clid shared-group" in shared-service. If this CLI is not configured, the clid of shared group member itself will be shown to called station.
 - Calling Name will be restricted to called station.
2. It is originator alerting state, thus, BLF turn to RED.
3. When opponent was answered, each BLF led turn to RED.

Shared-group configuration

Step	Command	Purpose
1	voice shared-group <i>number</i> Example) /configure# voice shared-group 3333	make a new shared-group with representative number 3333
2	member <0-7> station_number Example) /configure/ voice shared-group 3333# member 0 1000 /configure/ voice shared-group 3333# member 1 2000	add members up to 8.
3	secondary-number <1-3> <i>E.164number</i> Example) /configure/ voice shared-group 3333# secondary-number 1 0602345553333 /configure/ voice shared-group 3333# secondary-number 2 0702345553333	specify up to three secondary-number which is used to destination target for incoming call and caller-id for outgoing call.
4	description « desctiption » Example) /configure/ voice shared-group 3333# description "secretary 2000 and executive 1000"	set description to identify.

Service Assignments

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters configuration mode.
2	Voice station xxxx Example) /configure# voice station xxxx	Enters voice station number xxxx
3	type { snom300 snom320 snom360 snom370 } Example) /configure/voice/station/1000# type snom360	Select a type of this station. The station profile files will be made depends on this type and phone will get this profile and configured.
4	intercom Example) /configure/voice/station/1000# intercom	Enable intercom service.
5	hold-call-pickup Example) /configure/voice/station/1000# hold-call-pickup	Enable hold-call-pickup service
6	clid shared-group Example) /configure/voice/station/1000# clid shared-group	When this station originate a call, the caller id will be changed to one of the shared-group numbers. It is used to hide this station's original number to external.

Shared-service configuration

Step	Command	Purpose
1	shared-service Example) /configure/voice/station/1000# shared-service	Enter shared-service mode. It is related with shared-group configuration.
2	mode { executive secretary } Example) /configure/voice/station/1000/shared-service# mode executive	Select the role of this station within a shared group.
3	ring-type { bellCore1 silent } Example) /configure/voice/station/1000/shared-service# ring-type silent	Select a ring type for the call which is coming to the shared-group number and this station is member of that group.
4	exit	-

Phone-profile configuration

Step	Command	Purpose
1	phone-profile Example) /configure/voice/station/1000# phone-profile	Enter phone-profile configuration mode
2	mac-address <i>max_accress</i> Example) /configure/voice/station/1000/phone-profile# mac-address 00013344bb56	specify max address of this station.
3	blfext <1-12> <i>station_number</i> Example) /configure/voice/station/1000/phone-profile# blfext 1 2000	Assign a function key in snom phone with blf attribution. snom phone will send Subscribe to Ubigate to monitor the status of station 2000.

(continued)

Step	Command	Purpose
4	speed 2 *742000 Example) /configure/voice/station/1000/phone-profile# speed 2 *742000	Assign a function key in snom phone with speed dial attribution. If a user push the second button, snom will make a call with *742000 number. *74 is intercom feature code, Operator should configure a proper feature for its policy.

Verification of configuration

Shared-group configuration

```
DUT1# show voice shared-group all
Shared Group Number : 3333
member-number 0 1000 (EXECUTIVE)
member-number 1 2000 (SECRETARY)
```

Service assignments for each station

```
DUT1# show voice station call-service-list

----- SERVICE ID C C C C G GROUP C C L M P T C H G A P I O H N F D C M T I H B C TYPE: CFA, CFB, CFN, FLN
TYPE `----- OT W P P - I I N O R W L R C R N V L W L N R T B T P A F FORWARDING
ID EXTENSION S R T U U Num D B R H K C C N C B I T R D C M D T R S C U R W NUMBER (TIME)
-----
SIP 2 1000 . y y y y 222 y - y - - * y - - - - - y - - - y y - -
SIP 3 2000 . y - y y 222 y - - 1 - * y - - - - - y - - - y - y y - -

-----
Standalone Mode
(y): supported and configured (-): supported but not configured
(.): not supported in this mode/state (*): service provided by sip station itself

CFA : Call Forward All CFB : Call Forward Busy CFN : Call Forward No Ans CTR : Call Transfer
CWT : Call Waiting CPU : Call Pickup GPU : Group Call Pickup QID : Caller ID Display
CIDB : CID Blocking LCR : Last Number Redial MCH : Music On Hold PARK : Call Park
TWC : Three Way Calling(UA) CC : Conference Call(UA) HLN : Hotline Service GRC : Group Call
ACB : Automatic Call Back PRI V : Privacy CINT : Call Intrusion OVRD : Call Override
HOLD : Call Hold CNFD : Conf & Drop(Avaya UA) NWC : N-way Conference(1PT) FLM : Follow-Me
DND : Do Not Disturb CRT : Call Return MTR : Multi-Ring TBS : Time-based Service
ITOM : Intercom HOPU : Hold Call Pickup BARG : Barge-In
```

Phone profiles

```
DUT1# file ls

WARNING :
Do not remove Compact Flash or reboot during this process.

Contents of /cf0:

  size      date      time      name
  -----
245760    FEB-21-2000   09:09:30   711_3_r
      8      SEP-29-2009   22:00:48   Certificates.dat
     28      SEP-29-2009   22:00:48   Keys.dat
    51200    SEP-30-2009   00:32:14   command.log
      0      DEC-03-2000   21:22:22   config
      0      SEP-30-2009   00:56:14   dhcps.leases
     989     SEP-29-2009   21:51:20   general.xml
     668     SEP-25-2009   20:27:24   shdsakey
     602     SEP-25-2009   20:27:24   shdsakey.pub
     939     SEP-25-2009   02:08:40   snom-general.template
     678     SEP-25-2009   02:09:06   snom-mac.template
     880     SEP-29-2009   22:00:50   snon820-000413241898.htm
     120     SEP-29-2009   22:00:50   snon820.htm
     877     SEP-29-2009   22:00:50   snon860-000413291b71.htm
    757020   DEC-22-2008   11:19:46   snon860-3.38-l.bin
   1525596   DEC-22-2008   11:20:08   snon860-6.5.15-SIP-j.bin
   3458104   DEC-22-2008   11:20:52   snon860-from6to7-1.30-bf.bin
      120     SEP-29-2009   22:00:48   snon860.htm
    11332    SEP-29-2009   22:00:48   system.cfg
.....
```

Subscription Status

Verify that phones are registered and also check the subscription status.

If there is no subscription of dialog info package, blf is not working.

```
DUT1# show sip-registrar
SIP Local Registrar: ENABLE
Registration expiration: min(60s) max(600s)

ID  LINE    IP Address      Port Trans  Expires  Type
-----
 2  1000     90.90.13.201    5060 UDP   3600  3599   snon860/7.3.14
 3  2000     90.90.13.188    5060 UDP   3600  3566   snon860/7.3.14

DUT1# show sip-subscription
<< DialogInfo Package >>

ID  LINE    SUBSCRIBER      CALL-ID      IP-ADDRESS
-----
10013 1000     2000@90.90.13.188 3c2a57c21088-061k9trkfh6 90.90.13.188:2050
10019 2000     1000@90.90.13.201 3c2a55f32edd-8fky602mnhk 90.90.13.201:5060
```



CAUTION

The Subscription of Dialog info package for BLF is solely depends on phone's behavior. When there is no subscription information, log in to SNOM phone Web GUI, and select an "Identify x" and click "Re-register" button till subscription status is on.

Configuration Identity 1

VERSION 7

HTTP Password not set!

Operation

Home

Directory

Setup

Preferences

Speed Dial

Function Keys

Identity 1

Identity 2

Identity 3

Identity 4

Identity 5

Identity 6

Identity 7

Identity 8

Identity 9

Identity 10

Identity 11

Identity 12

Action URL Settings

Advanced

Trusted Certificates

Software Update

Status

System Information

Log

LoginSIPNATRTP

Login Information:

Identity active:

on

off

Displayname:

Account:

2341

Password:

Registrar:

90.90.13.150

Outbound Proxy:

Fallover Identity:

None

Authentication Username:

Mailbox:

Ringtone:

Ringer 1

Custom Melody URL:

Display text for idle screen:

Ring After Delay (sec):

Record Missed Calls:

on

off

Record Dialed Calls:

on

off

Record Received Calls:

on

off

Save

Re-Register

Play Ringer

Remove Identity

Remove All Identities

Subscriptions status

VERSION 7

HTTP Password not set!

Operation

Home

Directory

Setup

Preferences

Speed Dial

Function Keys

Identity 1

Identity 2

Identity 3

Identity 4

Identity 5

Identity 6

Identity 7

Identity 8

Identity 9

Identity 10

Identity 11

Identity 12

Action URL Settings

Advanced

Trusted Certificates

Software Update

Status

System Information

Log

SIP Trace

DNS Cache

Subscriptions

PCAP Trace

Memory

Settings

Outgoing Subscriptions:

From	To	Event	Expires
2341@90.90.13.150	5611@90.90.13.150	dialog	88

Incoming Subscriptions:

From	To	Event	Expires

446

© SAMSUNG Electronics Co., Ltd.

Configure Intercom Services

Enable Intercom Features

This section describes how to enable intercom feature.

How to assign a service

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters configuration mode.
2	Voice station <station number> Example) /configure# voice station 1234	Enters voice station number xxxx
3	type { snom300 snom320 snom360 snom370 } Example) /configure/voice/station/1234# type snom360	Select a type of this station. The station profile files will be made depends on this type and phone will get this profile and configured.
4	intercom Example) /configure/voice/station/1234# intercom	Enable intercom service.

How to change a auto answer options

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters configuration mode.
2	voip-intserver feature-options Example) /configure# voip-intserver feature-options	Enters voice service feature-code mode
3	auto-answer ring-type <bellCore1-silent> answer-after <0-5> Example) /configure/voip-intserver /feature-options# auto-answer ring-type bellCore2 answer-after 2	answer-after <count> : Phone will automatic answer after a number of "count" ringing. If this is "0", no ringing. ring-type: specify the ring type when ringing.

How to change a feature code

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters configuration mode.
2	voice service feature-code Example) /configure# voice service feature-code	Enters voice service feature-code mode
3	intercom *74 max <1-32> min <1-32> Example) /configure/ voice service/ feature-code # intercom *74 max 12 min 4	Change feature code string and minimum and maximum digit number.

Verification of configuration

DUT1# show voice station call-service-list

```
----- SERVICE ID C C C C G GROUP C C L M P T C H G A P I O H N F D C M T I H B C TYPE: OFA, OFB, OFN, FLM
TYPE ----- OT W P P - I I N O R W L R C R N V L W L N R T B T P A F FORWARDING
ID EXTENSION S R T U U Num. D B R H K C C N C B I T R D C M D T R S C U R W NUMBER (TIME)
-----
```

SIP 2 1000 . y y y y 222 y - y - - * y - - - - y - - - y y - y y - -

SIP 3 2000 . y - y y 222 y - - 1 - * y - - - - y - - - - y - y y - -

Standalone Mode

(y): supported and configured

(-): supported but not configured

(.): not supported in this mode/state

(*): service provided by sip station itself

OFA : Call Forward All OFB : Call Forward Busy OFN : Call Forward No Ans CTR : Call Transfer
 CWF : Call Waiting CPU : Call Pickup GPU : Group Call Pickup CID : Caller ID Display
 CIDB : CID Blocking LCR : Last Number Redial MOH : Music On Hold PARK : Call Park
 TVC : Three Way Calling(UA) CC : Conference Call(UA) HLN : Hotline Service GRC : Group Call
 ACB : Automatic Call Back PRIV : Privacy CINT : Call Intrusion OVRD : Call Override
 HCLD : Call Hold CNFD : Conf & Drop(Avaya UA) NWC : N-way Conference(IPT) FLM : Follow-Me
 DND : Do Not Disturb CRT : Call Return MFR : Multi-Ring TBS : Time-based Service
 ITCM : Intercom HCPU : Hold Call Pickup BARG : Barge-In

DUT1 CM# show voice service feature-options

VolP Internal-Server Feature Options (*) : default

Auto-Answer options -----

- ringtype : belCore5
 - answer-after : 1 (1)

Automatic-call back options -----

- idle-guard-time : 10 (10)
 - max-origin-session : 2 (2)
 - max-ringing-time : 10 (10)
 - max-term-session : 5 (5)
 - monitor-minutes : 30 (30)

Transfer options -----

Configure Hold call pickup Services

Enable Hold call pickup Features

This section describes how to enable hold call pickup feature.

How to assign a service

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters configuration mode.
2	Voice station xxxx Example) /configure# voice station xxxx	Enters voice station number xxxx
3	type { snom300 snom320 snom360 snom370 } Example) /configure/voice/station/1000# type snom360	Select a type of this station. The station profile files will be made depends on this type and phone will get this profile and configured.
4	hold-call-pickup Example) /configure/voice/station/1000# hold-call- pickup	Enable hold-call-pickup service

How to change a feature code

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters configuration mode.
2	voice service feature-code Example) /configure# voice service feature-code	Enters voice service feature-code mode
3	hold-call-pickup *75 max <1-32> min <1-32> Example) /configure/voice/station/1000# intercom *74 max 12 min 4	Change feature code string and minimum and maximum digit number.

Verification of configuration

-----		SERVICE ID		CCCCG		GROUP		CCL		MPT		CH		GAP		IO		HN		FD		CM		T		I		H		B		C		TYPE: CFA, CFB, CFN, FLM																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																	
TYPE		-----		OT		WPP		-		I		I		NORW		L		R		C		R		N		V		L		W		L		N		R		T		B		T		P		A		F		FORWARDI NG																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																	
ID		EXTENSION		S		R		T		U		U		Num.		D		B		R		H		K		C		C		N		C		B		I		T		R		D		C		M		D		T		R		S		C		U		R		W		NUMBER		(TIME)																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																	
SIP		2 1000		.		y		y		y		y		222		y		-		y		-		-		*		y		-		-		-		-		-		y		-		y		y		y		y		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-	

Configure Multi-ring Services

Enable Multi-ring Features

This section describes how to enable multi-ring feature.

How to assign a service

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters configuration mode.
2	Voice station xxxx Example) /configure# voice station xxxx	Enters voice station number xxxx
3	findme-number 1 xxxxx findme-number 2 yyyyyy findme-number 3 zzzzzz Example) /configure/voice/station/1000# type snom360	Add the station's reachable number in fine-me number..
4	multi-ring Example) /configure/voice/station/1000# multi-ring	Enable multi-ring service

Verification of configuration

show voice station call-service-list

DUT1# show voice station call-service-list																			
----- SERVICE ID		CCCCCG		GROUP		CCLMPTCH		GAPI		OHNIFDC		MT		IHB		C		TYPE: OFA, OFB, OFN, FLM	
TYPE		OTWPP		IINORW		LR		CRNV		LWL		NRT		BT		PA		F	
ID EXTENSION		SRTUU		Num		DBRHK		CCNC		BIT		RDC		MD		TRS		CURW	
																		NUMBER	
																		(TIME)	
SIP 2 1000		. y y y y		222 y - y		- * y		- - - - -		y - - - -		y y - -		y y - -					
SIP 3 2000		. y - y y		222 y - 1 -		* y		- - - - -		y - - - -		y y - -		y y - -					

Standal one Mode																			
(y): supported and configured (-): supported but not configured																			
(.): not supported in this mode/state (*): service provided by sip station itself																			
OFA : Call Forward All					OFB : Call Forward Busy					OFN : Call Forward No Ans					CTR : Call Transfer				
CWT : Call Waiting					CPU : Call Pickup					GPU : Group Call Pickup					CID : Caller ID Display				
QDB : Q.D Blocking					LCR : Last Number Redial					MOH : Music On Hold					PARK : Call Park				
TWC : Three Way Calling(UA)					CC : Conference Call(UA)					HLN : Hotline Service					GRC : Group Call				
ACB : Automatic Call Back					PRIV : Privacy					CINT : Call Intrusion					OVRD : Call Override				
HOLD : Call Hold					CNFD : Conf & Drop(Avaya UA)					NWC : N-way Conference(1PT)					FLM : Follow-Me				
DND : Do Not Disturb					CRT : Call Return					MTR : Multi-Ring					TBS : Time-based Service				
ITOM : Intercom					HCPU : Hold Call Pickup					BARG : Barge-In									

show voice station number xxxx

Configure Transfer Recall Services

Enable Transfer Recall Features

This section describes how to enable transfer recall feature.

How to configure a service

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters configuration mode.
2	voip-intserver feature-options Example) /configure# voip-intserver feature-options	Enters voice station number xxxx
3	transfer-recall { enable disable } Example) /configure/voip-intserver feature-options# transfer-recall enable	This service is default Enabled.

Configure Call Override Services

Enable Call Override Features

This section describes how to enable override feature.

How to assign a service

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters configuration mode.
2	Voice station xxxx Example) /configure# voice station xxxx	Enters voice station number xxxx
3	override Example) /configure/voice/station/1000# override	Enable override service

How to change a feature code

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters configuration mode.
2	voice service feature-code Example) /configure# voice service feature-code	Enters voice service feature-code mode
3	override *75 max <1-32> min <1-32> Example) /configure/voice/station/1000# override *78 max 12 min 4	Change feature code string and minimum and maximum digit number.

Configure Group Call (Dispatch, Paging) Services

group-call group configuration

Step	Command	Purpose
1	voice group-call <i>pilot-number</i> Example) /configure# voice group-call 3333	make a new group-call group with pilot number 3333
2	member <0-15> number Example) /configure/ voice shared-group 3333# member 0 1000 /configure/ voice shared-group 3333# member 1 2000	add members up to 16 in CLI but. It is recommend that do not configure over 8 members because of mixing voic quality, Next release will be supported up to 16 members.
3	call-type { dispatch paging } Example) /configure/ voice group-call 3333# call-type dispatch	Configure group call type. Dispatch : two-way conference call Paging: one-way broadcasting call with auto-answer.
4	description « desctiption » Example) /configure/ voice group-call 3333# description "dispatch for xxxxx"	set description to identify.

Verification of configuration

**show voice group-call { all | name <name> | sort { ascending | descending }
| summary }**

DUT_ICM/configure# show voice group-call summary

Group number	Type	Descriptions / Members
2222	dispatch	test group call
		0 5611
		1 0002
2223	paging	
		0 5611
		1 0002
		2 5700

Configure Barge-In Services

Enable Barge-In Features

This section describes how to enable barge-in feature.

How to assign a service

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters configuration mode.
2	Voice station xxxx Example) /configure# voice station xxxx	Enters voice station number xxxx
3	barge-in Example) /configure/voice/station/1000# barge-in	Enable barge-in service

How to change a feature code

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters configuration mode.
2	voice service feature-code Example) /configure# voice service feature-code	Enters voice service feature-code mode
3	barge-in *75 max <1-32> min <1-32> Example) /configure/voice/station/1000# barge-in *78 max 12 min 4	Change feature code string and minimum and maximum digit number.

Enable Barge-in warning tone Features

This section describes how to enable Barge-in warning tone feature.

How to configure a service

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters configuration mode.
2	voip-invserver feature-options Example) /configure# voip-intserver feature-options	Enters voice station number xxxx
3	barge-in-warning-tone { enable disable } Example) /configure/voip-intserver feature-options# barge-in-warning-tone enable	This service is default Disabled .

Configure Ring-Group Services

Ring-group configuration

Step	Command	Purpose
1	voice ring-group <i>name</i> Example) /configure# voice ring-group test	make a new ring group with name "test"
2	pattern <0-63> <i>patteerns</i> Example) /configure/ voice ring-group test# pattern 0 5.... pattern 1 ##....T pattern 2 [2-5].. pattern 3 9.....+	add patterns for this ring-group
3	ring-id <1-10> Example) /configure/ voice ring-group test# call-type dispatch	configure ring-id for this ring-group. verify using show voice service media
4	description « desctiption » Example) /configure/ voice ring-group test# description "ring-group for xxxxx"	set description to identify.

Verification of configuration

```
show voice ring-group { all | name <name> | sort { ascending |
descending } | summary }
```

Configure Convert COR Services

Enable Convert COR Features

This section describes how to enable convert COR feature when transfer or call forwarding.

How to configure a service

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters configuration mode.
2	voip-intserver feature-options Example) /configure# voip-intserver feature-options	Enters voice station number xxxx
3	convert-cor-transfer { originator diverter } convert-cor-forward { originator diverter } Example) /configure/voip-intserver feature-options# convert-cor-forward originator	Default is diverter. Originator: Original caller to diverter. Diverter: Transferor or Forwarder who diver this call to final destination.

Configure Mixer Warning Tone Services

Enable Mixer Warning Tone Features

This section describes how to enable mixer warning tone feature when when joining to or leaving from the conference mixer.

How to configure a service

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters configuration mode.
2	voip-invserver feature-options Example) /configure# voip-intserver feature-options	Enters voice station number xxxx
3	mixer-warning-tone { enable disable } Example) /configure/voip-intserver feature-options# mixer-warning-tone enable	Enable the warning tone when joining to or leaving from the conference mixer. This is for conference services Default enabled.

Verification of configuration

show voice service feature-options

Configure Call Forwarding Unreachable Services

Enable Call Forwarding Unreachable Features

To enable Call Forwarding Unreachable service, enable the services and configure a forwarding number in case of unreachable for SIP phone for example, sip phone not registered.

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters global configuration mode.
2	voice station <number> Example) /configure# voice station 3333	Enter voice station with number to assign service.
3	call-forwarding unreachable number Example) /configure/voice station 3333# call-forwarding unreachable 7777	Setup forwarding target number by CLI or by feature code.

Configure Call Forwarding DND Services

Enable Call Forwarding DND Features

To enable Call Forwarding DND service, enable the services and configure a forwarding number in case of DND setup by feature code from SIP phone or Analog FXS station.

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters global configuration mode.
2	voice station <number> Example) /configure# voice station 3333	Enter voice station with number to assign service.
3	call-forwarding unreachable number Example) /configure/voice station 3333# call-forwarding dnd 77777	Setup forwarding target number by CLI or by feature code.

Configure Call Forwarding VMS Services

Enable Call Forwarding VMS Features

To enable Call Forwarding VMS service, enable the services and configure 'vms' instead of a forwarding number in case of all/busy/no-answer for the SIP phone or Analog FXS station.

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters global configuration mode.
2	voice station <number> Example) /configure# voice station 3333	Enter voice station with number to assign service.
3	call-forwarding <case> vms Example) /configure/voice station 3333# call-forwarding busy vms	Setup forwarding target to vms by CLI or by feature code.

Configure Huntgroup logout Services

Enable Huntgroup logout Features

This section describes how to enable huntgroup logout feature.

How to enable a service

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters configuration mode.
2	voip-intserver feature-options Example) /configure# voip-intserver feature-options	Enters feature-option mode.
3	huntgroup-logout <enable disable> Example) Huntgroup-logout enable	Enable or disable huntgroup logout features. Default: enable
4	huntgroup-autologout <count> Example) Huntgroup-autologout 5	Enable autologout services for the hunt-group. If this command is set and a member does not answer the huntgroup call, the member will be logged out automatically. Count 0 means disablement of this service.(Default: 0).

How to configure SNOM key for huntgroup logout

Step	Command	Purpose
1	configure terminal	Enters global configuration mode.
2	voice station <i>number</i>	Enters station configuration mode
3	type <i>type</i> example) voice station 3000# type snom360	Set the phone type
4	authentication username <i>username</i> password <i>password</i> example) authentication username 5611 password 5611	Set the user number and password for registration.
5	phone-profile	Enters phone provision configuration mode
6	mac-address <mac_address>	Set the mac address of the phone
7	speed <i>tag number</i> example) voice station 3000/phone-profile# speed 8 *80	Set the feature code of huntgroup logout to a button on sip phone as speed dial attribute. tag: location index of free keys number : feature code
8	save local	Generate or update the provision files(snom3xx.htm, snom3xx-<mac>.htm)

After this, SNOM phone must be rebooted for updating provision files.
When sip phone is in registration, using ‘voice reboot station <station number>’ CLI to reboot SNOM phone.

Configuring Media Connection Point (MCP)

Prerequisites

MCP provides media proxy services between two different network regions. The system region represents the local network where all terminals reside. On the other hand, the public region represents the public network via SIP trunk. The public network could be ITSP – Internet Telephony Service Provider. MCP manages both signaling – i.e. SIP protocol – and RTP streams.

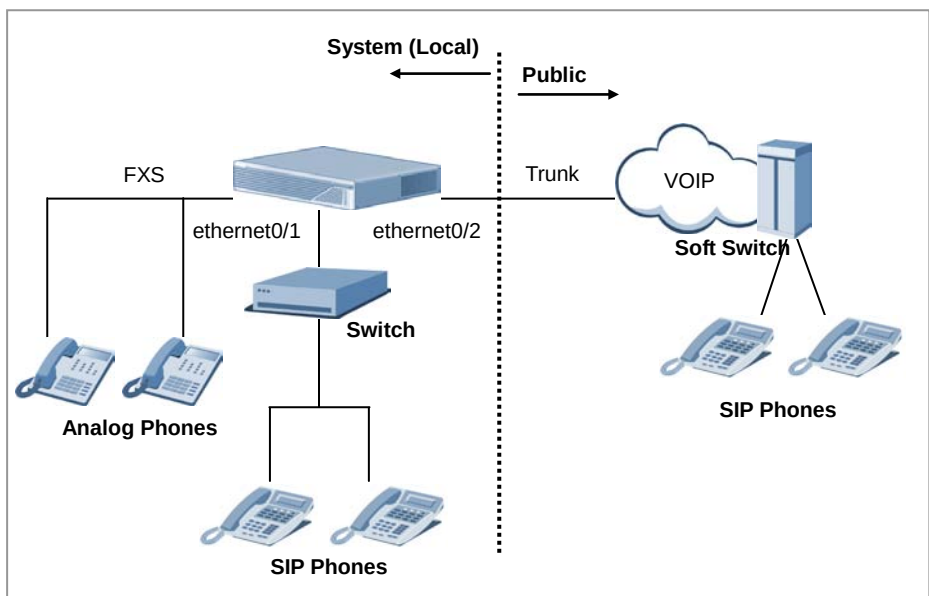


Figure 133.4 MCP Network Diagrams

There are some restrictions for MCP services.

1. Two regions and two media-pools are required.
2. One media-pool must be “system”. And the system media-pool must be same to the interface bound by “Integrated Communication Manager”
 - The interface bound by “voip-gateway” configuration.
3. The other media-pool must be “public”. And the public media-pool must be different from the “system” media-pool.

4. The name of regions are same to that of media-pools. The “public” region must be created and assigns interfaces for this region while the “system” region should not. The “system” region is internally maintained.

Media-pool	Interface	Region	Description
system	Same to “voip-gateway” bound interface	Internally maintained	where ICM and all subscribers reside
public	Outbound interface where public calls come and go	Must be created and assigned	-

How to enable Allow-interfaces on VoIP Gateway

In order to provide the MCP service, ICM should be able to accept SIP signaling messages from local and public interfaces. This is “Allow-interfaces” feature that enables Ubigate could accept SIP signaling messages from any interface.

The existing “bind interface” configurations for control and media should be well configured before enable this feature.

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters configuration mode.
2	voip-gateway Example) /configure# voip-gateway	Enters voip-gateway mode
3	any-interface Example) /configure/voip-gateway# bind control any-interface	Allow the SIP UA to accept incoming SIP messages from any interface.

How to configure MCP

The following steps describe how to enable MCP service.

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters configuration mode.
2	voip-intserver Example) /configure# voip-intserver	Enters voip-intserver mode
3	media-proxy Example) /configure/voip-intserver# media-proxy	Enters media-proxy mode
4	media-pool {system} Example) /configure/voip-intserver/media-proxy# media-pool system	Creates the system media-pool.
5	ip-address A.B.C.D Example) /configure/voip-intserver/media-proxy/media-pool system# ip-address 192.168.1.100	-
6	media-port {start-port} {range} Example) /configure/voip-intserver/media-proxy/media-pool system# media-port 40000 1000	-
7	media-pool {public} Example) /configure/voip-intserver/media-proxy# media-pool public	Creates the public media-pool.

(continued)

Step	Command	Purpose
8	ip-address A.B.C.D Example) /configure/voip-intserver/media-proxy/media-pool public# ip-address 90.90.13.10	-
9	media-port {start-port} {range} Example) /configure/voip-intserver/media-proxy/media-pool public# media-port 41000 1000	-
10	region {public} interface {interface name} Example) /configure/voip-intserver/media-proxy# region public interface ethernet 0/2	Assign interfaces for the public region. Only sessions come and go through this interfaces would get media-proxy services.
10	no shutdown Example) /configure/voip-intserver/media-proxy# no shutdown	Start the MCP service.

Verification of configuration

This section describes how to verify MCP configuration corresponding “interface” and “voip-gateway” configuration. This examples are based on “MCP network diagrams” in *Prerequisites* section.

Media Pool configuration

Ubigate# show media-proxy media-pool

```
Media-pool name : system [0]
  IP address : 192.168.1.100
  Port Range : Start=40000, Range=1000, (40000 - 41000)

Media-pool name : public [1]
  IP address : 90.90.13.10
  Port Range : Start=41000, Range=1000, (41000 - 42000)
```

The IP address of the “public” media-pool must be equivalent to that of the outbound interface for public calls. In this example, IP address 90.90.13.10 of media-pool “public” is same to the IP address of “ethernet0/2”

Ubigate# show ip interface brief

Interface	Type	IP-Address/Mask
Status		
ethernet0/1	ETHERNET (802.3)	192.168.1.100/24
Up		
ethernet0/2	ETHERNET (802.3)	90.90.13.10/24
Up		

And thus, the IP address of the system media-pool must be equivalent to that of the interface bound by “Integrated Communication Manager” – i.e. voip-gateway.

In this example, interface “ethernet0/1 (192.168.1.100)” for the “system” media-pool is same to the interface bound by “voip-gateway”.

Ubigate# show voip gateway

```

VoIP Gateway Status
Gateway Admin Status      : UP
Gateway Operation Status  : Stand-alone ICM mode (Ready)

Gateway IP address
  Binding status : ethernet 0/1, ethernet 0/1
  Control IP address : ipv4:192.168.1.100 [Allow any-
interface]
  Media IP address   : ipv4:192.168.1.100

```

Show Media Session

Ubigate# show media-proxy media-session brief

Id	Type	Proxy Addr:Port		PeerAddr:Port(U)	
		OrigSdpAddr:Port	send	recv	
2	REQ	90.90.13.1:41002	549	560	n/a
2	RESP	172.1.1.7:40002	559	549	n/a

Configuring Basic Automatic Call Distributor (B-ACD)

Overview

A Basic Automatic Call Distributor (B-ACD) service is available to provide the following functionality.

- Automatic answering of outside calls with interactive menus that allow callers to select the appropriate department or to dial known extension numbers.
- Call queues for hunt groups that route calls for different menus.

B-ACD provides automatic answering and call distribution for calls through interactive menus and local hunt groups.

An incoming call from outside dials the B-ACD pilot number and hears a prompt that provides a greeting and instructions to help the caller automatically route the call.

For example, calls to a company might hear: “Thank you for calling. For sales press 1, for customer service press 2, to dial by extension press 3, to speak to an operator press zero.”

After a caller presses a digit to be connected to a particular department or service, the call is routed to a call queue for a hunt group or station that has been set up to answer calls for that department or service. If an agent is available in the hunt group, the call is connected. If no agent is available in the hunt group, the call goes to call queue. While the call is in the queue, the caller hears music on hold. At intervals, the caller hears a second greeting audio prompt. From the queue, the call periodically reattempts to connect to a phone in the hunt group. If no agent becomes available within a specified period, the call is routed to an alternate, configurable destination.

How to Configure B-ACD

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters configuration mode.
2	voice application Example) /configure# voice application	Enters voice application configuration mode
3	acd service name Example) /configure/voice application# acd test	Create new acd service or enter the service
4	mode {interactive drop-through} Example) /configure/voice/application/acd test# mode interactive	Set operation mode of an ACD service
5	language {gb it kr us} Example) /configure/voice/application/acd test# language kr	Define the language code of audio files that are used for prompts in an ACD service
6	pilot-number <digit string> Example) /configure/voice/application/acd test# pilot-number 1000	Set the representative number to be dialed into an ACD service
7	alternate-number<number> Example) /configure/voice/application/acd test# alternate-number 9999	Optional) Set the alternate destination for calls that are not answered by a routed hunt group.

(continued)

Step	Command	Purpose
8	hunt-menu <1-9> <hunt pilot number> Example) /configure/voice/application/acd test# hunt-menu 1 2000 /configure/voice/application/acd test# hunt-menu 2 3000	Associate a menu number with a hunt group pilot number. The operator hunt menu 0 will be assigned automatically with the last hunt-menu number.
9	dial-by-ext-menu <1~9> Example) /configure/voice/application/acd test# dial-by-ext-menu 3	Set dial-by-extension services menu number that allow the caller could dial into the specific extension.
10	max-extension-length <3~16> Example) /configure/voice/application/acd test# max-extension-length 4	Set the maximum number of digits that can be dialed by callers using the dial-by-extension option.
11	prompt-welcome <prompt index> Example) /configure/voice/application/acd test# prompt-welcome 1110	Define welcome prompt audio file index for an ACD service. The default prompt index is 1110. User can change welcome prompt index between 1121~1200. But an audio file should be exist in /CF0/AnnCfg and it should be loaded to memory before enable the ACD service. For example, an user set language of an ACD to "kr" and set prompt welcome to 1130, then the audio file named "kr-1130.pcm" and/or "kr-1130.g729" should be in /CF0/AnnCfg and be loaded to memory. All the other prompts are follows same rule above" Verify with "show voice service media" CLI.

(continued)

Step	Command	Purpose
12	prompt-menu <prompt index> Example) /configure/voice/application/acd test# prompt-menu 1111	Define option menu prompt audio file index for an ACD. The default prompt index is 1111.
13	prompt-second-greeting <prompt index> Example) /configure/voice/application/acd test# prompt-second-greeting 1112	Optional) Define second prompt audio file index for an ACD. The default prompt index is 1112.
14	music-on-hold <prompt index> Example) /configure/voice/application/acd test# music-on-hold 1120	Define music on hold audio file index for an ACD. The default prompt index is 1120.
15	second-greeting-time {seconds} Example) /configure/voice/application/acd test# second-greeting-time 60	Optional) Define the time delay before the second greeting is played after caller joins an ACD call queue. The range is 30-120 seconds. Default value is 60 seconds.
16	menu-timeout {times} Example) /configure/voice/application/acd test# menu-timeout 5	Set the number of times an ACD will loop the menu option before connecting the caller to an operator. The range is 0 ~ 10 times. Default value is 4 times.
17	alternate-max-retry-count {times} Example) /configure/voice/applicatoin/acd test# alternate-max-retry-count 3	Optional) Set the maximum number of retry time that an ACD should try to get to the alternate destination. The range is 1 ~ 3 times. Default value is 1 time.

Configure Call Queue

The incoming calls to B-ACD service are transferred to call queues associated with hunt groups. If a member of the hunt group is available to take a call, the call is connected. If no member of the hunt group is available, the call remains in the call queue for that hunt group and caller hears music on hold. A call queue, although dedicated to a particular hunt group, is managed by the B-ACD not by the hunt group itself.

Step	Command	Purpose
1	configure terminal Example) # configure terminal /configure#	Enters configuration mode.
2	voice service call-queue {pilot-number} Example) /configure#voice service call-queue 3000	Create a call queue for a hunt group. The pilot-number of this call-queue is the pilot-number of relevant hunt-group.
3	queue-length <1-30> Example) /configure/voice/service/ call-queue 3000/ queue-length 10	Set the maximum number of calls could be queued in each hunt group queue.
4	call-retry-timer {seconds} Example) / configure/voice/service/ call-queue 3000/ call-retry-timer 20	Set the amount of time that a call should wait until the call gets connected to the hunt group. The range is 1 ~ 30 seconds. Default value is 15 seconds.
5	call-retry-max-time {seconds} Example) / configure/voice/service/ call-queue 3000/ call-retry-max-time 360	Set the maximum amount of time for the call-retry timer. The range is 20 ~ 3600 seconds. Default value is 600 seconds.

Verification of configuration

Show ACD configuration

Step	Command	Purpose
1	show voice application acd name {service name} Example) /show voice application acd name test	Show an ACD configuration.

Show call-queue configuration and status

Step	Command	Purpose
1	show voice service call-queue Example) /show voice service call-queue	Show a call-queue configuration and status.

Audio Prompts Files

The welcome and other prompts are audio files that is played when a call is answered by ACD pilot number. These audio files are used with B-ACD service to inform callers of their status and any actions that they may take. The default audio files will be released with SNOS image. In particular, you can create personalized audio files to describe the menu choices that are available to your callers.

Default Audio Files

Defaults audio files are provided for each point in the ACD operation at which prompts are given to callers. The audio files will be provided with SNOS image. The audio files are bundled in a tar archive called `ibg_audio_prompt_x.x.x.tar`. The audio files and their messages are listed in Table 1. You can rerecord personalized messages over the defaults messages, but you should not change the names of the audio files.

The filename of audio files consists with prefix and index of prompts. The prefix can be changed to represent any of the following language packages :

- gb–United Kingdom
- it–Italy
- kr–Korea(default)
- us–United States

Default Filename	Default Annoiucement
<pre><prefix>_1000.pcm ~ <prefix>_1100.pcm <prefix>_1000.g729 ~ <prefix>_1100.g729</pre>	Digits, from 0 to hundred.
<pre><prefix>_1110.pcm <prefix>_1110.g729</pre>	Default welcome prompt
<pre><prefix>_1111.pcm <prefix>_1111.g729</pre>	Default menu prompt
<pre><prefix>_1112.pcm <prefix>_1112.g729</pre>	Default second greeting prompt
<pre><prefix>_1113.pcm <prefix>_1113.g729</pre>	Default disconnect prompt
<pre><prefix>_1114.pcm <prefix>_1114.g729</pre>	Default invalid option prompt
<pre><prefix>_1115.pcm <prefix>_1115.g729</pre>	Default dial-by-extension menu prompt
<pre><prefix>_1116.pcm <prefix>_1116.g729</pre>	Default all busy prompt

Install Audio Prompts

To install the audio prompts, follows the steps.

1. Copy audio archive file named “ibg_audio_prompts_x.x.x.tar” to Compact Flash (/CF0).
2. Enter “file” command
3. Enter “tar extract ibg_audio_prompts_x.x.x.tar”
4. Enter “ls” command, and you can find new directory “AnnCfg.”
5. Enter “cd AnnCfg”, and you can find default audio files.
6. Enter “reboot” command

How to Configure Announcement Prompt Files

Announcement Prompt File indicates the voice sound source which is managed by Ubigate. If there is no voice source for voip service, Ubigate won't service the Interactive Voice Response. After configuration them, Ubigate must be rebooted for Adjusting them.

Step	Command	Purpose
1	configure terminal	Access file commands
2	tar extract <AnnName.tar>	Extract Announcement Prompt Files from tar file

How to Show Announcement Prompt Files

Step	Command	Purpose
-	show voice service media	Show Announcement Prompt Files information

How to Load Announcement Prompt File

Step	Command	Purpose
1	configure terminal	Enters global configuration mode.
2	voice service media load-media <AnnFile>	Load Announcement File to memory

How to UnLoad Announcement Prompt File

Step	Command	Purpose
1	configure terminal	Enters global configuration mode.
2	voice service media unload-media <AnnFile>	Unload Announcement File from memory

Configuring Personal Web Pages Service

Prerequisites

Personal web pages(PWP) is available after snom phone registers to MSBG ICM.

Only IE5.5 above browser and firefox3.5 can be used for PWP, and cancel popup window interception. In case of firefox browser, web access through HTTPs is not available at this time.

Configuring Server(HTTP, HTTPs)

To use PWP function, MSBG ICM's HTTP or https server must be run.

How to enable http servers

Step	Command	Purpose
1	configure terminal	Enters global configuration mode.
2	ip http server	Enable http server
3	ip http secure-server	Enable https server

Confirm whether relevant files exist for pwp service

Necessary files(pwp.htm, pwplogin.htm, logout.htm, errlogin.htm, samsung.jpg) should exist under / cf0/pwp/ to access to PWP. Files are offered at release time with SNOS image.

How to check files

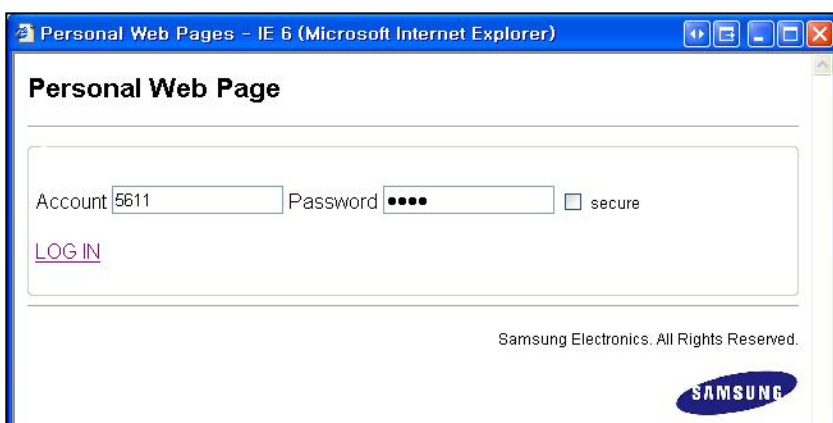
Step	Command	Purpose
1	configure terminal	Enters global configuration mode.
2	file	access file commands
3	cd pwp	Change working directory
4	ls	List files on /cf0/pwp device

Connect to personal web page

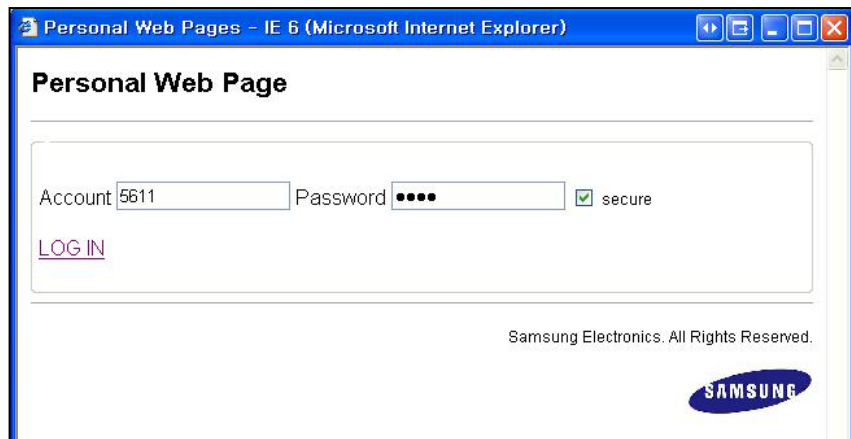
Registered station subscriber can connect to PWP with following URL.
If connect to <http://ICM IP address/pwp/> or <https://ICM IP address/pwp/>, login screen appears as popup. Login ID is station number and password is authentication password.

How to login

1. Input URL(ex. MSBG iBG binding IP address: 90.90.13.60)
<http://90.90.13.60/pwp/>
2. Login with HTTP

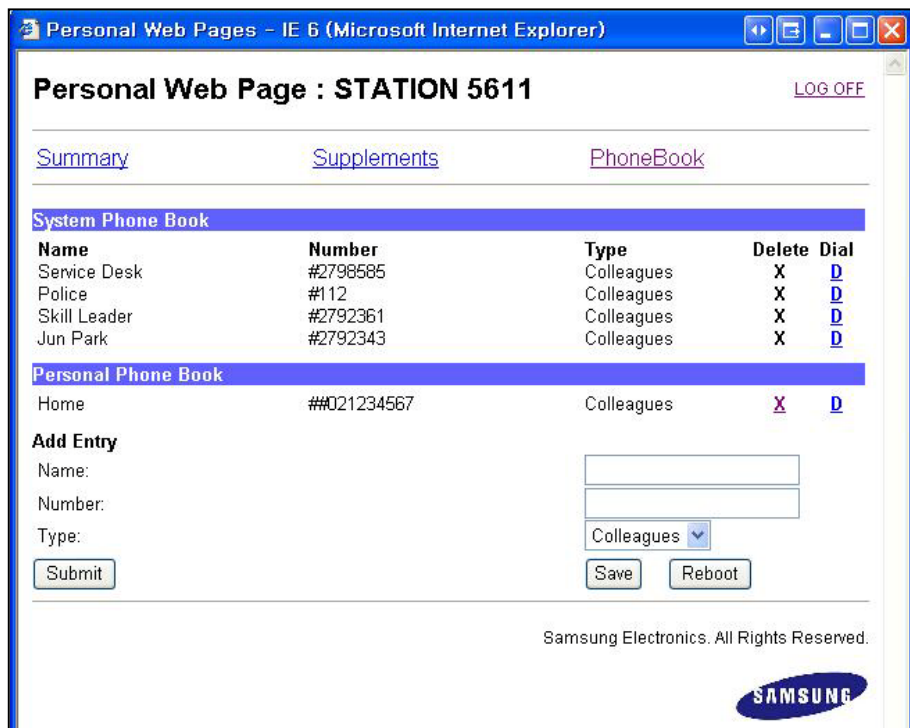


3. Login with HTTPs



Configure personal phone book

Individual phonebook is possible. For phone book is possible entry addition, clear through PWP.



How to add entry of phone book

After inputting person's a name and number to add, an entry is added when the “Submit” button is pressed.

How to save phone book file

When pressing “Save” button, phonebook.csv and phone provision profile that save phone book information of system are updated.

How to apply phone book to snom phone

Reboot the phone or push the “Reboot” button in order to apply the phonebook to phone.

How to delete entry of phone book

Deletion is possible when the entry is added by user. Push the ‘X’ button and “Save”, “Reboot” button, changed phonebook is applied to phone.

How to click to dial

Click to dial function from PWP is only for snom phone. Push the ‘D’ button when you want to call the peer in phonebook. Actually, Call is accomplished using the snom phone.

Exit from Personal web page

In 3 kinds occasion, become log out.

How to log off session

1. “LOG OFF” button is pushed.
2. Window ‘x’ button is pushed.
Become automatic log off by session timeout if doing nothing for 300 seconds after Log in.

Configuring Voice Mail (Internal Voice Mail)

Prerequisites

IVM provides the voice mail services to the subscribers. Internal voice mail is normally the system of managing voice messages for the subscribers. Internal voice mail also provides the auto attendant service for the incoming call from public network(i.e. PSTN or ITSP).

The communication protocol between IVM and MSBG ICM is SIP.

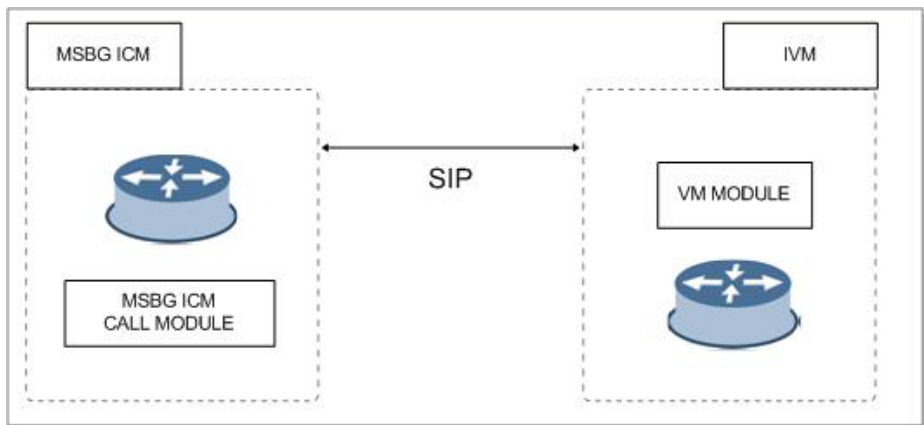


Figure 13.5 General architecture of IVM

How to update IVM packages

First of all, There must be IVM packages in the Compact Flash of MSBG.

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters configuration mode.
2	ivm Example) /configure# ivm	Enters ivm mode
3	update <file name> [reboot] Example) /configure/ivm# update /cf0/ivm_1.0.0.tar	Update IVM packages. [reboot] is optional. After updating, ivm must be rebooted.

How to reset IVM

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters configuration mode.
2	ivm Example) /configure# ivm	Enters ivm mode
3	reset Example) /configure/ivm# reset	Reset the IVM.

How to configure voice-mail entity

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters configuration mode.
2	voice application Example) /configure# voice application	Enters voice application mode.
3	voice-mail <name> Example) /configure/voice application# voice-mail ivm	Creates voice-mail entity.
4	pilot-number <number> Example) /configure/voice application/voice-mail ivm# pilot-number 519	Assigns the pilot-number for voice-mail.

(continued)

Step	Command	Purpose
5	country <country> Example) /configure/voice application/voice-mail ivm# country kr	Configures the country code. If the country code is changed, it need to reset the ivm board
6	no shutdown Example) /configure/voice application/voice-mail ivm# no shutdown	Activates the voice-mail entity

How to configure voice station to use voice-mail

Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters configuration mode.
2	voice station <number> Example) /configure# voice station 1000	Creates the extension.
3	type generic-sip-phone Example) /configure/voice station 1000# type generic-sip-phone	Configures the type of the phone
4	mailbox Example) /configure/voice station 1000# mailbox	Configures the mailbox to use the voice-mail

Verification of configuration

Show voice application voice-mail

```
Ubigate# show voice application voice-mail summary

SERVICE-NAME      PILOT-NUMBER      COUNTRY DP-ID STATE
SESSION-TARGET
-----
vm                  519                kr      10012 up
127.200.1.2:5060

Ubigate# show voice application voice-mail name vm
* VOICE-MAIL INFORMATION
Service Name       : vm
Pilot Number       : 519
Country            : kr
Operation Mode      : day
Session Target     : 127.200.1.2:5060
State              : up
```

Auto Configuration

The Ubigate IVM is designed to simplify the installation procedure and to minimize setup time. The following is configured automatically by exchanging information between Ubigate ICM and IVM.

Extensions are created on IVM by receiving profile information from Ubigate ICM. Any change in the extension information (deletion, or addition, etc.) will be automatically updated onto IVM.

A mail box is also created automatically by receiving mailbox information for each extension from Ubigate ICM. Note that mailboxes may be created for unused extensions. It should delete these if not needed to prevent unauthorized use.

The menu mode for the Day / Night service will change automatically when the mode of the Ubigate ICM changes. There are four menu modes in IVM: Day, Night, Holiday, and Bad weather modes where each mode has its own menus for services.

Quick Setup

Although the set up process has been automated as much as possible, the following functions must be manually configured.

Record a greeting for the Day Mode operation (prompt number 1001). The Night Mode operation (prompt number 1002) and optionally the Holiday and Bad Weather Modes (prompt numbers 1003 and 1004 respectively).

Give everyone the user instructions and have them enter a new personal password [#][7][1], record their name [#][7][2], enter their directory name (Last and First names) [#][7][3], and record both a Primary (No-Answer Greeting) [5][1] and Mailbox Greeting [5][7].

System Administration

There are two levels of administration. There is individual or personal administration that can be performed by the Subscriber, and administration to be performed by a system administrator at a higher level for both subscribers and system.

Subscriber

A subscriber is someone who has an extension and/or a mailbox on IVM. Each subscriber has control over individual options on his/her mailbox and extension settings. Each subscriber (mailbox owner) will have privilege of setting or changing certain mailbox options. The mailbox owner will use DTMF subscriber administration to change and set these options.

System Administrator

The installing Technician or System Administrator has ultimate authority over the operation of the Ubigate IVM system and can set or change all the options that require specialized knowledge.

It is the responsibility of the installing Technician to install and program the Ubigate IVM to suit the customer's requirements. This includes initial set up and creation of the customer database. The Technician will use the management Interface to program and set up the Ubigate IVM.

All System Administration will be performed using a web management. Some limited System Administration can be performed via DTMF.

This is limited to Recording System Prompts, Entering Subscriber Administration, Changing the operating mode (Day, Night, Holiday, and Weather) of the System, Shutting Down the System.

Configuration Tools

Data may be entered and changed in the Ubigate IVM by three methods. These are, the web management Interface, DTMF System Administration, and DTMF Subscriber Administration.

Web Management

Most of the configuration is achieved with the web management interface. This is considered necessary for initial set up.

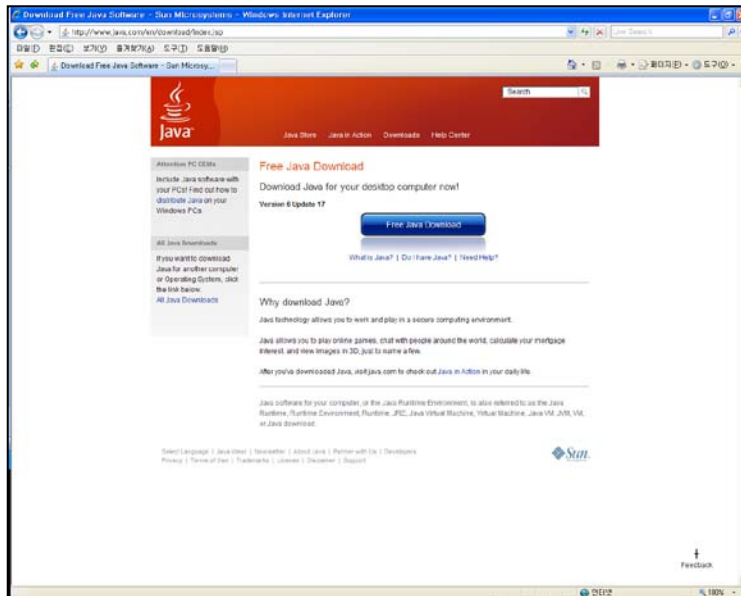
Connecting Web server

A user can connect to the Ubigate IVM GUI with a web browser. Execute a web browser and type “https://Ubigate IP address:60443”.



Java Web Start Plugin Installation

Java Web Start Plugin should be installed to use Ubigate IVM GUI. If it's not, click [\[Java Web Start\] PlugIn](#) , then click the button “Free Java Download” to install.



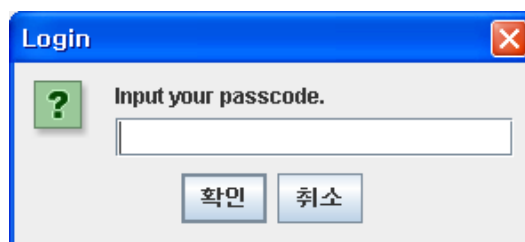
At least JRE 1.6 should be installed to use Ubigate IVM GUI. If an old version of JRE(i.e., lower than the version 1.6) is installed, please remove it and replace with a new one.

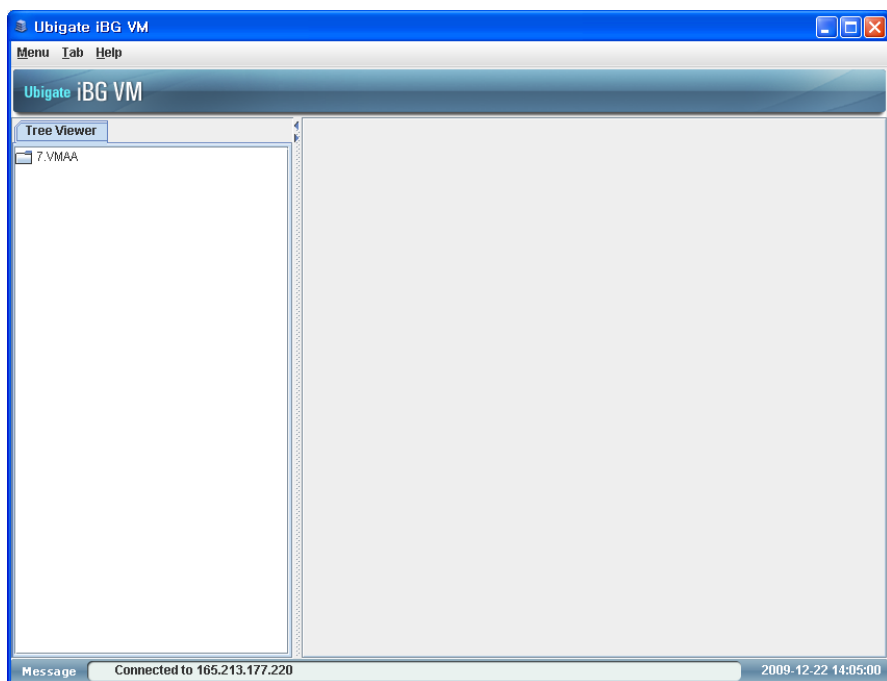
Execution of Ubigate IVM GUI

If Java Web Start Plugin is installed in your browser, Ubigate IVM GUI will be available automatically.

It will ask system admin password to login. The initial password is 0000.

Please change it with your own password in System Parameter page.





DTMF System Administration

Some System Administration functions can be accessed by calling the Ubigate IVM from a touch tone phone. These administrative functions allow the System Administrator to:

- [1] Edit System Prompts
- [2] Edit (create, Delete, and modify) Subscribers
- [3] Change the Operating Mode (Day, Night, etc.)
- [4] Shut the Ubigate IVM down.

Accessing DTMF System Administration

To access the DTMF System Administration mode:

- 1) Call the Ubigate IVM and from the Main Menu press the '#' key followed by 4 zeros. If you are answered by a prompt to enter your password you are in a mailbox and must first press '*' to reach the Main Menu.
- 2) When prompted, enter the administration password specified in the System Wide Parameters. You will be presented with the System Administration Menu.

Edit System Prompts

This allows you to create or edit system prompts.

- Call the Ubigate IVM, and access the System Administration Menu.
- Press 1 to edit system prompts.
- Follow the spoken instructions to edit system prompts.

At the very least you will probably need to create the following:

- Day Greeting = Prompt 1001
- Night Greeting = Prompt 1002
- Holiday Greeting = Prompt 1003
- Emergency (Bad Weather) Greeting = Prompt 1004

Only prompts above prompt # 1000 may be recorded using the DTMF System Administration. To record prompts lower than # 1000 (system prompts) you must use the Voice Studio Administration Tool.

Subscriber Administration

This allows you to add and delete subscribers.

- Call the Ubigate IVM, and access the System Administration Menu.
- Press 2 for subscriber information.
- Follow the spoken instructions to create or delete subscribers.

Manual Mode Selection

This allows you to change the operating mode of the Ubigate IVM. You may select a specific mode (as long as it has been defined as a mode block) or you may select automatic scheduling. The change to a specific mode will remain in effect until you manually change it back to automatic scheduling.

You may select a mode for each port in the system.

- Call the Ubigate IVM, and access the System Administration Menu.
- Press 3 to manually set the mode.
- Follow the spoken instructions to change the port number
- Follow the spoken instructions to change the operating mode. According to the following list of options:

- 1 Day Mode
- 2 Night Mode
- 3 Holiday Mode
- 4 Emergency (Bad Weather) Mode
- 5-99 To select any additional modes that may have been created
- 0 Automatic Scheduling - automatically follow the system Schedule Table

DTMF System Shut Down

This allows you to do a proper shut down of the Ubigate IVM when you do not have access via a PC web management and you need to reboot the switch.

- Call the Ubigate IVM, and access the System Administration Menu.
- Press 4, this will NOT be a spoken option.
- You will then be prompted to again enter the System Administration Password.
- Enter the System Administration Password (default password is: 0000)

Voice Mail CLI

The Voice Mail CLI is an extremely useful tool for diagnosing problems on an installed Ubigate IVM system. This screen will display all activities in real time as it occurs and is also being broken up and written to the Activity, User, and Error Logs simultaneously. This activity contains detailed information for both, Subscriber and Public Caller, call sessions. The viewable Monitors are Monit, CP, and Debug. When a system is restarted only the Monit and CP monitors are on.

This area is a command line driven utility. Type “help” after entering Voice Mail CLI will list all the commands we allow the Dealers and End User Administrators to use.

The following commands can be typed in at the => prompt to determine how much and what type of information is displayed:

To enter Voice Mail CLI, do the followings.

- Open a telnet terminal and enter the IP address of Ubigate. Then assign the port number to 60023.(If you have a serial cable that is suitable with IVM board, you can use it. Baud rate should be 115,200 bps)
- Enter ID and password.
- Select 3.Voice Mail CLI

ACTIVITY: Displays the Activity Log. This is also the same view that can be seen from the Operating Utilities Menu. It is some times more convenient to enter it from Voice Mail CLI.

Syntax: ACTIVITY

CP: Turns the Call Progress monitor on or off for one or all ports. When watching the voice mail CLI screen, the data preceded with a CP represents data reported by the Call Progress monitors. This monitor can be used alone or with either or both the Monit and debug Monitors.

Syntax: CP [port|ALL|OFF]

DEBUG: Turns the Debugging monitor on or off for one or all ports. This is useful when experiencing hard to detect problems.

Often you will need to leave this monitor and the CP monitor on and let the system run for a while. You can then follow the reported information in the Activity, User, and Error Logs for trouble shooting purposes. Leaving all the monitors on all the time will cause the time period stored in the logs to be shorter because there is so much more information being reported.

When watching the port activity screen or looking through the log files, the data preceded by a DB represents the data the DEBUG monitors reported. The information reported by the Debug monitor is often cryptic, but is very useful for the software engineer's when their assistance is required in troubleshooting a problem.

This monitor can be used alone or with either or both the Monit and debug Monitors.

Syntax: DEBUG [port|ALL|OFF]

ERROR: Displays the Error Log.

Syntax: ERROR

IPC: Turns on/off monitoring system communication messages for all or specific ports. Must be turned off with "OFF" command-not done by maintenance. It may be used in combination with any of the other monitors.

Syntax: IPC [port|ALL\Off]

LOCK: Will busy out a port(s), when in goes idle. You can view which ports have been forced into a locked condition

Syntax: LOCK [port|ALL]

MAINTENANCE: Schedules daily system maintenance to begin at the first available opportunity.

Syntax: MAINT

MONITOR: Turns the Activity monitor on or off for one or all ports.

Syntax: MONIT [port|ALL|OFF]

NET: The net command is used in two ways:

1. To show the current status of the IVM network connection at the very moment you typed

NET and hit the [enter] key.

2. Typing 'net ON' or 'net OFF' will toggle the state of network traffic reporting as it pertains to the IVM.

STATUS: Displays port status, available memory and hard drive space.

Syntax: STAT

PORTSTOP: Stops a port and puts it in the idle state.

Syntax: PORTSTOP [port]

UNLOCK: Returns a locked port to the idle state.

Syntax: UNLOCK [port]

USER: Displays the User Activity Log.

Syntax: USER

ENDVMCLI: Exit Voice Mail CLI and return to the Login menu.

Syntax: ENDMCLI

Configuration Categories

When configuring the Ubigate IVM there are three types of data: Subscriber Options, Ubigate IVM Administration Options, and Phone System Options.

Subscriber Options

These are options entered by a subscriber, that control the individual behavior of their mailbox.

Administration Options

These are configuration options that are unique to a particular installation.

Phone System Options

This is a collection of the configuration options to make Ubigate IVM operate correctly. When the Ubigate IVM is initialized, you have to configure it to use. Please refer to the phone system manual for these options.

Ubigate IVM Directory Structure

IVM directory is located in /os7100/vm.

The TABLE Files (*.TBL)

All customer configuration is located in the \dta*.tbl files.

- Block.TBL All block parameter data. Commonly referred to as application data.
- Schedule.TBL The schedule table is not a block, so its data is stored separately in this file.
- SiteInfo.TBL Useful customer data entered in "Site Information" off of the Main Menu.
- Message.TBL Automatically gets updated every time a new message is recorded, saved, forwarded, or deleted. This is sometimes referred to as the Message Index.
- Trunks.TBL When the Ubigate IVM is properly initialized with the switch it is installed in, this file will contain all the Trunk ID numbers of the trucks installed on the switch. This file is required for Ubigate IVM OverHead paging functionality to work.(NOT USED)

PMT Directories (Prompts)

All prompt directories are located in the \PMT directory. There will be a separate prompt directory for each language installed. The different language prompts are stored in a uniquely named language subdirectory located in the PMT directory; \PMT\EN_US for the English(United States) prompt set, \PMT\SP_CA for the Spanish(Castilian) prompt set, and \PMT\FR_CA for the French(Canadian) prompt set. The reference to speak the prompt in a particular block is stored in the "Block.TBL" file, but the recorded prompt itself and its associated text are stored in the PMT \xx_xx directory. The file format is '{4 digits}.726(or 729,711)' and '{4 digits}.TXT'. Prompts below 1000 are system prompts and should only be edited using great care.

MSG Directory (Messages)

All Voice Message data is located in the \Msg\ *.* files.

MBX Directory (Mailboxes)

All Personal Subscriber Extension and Mailbox data is located in the \Mbx\ *.* files.

This includes (but is not limited to) Recorded Names, all 10 personal Greetings (if recorded), personal password, notification, email addresses, and availability information.

TEMP Directory

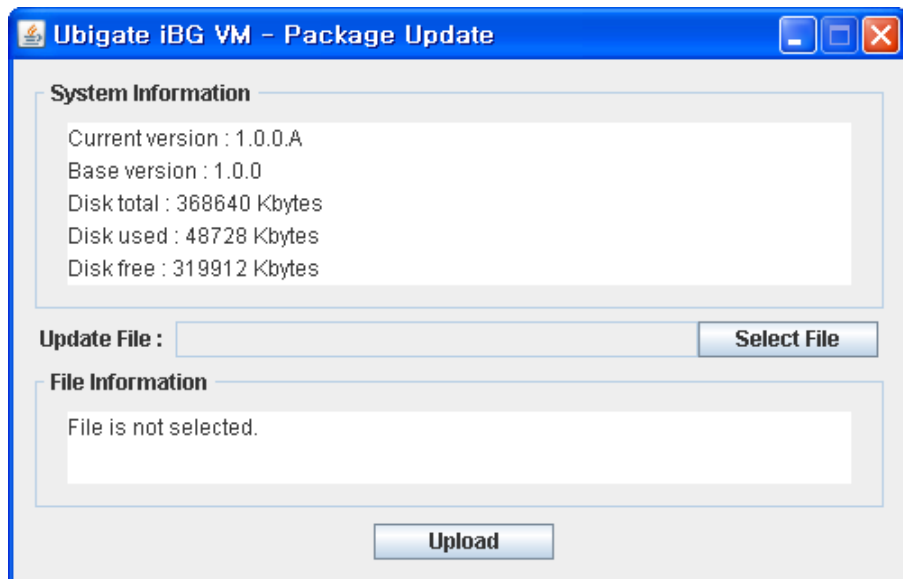
The TEMP directory is used by the application software for storing data during Call Session. An example of this data would be the Caller's spoken name if a subscriber has Call Screening enabled. Another example would be answers to a succession of Query Block questions. These recorded answers would be stored in the TEMP directory until the Last question and then compiled together as one message and sent to the designated recipient.

Defaulting the Configuration

To default the configuration connect web management and select Operating Utilities and select Initialize VM menu. This will restore default block configurations back to the factory preset settings and delete any existing mailboxes, messages and custom prompts or re-recorded prompts.

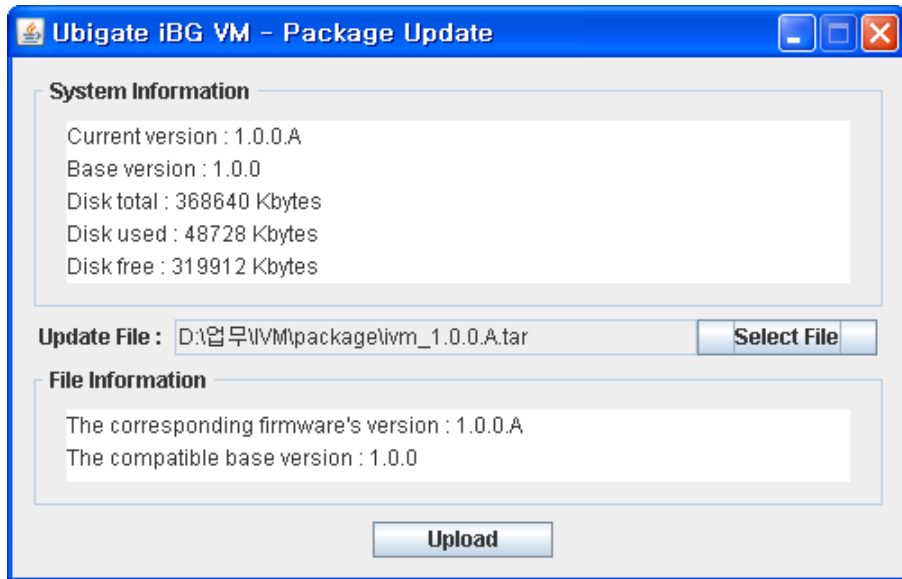
Select Package Update

Select “Package Update” in Menu tab of Ubigate ICM GUI.



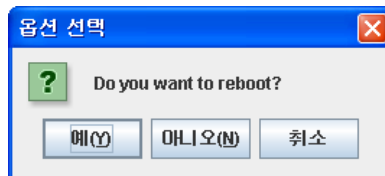
Select the file to update

Click “Select File” and assign the file to update. If the file is selected, “firmware” and “base version” will be displayed in File Information.

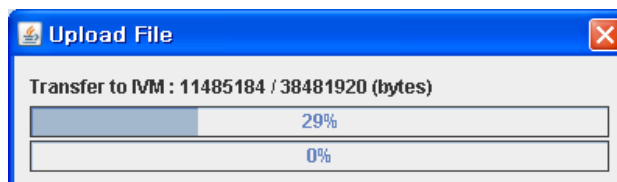


Upload the package

Click “Upload” button to start to upload the file. To apply the uploaded file, Ubigate should be restarted, so you have to select “YES” to use it immediately.



The progress bar displays current state.



Progress bar will be closed if it completes to upload.

Configurable Feature Codes

There are major changes of default values of feature codes from SNOS version 2.10.0.0.



NOTE

The default set of these values are not backward-compatible automatically. You must reconfigure these to fit your operation environments.

Changed default value of Feature codes

features	previous	SNOS 2.10.0.0	toggle
Group Call Pickup	**	**	-
Directed Call Pickup	*24	*24	-
Hold Call pickup	*75	*25	-
Disable Call Waiting for Next Call	*26	*26	-
Disable Call Waiting for Current Call	*29	*29	-
Activate Conference Call (UA)	*30	*30	-
Start N-way Conference (Internal)	*31	*31	-
Drop Last Joined Party	*32	*32	-
Call Forwarding Always Registration	*50	*50	-
Call Forwarding Always Cancel	*51	#50	-
Call Forwarding Always VMS Registration	-	*51	-
Call Forwarding Always VMS Cancel	-	#51	-
Call Forwarding Busy Registration	*52	*52	-
Call Forwarding Busy Cancel	*53	#52	-
Call Forwarding Busy VMS Registration	-	*53	-
Call Forwarding Busy VMS Cancel	-	#53	-
Call Forwarding No Answer Registration	*54	*54	-
Call Forwarding No Answer Cancel	*55	#54	-
Call Forwarding No Answer VMS Registration	-	*55	-
Call Forwarding No Answer VMS Cancel	-	#55	-
Call Forwarding Unreachable Registration	-	*56	-

(continued)

features	previous	SNOS 2.10.0.0	toggle
Call Forwarding Unreachable Cancel	-	#56	-
Call Forwarding DND Registration	-	*57	-
Call Forwarding DND cancel	-	#57	-
Cancel All Call Forwarding Configurations	*56	#59	-
Follow-Me Registration	*60	*60	-
Follow-Me Cancel	*61	#60	-
Do Not Disturb Activation	*62	*61	V
Do Not Disturb Deactivation	*63	#61	-
DND Local Activation	*68	*62	V
DND Local Deactivation	*69	#62	-
Last Number Redial	*64	*64	-
Call Return	*65	*65	-
Call Park	*66	*66	-
Call Park Retrieve	*67	#66	-
Blind Transfer	*20	*20	-
Auto CallBack Activation	*70	*70	-
Auto CallBack Deactivation	*71	#70	-
Auto CallBack Deactivation All	*72	#71	-
Auto CallBack Status	*73	*72	-
Intercom	*74	*74	-
Multi-Ring Activate	*76	*76	-
Multi-Ring Deactivate	*77	#76	-
Call Override	*78	*78	-
Call Barge-In	*79	*79	-
Hunt-group logout activate	-	*80	V
Hunt-group logout deactivate	-	#80	-
Quick Memo Vms	-	*88	-

Toggled feature code Example

Toggle feature code is specially useful when activate and deactivate using only a single button which was pre-configured by speed dial button on SIP phone-profile menu.



This page is intentionally left blank.



CHAPTER 14. Case Study

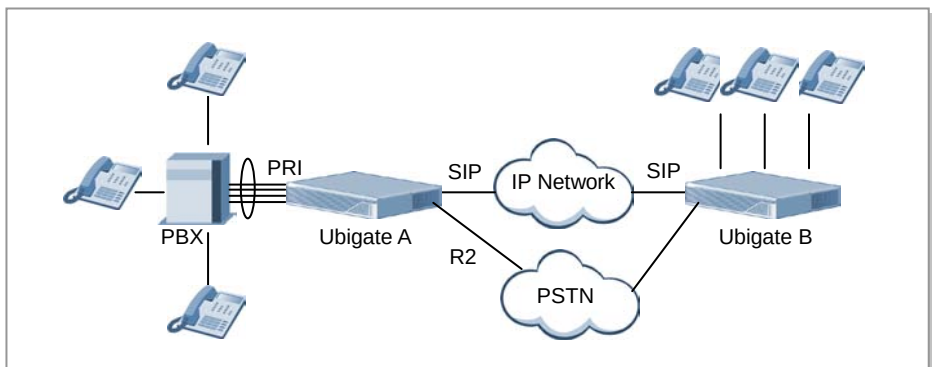
This section describes some examples to help in Ubigate configuration for VoIP service.

Toll-by-pass Configuration Examples

This section includes the following configuration examples:

- ISDN connection to a PBX configuration example
- E1 R2 connection to PSTN configuration example
- SIP trunk connection between Ubigate VoIP gateways configuration example

The configuration examples included in this section correspond to the topology shown below. The routers each include a T1E1-2M along with other interface cards and modules that are included for completeness. Ubigate A is connected to a PBX through ISDN and is connected to Ubigate B by an Ethernet interface. Both Ubigate's are connected to PSTN through E1-R2 for PSTN backup.



Topology Information

The following table shows Ubigate information for the above topology. Examples described below refer to this information.

-	Ubigate A	Ubigate B
IP Address	172.19.30.3	172.19.30.6
Public telephone prefix	031201	02501
Analog extension number	2001, 2002, 2003	3001, 3002, 3003

ISDN connection to a PBX configuration example

```
ntclk-select e1 1/0/2/1
module e1 0/2/1
exit
interface bundle pri021
    link pri_e1 0/2/1
    isdn
        switch-type primary-euro
        incoming-voice
    sending-complete
        activate
    exit
exit
voice-port 0/2/1:D
    no shutdown
    exit
dial-peer voice pots 2
    destination-pattern 2...
    port 0/2/1:D
    exit
```

E1 R2 connection to PSTN configuration example

```
ntclk-select e1 1/0/2/0
module e1 0/2/0
    cas-ds0-group 0
exit e1
voice-port 0/2/0:0
    timeslots 1-15,17-31
    signal cas r2-mfc
no shutdown
exit
dial-peer voice pots 511
    destination-pattern 02501.T
    port 0/2/0:0
    exit pots
```

SIP trunk connection between Ubigate VoIP gateways configuration example

```
voice class codec 1
codec-preference 1 g711alaw 20
codec-preference 2 g711ulaw 20
  codec-preference 3 g729 20
  exit
voice service voip
codec-list 1
  exit
dial-peer voice voip 501
  destination-pattern 02501.T
  session target ip-address ipv4:172.19.30.6
  exit
voip-gateway
  host domain-name company.com
  bind control interface ethernet 0/0
  bind media interface ethernet 0/0
sip-ua
no shutdown
  exit
no shutdown
exit
```

PSTN Fallback configuration example

When a failover event occurs at Ubigate A while monitoring the status of Ubigate B by sending periodic SIP OPTIONS requests, Ubigate A would route all the calls to the backup trunk that is configured as 'dial-peer voice pots 511'.

```
dial-peer voice pots 511
destination-pattern 02501.T
port 0/2/0:0
preference 1    [lower preference as a backup trunk]
  exit pots
dial-peer voice voip 501
  destination-pattern 02501.T
  session target ip-address ipv4:172.19.30.6
  peer-monitor expires 60 retry 60 [enable OPTIONS monitoring]
  exit
```

Ubigate A Configuration Examples

The following configuration example shows how a Ubigate router can be configured for the Toll-by-pass case.

```
module e1 0/2/1
  exit e1
module e1 0/2/0
  cas-ds0-group 0
  exit e1
interface ethernet 0/0
  ip address 172.19.30.3 255.255.255.0
  qos
  exit qos
  exit ethernet
interface bundle pri021
  link pri_e1 0/2/1
  isdn
    switch-type primary-euro
    incoming-voice
  sending-complete
    activate
  exit isdn
  exit bundle
voice class codec 1
  codec-preference 1 g711alaw 20
  codec-preference 2 g711ulaw 20
  codec-preference 3 g729 20
  exit codec
voice service voip
  codec-list 1
  exit voip
voice-port 0/2/0:0
  timeslots 1-15,17-31
  signal cas r2-mfc
  no shutdown
  exit voice-port
voice-port 0/2/1:D
  no shutdown
  exit voice-port
dial-peer voice pots 2
  destination-pattern 2...
  port 0/2/1:D
  exit pots
dial-peer voice pots 511
  destination-pattern 02501.T
```

```

port 0/2/0:0
preference 1
    exit pots
dial-peer voice voip 501
    destination-pattern 02501.T
    session target ip-address ipv4:172.19.30.6
    peer-monitor expires 60 retry 60
    exit voip
voip-gateway
    host domain-name company.com
    bind control interface ethernet 0/0
    bind media interface ethernet 0/0
sip-ua
no shutdown
    exit sip-ua
no shutdown
    exit voip-gateway

```

The following information shows dial-peers of Ubigate A to route the calls.
UbigateA# show dial-peer voice summary

ID	TYPE	PREFIX	DEST-PATTERN	PREF	SESS-TARGET	i	PORT	ADMIN
OPER	OUT-STAT							
2	POTS	2...	0		0/2/1:D	up	up	up
511	POTS	02501.T	1		0/2/0:0	up	up	up
501	VOIP	02501.T	0	ipv4:172.19.30.6		up	up	up

Ubigate B Configuration Examples

The following configuration example shows how a Ubigate router can be configured for the Toll-by-pass case.

```

module e1 0/1/1
    exit e1
module e1 0/1/0
    cas-ds0-group 0
    exit e1
interface ethernet 0/2
    ip address 172.19.30.6 255.255.255.0
    qos

```

```
exit qos
exit ethernet
voice class codec 1
codec-preference 1 g711alaw 20
codec-preference 2 g711ulaw 20
    codec-preference 3 g729 20
exit codec
voice service voip
codec-list 1
    exit voip
voice-port 0/2/0
    signal loop-start
    no shutdown
    exit voice-port
voice-port 0/2/1
    signal loop-start
    no shutdown
    exit voice-port
voice-port 0/2/2
    signal loop-start
    no shutdown
    exit voice-port
voice-port 0/2/3
    signal loop-start
    no shutdown
    exit voice-port
voice-port 0/1/0:0
    timeslots 1-15,17-31
    signal cas r2-mfc
    no shutdown
    exit voice-port
dial-peer voice pots 3001
    destination-pattern 3001
    port 0/2/0
    exit pots
dial-peer voice pots 3002
    destination-pattern 3002
    port 0/2/1
    exit pots
dial-peer voice pots 3003
    destination-pattern 3003
    port 0/2/2
    exit pots
dial-peer voice pots 211
    destination-pattern 031201.T
    port 0/1/0:0
```

```

preference 1
  exit pots
dial-peer voice voip 201
  destination-pattern 031201.T
  session target ip-address ipv4:172.19.30.3
  peer-monitor expires 60 retry 60
  exit voip
voip-gateway
  host domain-name company.com
  bind control interface ethernet 0/2
  bind media interface ethernet 0/2
sip-ua
  no shutdown
  exit sip-ua
  no shutdown
exit voip-gateway

```

The following information shows dial-peers of Ubigate B to route the calls.
 UbigateB# show dial-peer voice summary

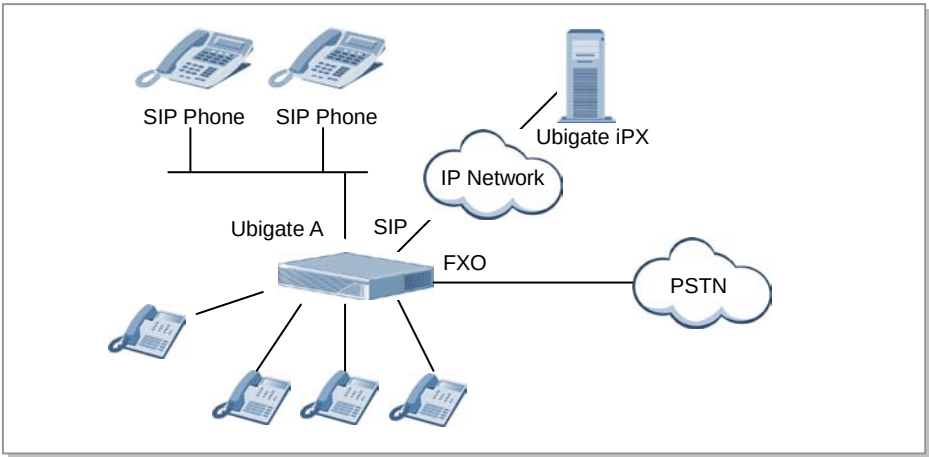
ID	TYPE	PREFIX	DEST-PATTERN	PREF	SESS-TARGET	i	PORT
ADMIN	OPER	OUT-STAT					
---	---	-----	-----	---	-----	---	---
3001	POTS	3001	0		0/2/0	up	up up
3002	POTS	3002	0		0/2/1	up	up up
3003	POTS	3003	0		0/2/2	up	up up
211	POTS	031201.T	1		0/1/0:0	up	up up
201	VOIP	031201.T	0	ipv4:172.19.30.3		up	up up

iPX Interworking Configuration Examples

This section includes the following configuration examples:

- FXS for Analog telephones configuration example
- FXO connection to PSTN configuration example
- Ubigate iPX interworking configuration example

The configuration examples include in this section correspond to the topology shown below. The router includes a FXS-4M and a FXO-4M along with other interface cards and modules that are included for completeness. Ubigate A is connected to PSTN through CO trunk and has a number of analog telephones. The SIP phones and Ubigate A on the network are connected to Ubigate iPX as a IP-PBX.



Topology Information

The following table shows Ubigate information for the above topology. Examples described below refer to this information.

-	Ubigate A	Ubigate iPX
IP Address	172.19.30.3	172.1.1.100
Public telephone prefix	031201	-
Analog extension number	2001, 2002, 2003	-
SIP extension number	4001, 4002, 4003	-
Attendant	2000	-

FXS for Analog telephones configuration example

```
voice-port 0/0/1
  signal loop-start
  no shutdown
  exit
voice-port 0/0/2
  signal loop-start
  no shutdown
  exit
voice-port 0/0/3
  signal loop-start
  no shutdown
  exit
dial-peer voice pots 2001
  authentication username 2001 password 2001
  destination-pattern 2001
  port 0/0/1
  register e164
  exit
dial-peer voice pots 2002
  authentication username 2002 password 2002
  destination-pattern 2002
  port 0/0/2
  register e164
  exit
dial-peer voice pots 2003
  authentication username 2003 password 2003
  destination-pattern 2003
  port 0/0/3
  register e164
  exit
```

FXO connection to PSTN configuration example

```
voice-port 0/1/0
  signal loop-start
  no shutdown
  exit
dial-peer voice pots 9
  destination-pattern 9.T
  port 0/1/0
  exit pots
```

- PLAR connection to the attendant configuration example
All the calls incoming from the port will directly route to the number configured. The number will be the attendant's.

```
voice-port 0/1/0
  signal loop-start
  connection plar 2000
no shutdown
exit voice-port
```

Ubigate iPX interworking configuration example

```
voice class codec 1
codec-preference 1 g711alaw 20
codec-preference 2 g711ulaw 20
  codec-preference 3 g729 20
  exit
voice service voip
codec-list 1
  exit
voip-gateway
  host domain-name company.com
  bind control interface ethernet 0/0
bind media interface ethernet 0/0
call-server
  ip-address ipv4:172.1.1.100
  gw-uri ibg03 expires 60
  exit call-server
sip-ua
no shutdown
  exit
no shutdown
exit
```

Ubigate A Configuration Examples

The following configuration example shows how a Ubigate router can be configured for the iPX interworking case.

```
interface ethernet 0/0
  ip address 172.19.30.3 255.255.0.0
  qos
  exit qos
exit ethernet
voice class codec 1
codec-preference 1 g711alaw 20
codec-preference 2 g711ulaw 20
codec-preference 3 g729 20
exit
voice service voip
  codec-list 1
  exit voip
voice-port 0/0/0
  signal loop-start
  connection plar 2000
no shutdown
exit voice-port
voice-port 0/0/1
  signal loop-start
  no shutdown
  exit voice-port
voice-port 0/0/2
  signal loop-start
  no shutdown
  exit voice-port
voice-port 0/0/3
  signal loop-start
  no shutdown
  exit voice-port
voice-port 0/1/0
  signal loop-start
  no shutdown
  exit voice-port
dial-peer voice pots 2000
authentication username 2000 password 2000
destination-pattern 2000
port 0/0/0
register e164
exit pots
dial-peer voice pots 2001
```

```
authentication username 2001 password 2001
destination-pattern 2001
port 0/0/1
register e164
exit pots
dial-peer voice pots 2002
authentication username 2002 password 2002
destination-pattern 2002
port 0/0/2
register e164
exit pots
dial-peer voice pots 2003
authentication username 2003 password 2003
destination-pattern 2003
port 0/0/3
register e164
exit pots
dial-peer voice pots 9
  destination-pattern 9.T
  port 0/1/0
  exit pots
voip-gateway
  host domain-name company.com
  bind control interface ethernet 0/0
  bind media interface ethernet 0/0
call-server
  ip-address ipv4:172.1.1.100
  gw-uri ibg03 expires 60
  exit call-server
sip-ua
no shutdown
  exit sip-ua
  no shutdown
exit voip-gateway
```

The following information shows the status of registration, service profiles given from iPX for survivability, and dial-peers of Ubigate A to route the calls.

- Registration status

```
UbigateA# show sip-ua registration
Call-Server(GW-URI): Expires=60 Registered
sip:ibg03@company.com
```

ID	USERINFO	EXPIRES	STATUS	PORT	AUTHENTICATION
2000	2000	3600	3600	yes	0/0/0 2000[****]
2001	2001	3600	3600	yes	0/0/1 2001[****]
2002	2002	3600	3600	yes	0/0/2 2002[****]
2003	2003	3600	3600	yes	0/0/3 2003[****]

Number of 4/total(4) is registered

- Service profiles from Ubigate iPX for Survivability

```
UbigateA# show voip profiles
```

Id	Public Number	Extension Contact
SIP 1	0312014001	4001
SIP 2	0312014002	4002
SIP 3	0312014003	4003
FXS 1	0312012000	2000
FXS 2	0312012001	2001
FXS 3	0312012002	2002
FXS 4	0312012003	2003

Total 7, SIP 3, FXS 4

- Dial-peers and routing information

```
UbigateA# show dial-peer voice summary
```

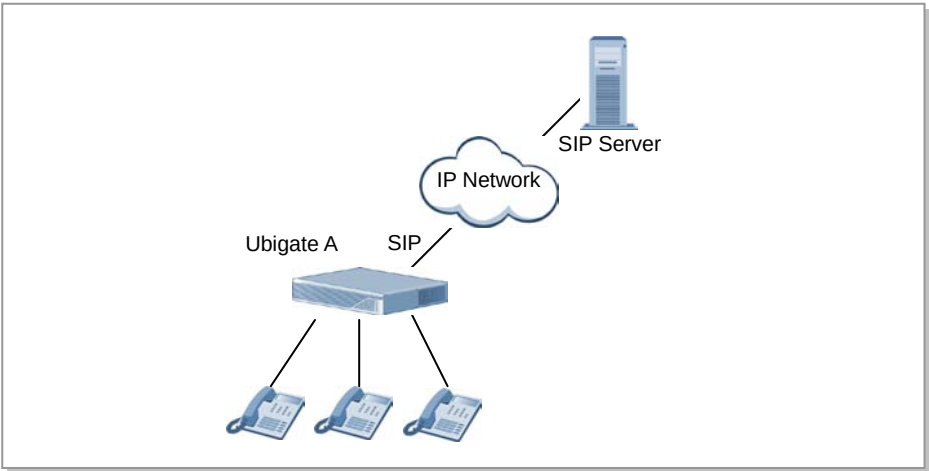
ID	TYPE	PREFIX	DEST-PATTERN	PREF	SESS-TARGET	PORT	ADMIN
OPER	OUT-STAT						
9	POTS		9.T	0	0/1/0	up	up
2000	POTS		2000	0	0/0/0	up	up
2001	POTS		2001	0	0/0/1	up	up
2002	POTS		2002	0	0/0/2	up	up
2003	POTS		2003	0	0/0/3	up	up

SIP Server Interworking Configuration Examples

This section includes the following configuration examples:

- SIP Server interworking configuration example

The configuration examples included in this section correspond to the topology shown below. The router includes a FXS-4M along with other interface cards and modules that are included for completeness. Ubigate A has a number of analog telephones connected to its FXS-4M module. SIP Server in this document means the RFC3261 based SIP Registrar and Proxy. Registrar and Proxy can reside on the same server.



Topology Information

The following table shows Ubigate information for the above topology. Examples described below refer to this information.

-	Ubigate A	SIP Server
IP Address	172.19.30.3	172.1.1.200
Analog telephone	0312012001, 0312012002, 0312012003	-

SIP Server interworking configuration example

```
voice class codec 1
codec-preference 1 g711alaw 20
codec-preference 2 g711ulaw 20
  codec-preference 3 g729 20
  exit
voice service voip
codec-list 1
exit
dial-peer voice voip 8
  destination-pattern 8.T
  session target sip-server
  exit voip
voip-gateway
  host domain-name company.com
  bind control interface ethernet 0/0
bind media interface ethernet 0/0
sip-ua
  registrar ip-address ipv4:172.1.1.200
sip-server ip-address ipv4:172.1.1.200
no shutdown
  exit
no shutdown
exit
```

Ubigate A Configuration Examples

The following configuration example shows how a Ubigate router can be configured for the SIP Server interworking case.

```
interface ethernet 0/0
  ip address 172.19.30.3 255.255.0.0
  qos
  exit qos
exit ethernet
voice class codec 1
codec-preference 1 g711alaw 20
codec-preference 2 g711ulaw 20
codec-preference 3 g729 20
exit
voice service voip
  codec-list 1
  exit voip
voice-port 0/0/0
  signal loop-start
no shutdown
```

```
    exit voice-port
voice-port 0/0/1
    signal loop-start
    no shutdown
    exit voice-port
voice-port 0/0/2
    signal loop-start
    no shutdown
    exit voice-port
voice-port 0/0/3
    signal loop-start
    no shutdown
exit voice-port
dial-peer voice pots 2001
authentication username 0312012001 password 2001
destination-pattern 0312012001
port 0/0/1
register e164
exit pots
dial-peer voice pots 2002
authentication username 0312012002 password 2002
destination-pattern 0312012002
port 0/0/2
register e164
exit pots
dial-peer voice pots 2003
authentication username 0312012003 password 2003
destination-pattern 0312012003
port 0/0/3
register e164
exit pots
dial-peer voice voip 8
    destination-pattern 8.T
    session target sip-server
    exit voip
voip-gateway
    host domain-name company.com
    bind control interface ethernet 0/0
bind media interface ethernet 0/0
sip-ua
    registrar ip-address ipv4:172.1.1.200
sip-server ip-address ipv4:172.1.1.200
no shutdown
    exit
no shutdown
exit
```


The following information shows the status of registration and dial-peers of Ubigate A to route the calls.

- Registration status

```
UbigateA# show sip-ua registration
ID    USERINFO    EXPIRES    STATUS PORT    AUTHENTICATION
-----
2001  0312012001    3600 3600  yes  0/0/1    0312012001[****]
2002  0312012002    3600 3600  yes  0/0/2    0312012002[****]
2003  0312012003    3600 3600  yes  0/0/3    0312012002[****]
-----
Number of 3/total(3) is registered
```

- Dial-peers and routing information

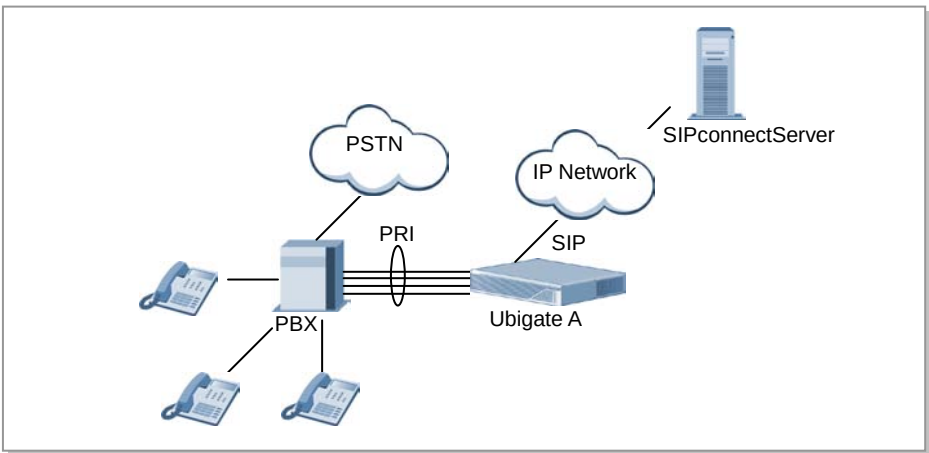
```
UbigateA# show dial-peer voice summary
ID  TYPE PREFIX DEST-PATTERN PREF SESS-TARGET PORT  ADMIN
OPER OUT-STAT
-----
-----
2001 POTS  0312012001    0          0/2/1:D  up   up   up
2002 POTS  0312012001    0          0/2/1:D  up   up   up
2003 POTS  0312012001    0          0/2/1:D  up   up   up
8    VOIP  8.T           0  ip-server    up   up   up
```

SIPconnect Interworking Configuration Examples

This section includes the following configuration examples:

- SIPconnect interworking configuration example
- PSTN Fallback configuration example

The configuration examples included in this section correspond to the topology shown below. The router includes a T1E1-2M along with other interface cards and modules that are included for completeness. Ubigate A is connected to PBX through ISDN. SIPconnect in this document means SIP Server -i.e. Registrar and Proxy - using SIP Forum’s SIPconnect based SIP trunking method. Refer to ‘Configuration SIP Server using SIPconnect’ for details.



Topology Information

The following table shows Ubigate information for the above topology. Examples described below refer to this information.

-	Ubigate A	SIP Server
IP Address	172.19.30.3	172.1.1.200
Public PSTN Identity	07070152000	-
Analog extensions at PBX	2001, 2002, 2003	-

SIPconnect interworking configuration example

```

voice class codec 1
codec-preference 1 g711alaw 20
codec-preference 2 g711ulaw 20
  codec-preference 3 g729 20
  exit
voice service voip
codec-list 1
exit
dial-peer voice voip 9
  destination-pattern .T
  session target sip-server
  exit voip
voip-gateway
  host domain-name company.com
  bind control interface ethernet 0/0
bind media interface ethernet 0/0
sip-ua
authentication username 07070152000 password 2000
sip-connect public-identity 07070152000
registrar ip-address ipv4:172.1.1.200
sip-server ip-address ipv4:172.1.1.200
no shutdown
exit
no shutdown
exit

```

PSTN Fallback configuration example

There are two different methods to support PSTN Fallback. One is PSTN Fallback by busyout monitoring, and the other is by hairpin.

PSTN Fallback by busyout monitoring make a voice-port busyout by shutting down ISDN layer2 when it detects a SIP server outage. When the port is shutdown PBX will not route calls to the connected port - i.e. to Ubigate A - and re-route the calls to PSTN.

PSTN Fallback by hairpin make Ubigate A route the call back to PBX when it detects SIP server outage.

- PSTN Fallback by busyout monitoring

```
interface bundle pri021
  link pri_e1 0/2/1
  isdn
    switch-type primary-euro
    incoming-voice
  sending-complete
    activate
    exit
  exit
voice-port 0/2/1:D
  busyout monitor sip-server
  no shutdown
  exit
voip-gateway
  host domain-name company.com
  bind control interface ethernet 0/0
  bind media interface ethernet 0/0
  sip-ua
  authentication username 07070152000 password 2000
  sip-connect public-identity 07070152000
  registrar ip-address ipv4:172.1.1.200
  sip-server ip-address ipv4:172.1.1.200
  peer-monitor expires 60 retry 60
  no shutdown
  exit
  no shutdown
  exit
```

- PSTN Fallback by hairpin

```
interface bundle pri021
  link pri_e1 0/2/1
  isdn
    switch-type primary-euro
    incoming-voice
  sending-complete
    activate
    exit
  exit
```

```

voice-port 0/2/1:D
no shutdown
exit
dial-peer voice pots 81
destination-pattern 2...
port 0/2/1:D
exit pots
dial-peer voice pots 82
destination-pattern .T
port 0/2/1:D
preference 1
exit pots
dial-peer voice voip 9
destination-pattern .T
session target sip-server
exit voip
voip-gateway
    host domain-name company.com
    bind control interface ethernet 0/0
bind media interface ethernet 0/0
sip-ua
authentication username 07070152000 password 2000
sip-connect public-identity 07070152000
registrar ip-address ipv4:172.1.1.200
sip-server ip-address ipv4:172.1.1.200
peer-monitor expires 60 retry 60
no shutdown
exit
no shutdown
exit

```

Ubigate A Configuration Examples

The following configuration example shows how a Ubigate router can be configured for the SIPconnect interworking case.

```

ntclk-select e1 1/0/2/1
module e1 0/2/1
exit
interface ethernet 0/0
    ip address 172.19.30.3 255.255.0.0
    qos
    exit qos

```

```
exit ethernet
interface bundle pri021
    link pri_e1 0/2/1
    isdn
        switch-type primary-euro
        incoming-voice
    sending-complete
        activate
        exit
    exit
voice class codec 1
codec-preference 1 g711alaw 20
codec-preference 2 g711ulaw 20
codec-preference 3 g729 20
exit
voice service voip
    codec-list 1
exit voip
voice-port 0/2/1:D
no shutdown
    exit
dial-peer voice pots 8
destination-pattern 2...
port 0/2/1:D
exit pots
dial-peer voice voip 9
    destination-pattern .T
    session target sip-server
    exit voip
voip-gateway
    host domain-name company.com
    bind control interface ethernet 0/0
bind media interface ethernet 0/0
sip-ua
    sip-connect public-identity 07070152000
registrar ip-address ipv4:172.1.1.200
sip-server ip-address ipv4:172.1.1.200
no shutdown
    exit
no shutdown
exit
```

The following information shows the status of registration and dial-peers of Ubigate A to route the calls.

- Registration status

```
UbigateA# show sip-ua registration
Registrar: 172.1.1.200
Public ID: sip:07070152000@company.com (Registered)
ID      USERINFO    EXPIRES          STATUS PORT      AUTHENTICATION
-----
Number of 1/total(1) is registered
```

- Dial-peers and routing information

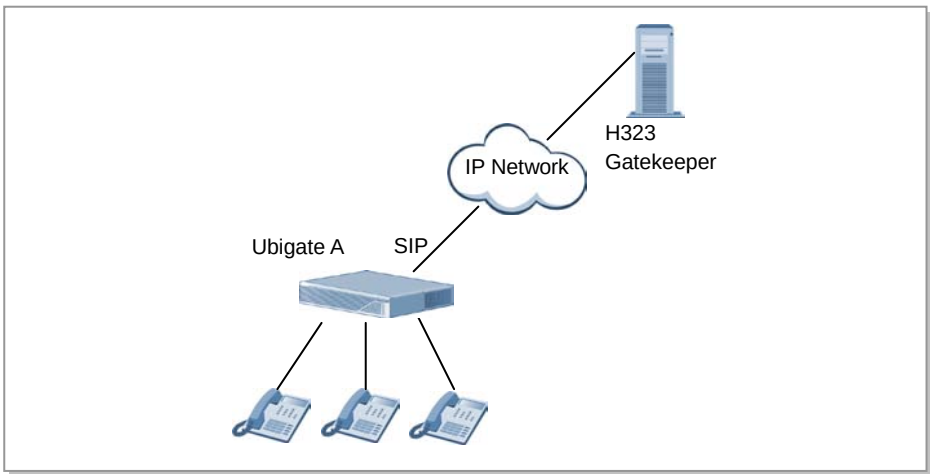
```
UbigateA# show dial-peer voice summary
ID  TYPE PREFIX DEST-PATTERN PREF SESS-TARGET  PORT  ADMIN
OPER OUT-STAT
-----
8   POTS  2...      0    0/2/1:D      up    up    up
9   VOIP  .T        0    sip-server   up    up    up
```

Gatekeeper Interworking Configuration Examples

This section includes the following configuration examples:

- Gatekeeper interworking configuration example

The configuration examples included in this section correspond to the topology shown below. The router includes a FXS-4M along with other interface cards and modules that are included for completeness. Ubigate A has a number of analog telephones connected to its FXS-4M module.



Topology Information

The following table shows Ubigate information for the above topology. Examples described below refer to this information.

-	Ubigate A	H323 Gatekeeper
IP Address	172.19.30.3	172.1.1.210
Analog telephone	0312012001, 0312012002, 0312012003	-

Gatekeeper interworking configuration example

```
voice class codec 1
codec-preference 1 g711alaw 20
codec-preference 2 g711ulaw 20
  codec-preference 3 g729 20
  exit
voice service voip
codec-list 1
exit
dial-peer voice voip 9
destination-pattern .T
session protocol h323
  session target gatekeeper
  exit voip
voip-gateway
  host domain-name company.com
  bind control interface ethernet 0/0
bind media interface ethernet 0/0
h323-gateway
  gatekeeper ip-address ipv4:172.1.1.210 1719 primary
no shutdown
  exit
no shutdown
exit
```

Ubigate A Configuration Examples

The following configuration example shows how a Ubigate router can be configured for the Gatekeeper interworking case.

```
interface ethernet 0/0
  ip address 172.19.30.3 255.255.0.0
  qos
  exit qos
exit ethernet
voice class codec 1
codec-preference 1 g711alaw 20
codec-preference 2 g711ulaw 20
codec-preference 3 g729 20
exit
voice service voip
  codec-list 1
  exit voip
voice-port 0/0/0
```

```
    signal loop-start
no shutdown
    exit voice-port
voice-port 0/0/1
    signal loop-start
    no shutdown
    exit voice-port
voice-port 0/0/2
    signal loop-start
    no shutdown
    exit voice-port
voice-port 0/0/3
    signal loop-start
    no shutdown
exit voice-port
dial-peer voice pots 2001
destination-pattern 0312012001
port 0/0/1
exit pots
dial-peer voice pots 2002
destination-pattern 0312012002
port 0/0/2
exit pots
dial-peer voice pots 2003
destination-pattern 0312012003
port 0/0/3
exit pots
dial-peer voice voip 8
destination-pattern 8.T
session protocol h323
session target gatekeeper
exit voip
voip-gateway
    host domain-name company.com
    bind control interface ethernet 0/0
bind media interface ethernet 0/0
h323-gateway
gatekeeper ip-address ipv4:172.1.1.210 1719 primary
no shutdown
    exit
no shutdown
exit
```

The following information show the status of registration and dial-peers of Ubigate A to route the calls.

- Dial-peers and routing information

```
UbigateA# show dial-peer voice summary
```

ID	TYPE	PREFIX	DEST-PATTERN	PREF	SESS-TARGET	PORT	ADMIN
OPER	OUT-STAT						
2001	POTS	0312012001		0	0/0/1	up	up
2002	POTS	0312012001		0	0/0/2	up	up
2003	POTS	0312012001		0	0/0/3	up	up
9	VOIP	.T		0	gatekeeper	up	up

ICM Configuration Example

This section describes the configuration example for Integrated Communication Manager.

Integrated Communication Manager Example

```
voip-intserver
  call-manager
    exit call-manager
  manage-station
  exit voip-intserver
```

Voice Station Example

```
voice station 1000
  type generic-sip-phone
  routing
    station-cor toll
    huntstop
  exit routing
exit station
voice station 2000
  type generic-fxs-phone
  routing
    station-cor internal
    huntstop
```

```
    exit routing
    port 0/0/0
    exit station
voice station 3000
    type generic-sip-phone
    routing
        station-cor international
        huntstop
        exit routing
    exit station
voice station 2341
    type snom320
    authentication username 2341 password 2341
    phone-profile
        mac-address 112233445566
        blfext 6 3000
        speed 7 2000
        exit phone-profile
    exit station
voice station 5611
    type snom320
    authentication username 5611 password 5611
    phone-profile
        mac-address aabbccddeeff
        blfext 6 2341
        blfext 7 3000
        exit phone-profile
    exit station
```

Dial-Peer Example

```
dial-peer voice pots 1
 destination-pattern 052.+
 port 1/1:D
 exit pots
dial-peer voice pots 2
 destination-pattern 911
 port 1/1:D
 no digit-strip
 exit pots
dial-peer voice pots 4
 destination-pattern 2413333...
 port 1/0:D
 no digit-strip
 exit pots
dial-peer voice voip 3
 destination-pattern 052.+
 session target ip-address ipv4:192.168.1.1
 exit voip
```

Number-Plan Example

```
dial-plan
 number-plan 1
 pattern 911 min 3 max 3
 type emergency
 exit number-plan
 number-plan 2
 pattern 2413333 min 10 max 10
 type internal
 exit number-plan
 number-plan 3
 pattern 052 min 10 max 13
 type toll
 exit number-plan
 exit dial-plan
```

Time-based service Example

```
voice service holiday-schedule hh
  weekend sunday
  schedule 0 start-date 1 1 2009 end-date 1 3 2009
  schedule 1 start-date 12 25 2009
  exit holiday-schedule

voice service time-schedule tt
  schedule 0 monday 8 0 17 0
  schedule 1 tuesday 8 0 17 0
  schedule 2 wednesday 8 0 17 0
  schedule 3 thursday 8 0 17 0
  schedule 4 friday 8 0 17 0
  schedule 5 saturday 8 0 12 0
  schedule 7 monday 18 0 20 0
  exit time-schedule

voice service timebased-service
  holiday-schedule hh
  time-schedule tt
  day-service find-me find-me1
  night-service forwarding 3002
  holiday-service forwarding 3002
  wait-time-before-fwd night 5
  enable
  exit timebased-service

voice station 3000
  timebased-service
  exit station
voice station 3001
  timebased-service
  exit station
```

Hunt Parallel Example

```
hunt-group 7777
  member-number 0 4000
  member-number 1 4001
  member-number 2 4002
  hunt-scheme parallel
  call-forwarding busy 3003
  exit hunt-group
```

Automatic Callback Example

- Configure DTMF Relay Option

The RFC 2833 DTMF relay option should be enabled to use automatic callback functions.

```
Ubigate/configure# voice service sip
Ubigate/configure/voice/service/sip# dtmf-relay ?
sip-notify                SIP NOTIFY method
sip-info                  SIP INFO method using named
events
sip-info-digits           SIP INFO method using decimal
numbers. Signal= 10 for *
inband                    Inband
rtp-nte                   Out-of-band 2833 (RTP-NTE)
queued-digits             Out-of-band 2833 (Queued-Digits)
Ubigate/configure/voice/service/sip# dtmf-relay rtp-nte
Ubigate/configure/voice/service/sip#
```

- Configure station

The automatic callback service should be enabled in originator station.

```
Ubigate/configure/voice/station 1000# ?
Ubigate/configure/voice/station 1000# automatic-callback
Ubigate/configure/voice/station 1000#
Ubigate/configure/voice/station 1000# show voice station
number 1000
* General Station Information
  Station type           = Generic_FXS_Phone
  Port                   = 0/3/0
  Station number         = 1000
    - Secondary number 1 =
    - Secondary number 2 =
    - Secondary number 3 =
  Find me numbers
    - Find-me-number 1   =
    - Find-me-number 2   =
    - Find-me-number 3   =
  Service Information
    - Call Forward All    = off [fwd-number: ]
    - Call Forward Busy   = off [fwd-number: ]
    - Call Forward No Answer = off [fwd-number: ]
    - Group Pickup        = off [group-number: ]
```

```

- Music On Hold           = off [music-id: 0]
- Follow Me               = off [follow-number: ]
- Last Number Redial      = off [last-number: ]
- Call Return             = off [return-number: ]
- Do Not Disturb          = off
- Clid Override           = off
- Clid Restrict           = off
- Clid Remove Name        = off
- Clid Network Number     =
Time-based service
- Service assignment      = off
- Night Service           = Follow global setting
- Holiday Service         = Follow global setting
Automatic-callback Information
- Service assignment      = on
- Originator session count = 0
- Terminator session count = 0
Authentication Information
- Authentication Userid    =
- Authentication Passwd    =
Routing Information
- Digit Strip             = on
- Hunt Stop               = off
Ubigate/configure/voice/station 1000#

```

Shared-Group & Service Example

```

# Make a shared-group with representative number which is
used as caller-id when a member originate a call
UbigateC/configure# voice shared-group 3333
# Assign members in shared-group
UbigateC/configure/voice/shared-group 3333# member 0 1000
UbigateC/configure/voice/shared-group 3333# member 1 2000
# set up to three secondary-number which is used as
destination number and/or caller-id when a member originate
a call to trunk.
UbigateC/configure/voice/shared-group 3333# secondary-number
1 006011113333
UbigateC/configure/voice/shared-group 3333# secondary-number
2 090022223333
UbigateC/configure/voice/shared-group 3333# secondary-number
3 090022223333
UbigateC/configure/voice/shared-group 3333# exit

```



```

UbigateC/configure# voice station 1000
# specifies phone type as snomxxx only snom can support
shared-group service now.
UbigateC/configure/voice/station 1000# type snom360
# Use shared-group number 3333 as caller-id not station
number 1000. It's useful to hide originator's number
UbigateC/configure/voice/station 1000# clid shared-group
UbigateC/configure/voice/station 1000# intercom
UbigateC/configure/voice/station 1000# hold-call-pickup
UbigateC/configure/voice/station 1000# shared-service
# set mode and ring type
UbigateC/configure/voice/station 1000/shared-service# mode
executive
UbigateC/configure/voice/station 1000/shared-service# ring-
type silent
UbigateC/configure/voice/station 1000/shared-service# exit
shared-service
UbigateC/configure/voice/station 1000# phone-profile
UbigateC/configure/voice/station 1000/phone-profile# max-
address 00011122AA33
# set blf button to monitor line 2000
UbigateC/configure/voice/station 1000/phone-profile# blfext
0 2000
# set blf button to intercom line 2000 ( *74 is intercom
feature code)
UbigateC/configure/voice/station 1000/phone-profile# blfext
1 *742000
UbigateC/configure/voice/station 1000# exit station

UbigateC/configure# voice station 2000
# specifies phone type as snomxxx only snom can support
shared-group service now.
UbigateC/configure/voice/station 2000# type snom360
# Use shared-group number 3333 as caller-id not station
number 1000. It's useful to hide originator's number
UbigateC/configure/voice/station 2000# clid shared-group
UbigateC/configure/voice/station 2000# intercom
UbigateC/configure/voice/station 2000# hold-call-pickup
UbigateC/configure/voice/station 2000# shared-service
# set mode and ring type
UbigateC/configure/voice/station 2000/shared-service# mode
secretary
UbigateC/configure/voice/station 2000/shared-service# ring-
type bellCore3
UbigateC/configure/voice/station 2000/shared-service# exit
shared-service

```

```
UbigateC/configure/voice/station 2000# phone-profile
UbigateC/configure/voice/station 2000/phone-profile# max-
address 00011122BB44
# set blf button to monitor line 1000
UbigateC/configure/voice/station 2000/phone-profile# blfext
0 1000
# set blf button to intercom line 1000 ( *74 is intercom
feature code)
UbigateC/configure/voice/station 2000/phone-profile# blfext
1 *741000
UbigateC/configure/voice/station 2000# exit station

# Make a shared-group with representative number which is
used as caller-id when a member originate a call
UbigateC/configure# voice shared-group 3333
# Assign members in shared-group
UbigateC/configure/voice/shared-group 3333# member 0 1000
UbigateC/configure/voice/shared-group 3333# member 1 2000
# set up to three secondary-number which is used as
destination number and/or caller-id when a member originate
a call to trunk.
UbigateC/configure/voice/shared-group 3333# secondary-number
1 006011113333
UbigateC/configure/voice/shared-group 3333# secondary-number
2 090022223333
UbigateC/configure/voice/shared-group 3333# secondary-number
3 090022223333
UbigateC/configure/voice/shared-group 3333# exit

UbigateC/configure# voice station 1000
# specifies phone type as snomxxx only snom can support
shared-group service now.
UbigateC/configure/voice/station 1000# type snom360
# Use shared-group number 3333 as caller-id not station
number 1000. It's useful to hide originator's number
UbigateC/configure/voice/station 1000# clid shared-group
UbigateC/configure/voice/station 1000# intercom
UbigateC/configure/voice/station 1000# hold-call-pickup
UbigateC/configure/voice/station 1000# shared-service
# set mode and ring type
UbigateC/configure/voice/station 1000/shared-service# mode
executive
UbigateC/configure/voice/station 1000/shared-service# ring-
type silent
UbigateC/configure/voice/station 1000/shared-service# exit
shared-service
```

```
UbigateC/configure/voice/station 1000# phone-profile
UbigateC/configure/voice/station 1000/phone-profile# max-
address 00011122AA33
# set blf button to monitor line 2000
UbigateC/configure/voice/station 1000/phone-profile# blfext
0 2000
# set blf button to intercom line 2000 ( *74 is intercom
feature code)
UbigateC/configure/voice/station 1000/phone-profile# blfext
1 *742000
UbigateC/configure/voice/station 1000# exit station

UbigateC/configure# voice station 2000
# specifies phone type as snomxxx only snom can support
shared-group service now.
UbigateC/configure/voice/station 2000# type snom360
# Use shared-group number 3333 as caller-id not station
number 1000. It's useful to hide originator's number
UbigateC/configure/voice/station 2000# clid shared-group
UbigateC/configure/voice/station 2000# intercom
UbigateC/configure/voice/station 2000# hold-call-pickup
UbigateC/configure/voice/station 2000# shared-service
# set mode and ring type
UbigateC/configure/voice/station 2000/shared-service# mode
secretary
UbigateC/configure/voice/station 2000/shared-service# ring-
type bellCore3
UbigateC/configure/voice/station 2000/shared-service# exit
shared-service
UbigateC/configure/voice/station 2000# phone-profile
UbigateC/configure/voice/station 2000/phone-profile# max-
address 00011122BB44
# set blf button to monitor line 1000
UbigateC/configure/voice/station 2000/phone-profile# blfext
0 1000
# set blf button to intercom line 1000 ( *74 is intercom
feature code)
UbigateC/configure/voice/station 2000/phone-profile# blfext
1 *741000
UbigateC/configure/voice/station 2000# exit station
```

MCP example

```
voip-intserver

media-proxy
  media-pool system
    ip-address 90.90.13.7
    media-port 40000 1000
  exit media-pool
  media-pool public
    ip-address 172.1.1.7
    media-port 42000 1000
  exit media-pool
  region public interface ethernet 0/2
  no shutdown

voip-gateway
  host domain-name samsung.com
  bind control interface ethernet 0/1
  bind control any-interface
  bind media interface ethernet 0/1
  rtp payload-type nte 101
  sip-ua
    authentication username 0312121000 password 123456
    sip-connect public-identity 0312121000 type option2
    sip-server ip-address ipv4:192.168.1.231
    registrar sip-server expires 3600 retry 60
  no shutdown
  exit sip-ua
no shutdown
exit voip-gateway
```

Ring-group example

```
voice ring-group test
  pattern 0 0...
  pattern 2 [2-5]...
  ring-id 1
  description "ring group for stations"
  exit ring-group
voice ring-group 3
  pattern 0 5....
  pattern 1 ##....T
  pattern 2 2000
  pattern 3 0303
```

```
ring-id 1
exit ring-group
voice ring-group 21
pattern 0 99....
pattern 1 9.....+
pattern 2 990....
pattern 3 2..+
ring-id 1
exit ring-group
voice ring-group 1
ring-id tone
description "ring group for stations"
exit ring-group
voice ring-group 22
pattern 0 5611
pattern 1 990....
ring-id 1
exit ring-group
```

Group-call example

```
voice group-call 2222
call-type dispatch
member 0 5611
member 1 0002
description "test group call "
exit group-call
voice group-call 2223
call-type paging
member 0 5611
member 1 0002
member 2 5700
exit group-call
```

voice-mail example

```
voice application
  voice-mail vm_test
    country it
    pilot-number 519
    no shutdown
    exit voice-mail
  exit application
voice station 2002
  type generic-sip-phone
  mailbox
  exit station
voice station 3000
  type generic-fxs-phone
  port 0/0/1
  mailbox
  exit station
```

Ubigate iBG series Configuration Guide

©2007~2010 Samsung Electronics Co., Ltd.
All rights reserved.

Information in this manual is proprietary to SAMSUNG
Electronics Co., Ltd.

No information contained here may be copied, translated,
transcribed or duplicated by any form without the prior written
consent of SAMSUNG.

Information in this manual is subject to change without notice.



