SCM

Installation Manual

Every effort has been made to eliminate errors and ambiguities in the information contained in this document. Any questions concerning information presented here should be directed to SAMSUNG TELECOMMUNICATIONS AMERICA, 1301 E. Lookout Dr., Richardson, TX. 75082 telephone (972) 889-6700. SAMSUNG TELECOMMUNICATIONS AMERICA disclaims all liabilities for damages arising from the erroneous interpretation or use of information presented in this manual

Publication Information

SAMSUNG TELECOMMUNICATIONS AMERICA reserves the right without prior notice to revise information in this publication for any reason. SAMSUNG TELECOMMUNICATIONS AMERICA also reserves the right without prior notice to make changes in design or components of equipment as engineering and manufacturing may warrant.

Copyright 2013

Samsung Telecommunications America

All rights reserved. No part of this manual may be reproduced in any form or by any means-graphic, electronic or mechanical, including recording, taping, photocopying or information retrieval systems – without express written permission of the publisher of this material.

TRADEMARKS

Product names mentioned in this manual may be trademarks and/or registered trademarks of their respective companies.

INTRODUCTION

Purpose

This manual describes how to install and configure the Samsung Communication Manager (SCM).

Document Content and Organization

This document consists of 6 Chapters and an Abbreviation as follows.

CHAPTER 1. Pre-Installation

Describes how to prepare the environment.

CHAPTER 2. Network Design Guide

Describes how to design the IP network.

CHAPTER 3. License Guide

Describes how to configure license.

CHAPTER 4. Installing SCM Server

Describes how to install the SCM server.

CHAPTER 5. Installing Ubigate iBG Series Gateway

Describes how to install Ubigate iBG Series gateways.

CHAPTER 6. Installing SIP Phones

Describes how to install the SIP telephones.

ABBREVIATION

Provides the definitions of the abbreviations used in this manual.

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.

> ⚠ WARNING
>
> **WARNING**
>
> Provides information or instructions that the reader should follow in order to avoid personal injury or fatality.

> ⚠ CAUTION
>
> **CAUTION**
>
> Provides information or instructions that the reader should follow in order to avoid a service failure or damage to the system.

> ✎ NOTE
>
> **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.

Revision History

VERSION	DATE OF ISSUE	REMARKS
4.0	01. 2013.	Updated for modification of the SCM version 3.3.
3.0	11. 2011.	Updated for modification of the SCM version 3.2.2.x. * Manual Edition allocation method is changed. (Ed.02 → Ver.3.0)
01	07. 2010.	- Add installing Server hardware, Gateway and Phones. - Modified hardware requirements, basic accounts information, database setting subjects.
00	04. 2010.	First Draft

SAFETY CONCERNS

The purpose of the Safety Concerns section is to ensure the safety of users and prevent property damage. Please read this document carefully for proper use.

Symbols

⚠ **Caution**

Indication of a general caution

🛇 **Restriction**

Indication for prohibiting an action for a product

❗ **Instruction**

Indication for commanding a specifically required action

⚠ WARNING

⚠ **HIGH LEAKAGE CURRENT!**

Earth connection is essential before connecting supply.

❗ Unplug the power cord from the AC outlet before attempting to connect the ground. Hazardous voltage may cause death or injury. Observe extreme caution when working with AC power. Remove lines from trunk cards.

⚠ CAUTION

⚠ All the data stored in the HDD will be deleted when installing the SCM software.

⚠ All the existing data will be deleted when initializing the database.

⚠ When assigning IP addresses to configure the system, their subnet addresses should be set carefully..

- For the data link IP addresses (eth0, eth1), their subnet addresses must be identical.
- For the data link IP addresses of the active and standby systems, their subnet addresses must be also identical.
- For the system IP addresses of the active and standby systems, their subnet addresses must be identical.
- For the heartbeat IP addresses of the active and standby systems, their subnet addresses must be identical.
- For the data link IP address, system IP address, and heartbeat IP address, their subnet addresses must be different from each other.

⚠ When updating the SCM software, all the services of the SCM stop. When the upgrade is complete, the SCM restarts automatically.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1. Pre-Installation

1.1 Site Requirements

Select a location that satisfies the following conditions for safety, temperature, humidity, power and grounding.

1.1.1 Safety Conditions

- The SCM Servers and Gateways should not be installed near materials that can cause a fire, such as explosive gas and inflammables. The SCM Servers and Gateways should not be near equipment that generates electromagnetic waves, such as monitors or copying machines.
- The installation location should be convenient for distributing trunk lines and extension lines, for connecting power and grounding wires, and for maintenance and repair.
- The SCM Servers and Gateways should not be installed in aisles or passageways that are populated or used for moving equipment.
- Always maintain cleanliness to prevent dust from damaging the board connectors of the cabinet.
- Before installing the SCM Servers and Gateways, check items such as the electrical wiring status, grounding status, voltage and frequency.
- Do not expose equipment to direct sunlight, corrosive fumes, and constant vibrations.
- Do not install in close proximity to a fire sprinkler or other sources of water.
- A dedicated commercial AC power outlet is required. Do not use extension cords.
- Ensure that all wires and cables to and from the SCM Servers and Gateways do not cross fluorescent lights or run in parallel with AC wires.
- This equipment is to be installed only in restricted access areas (dedicated, equipment closets, etc.) in accordance with articles 110-16, 110-17, 110-18 of the National Electric Code, ANSI/NFPA 70.

1.1.2 Environmental Conditions

The section describes conditions for temperature, humidity and others environmental conditions as follows:

1.1.2.1 SCM Server

NOTE

This section referenced on the Dell's R210 environmental datasheets by Dell.

For additional information about environmental measurements for specific system configurations, see www.dell.com.

Table 1.1 Environmental conditions for SCM server (Dell R210)

Environment	Condition
Temperature	Operating: 10 to 35°C (50 to 95°F) with a maximum temperature graduation of 10°C per hour Storage: -40 to 65°C (-40 to 149°F) with a maximum temperature gradation of 20°C per hour
Humidity	Operating: 20 to 80 % (non condensing) with a maximum humidity gradation of 10 % per hour Storage: 5 to 95 % (non condensing)
Maximum vibration	Operating: 0.26 Grms at 5-350 Hz for 15 min Storage: 1.54 Grms at 10-250 Hz for 15 min
Maximum shock	Operating: One shok pulse in the positive z axis (one pulse on each side of the system) of 31 G for 2.6ms in the operational orientation. Storage: Six consecutively executed shock pulse in the positive and negative x, y, and z axes (one pulse on each side of the system) of 71 G for up to 2 ms. Six consecutively executed shock pulses in the positive and negative x, y, and z axes (one pulse on each side of the system) of 32 G faired square wave pulse with velocity change at 270 inches/second (686 centimeters/second)
Altitude	Operating: -16 to 3,048 m (-50 to 10,000 ft) Storage: -16 to 10,600 m (-50 to 35,000 ft)
Airborne Contaminant Level	Class: G2 or lower as defined by ISA-S71.04-1985

Table 1.2 Environmental conditions for SCM server (Dell R210-II)

Environment	Condition
Temperature	Operating: 10 to 35°C (50 to 95°F) with a maximum temperature graduation of 10°C per hour Storage: -40 to 65°C (-40 to 149°F) with a maximum temperature gradation of 20°C per hour
Humidity	Operating: 20 to 80 % (non condensing) with a maximum humidity gradation of 10 % per hour Storage: 5 to 95 % (non condensing)
Maximum vibration	Operating: 0.26 Grms at 5-350 Hz for 15min Storage: 1.87 Grms at 10-250 Hz for 15min
Maximum shock	Operating: One shock pulse in the positive z axis (one pulse on each side of the system) of 31 G for 2.6 ms in the operational orientation. Storage: Six consecutively executed shock pulses in the positive and negative x, y, and z axes (one pulse on each side of the system) of 71 G for up to 2 ms. Six consecutively executed shock pulses in the positive and negative x, y, and z axes (one pulse on each side of the system) of 32
Altitude	Operating: -16 to 3,048 m (-50 to 10,000 ft) Storage: -16 to 10,600 m (-50 to 35,000 ft)

Table 1.3 Environmental conditions for SCM server (Dell R410I)

Environment	Condition
Temperature	Operating: 10 to 35°C (50 to 95°F) with a maximum temperature gradation of 10°C per hour Note: For altitudes above 2950 feet, the maximum operating temperature is debated 1°F/550 ft. Storage: -40 to 65°C (-40 to 149°F) with a maximum temperature gradation of 20°C per hour
Humidity	Operating: 20 to 80 % (noncondensing) with a maximum humidity gradation of 10 % per hour Storage: 5 to 95 % (noncondensing) with a maximum humidity gradation of 10 % per hour
Maximum vibration	Operating: 0.26 Grms at 5-350 Hz in operational orientations Storage: 1.54 Grms at 10-250 Hz in all orientations
Maximum shock	Operating: Half sine shock in all operational orientations of 31 G +/- 5 % with a pulse duration of 2.6 ms +/-10 %. Storage: Half sine shock on all six sides of 71 G +/- 5 % with a pulse duration of 2 ms +/-10 % Square wave shock on all six sides of 27 G with velocity change @ 235 in/sec or greater
Altitude	Operating: -16 to 3,048 m (-50 to 10,000 ft) Storage: -16 to 10,600 m (-50 to 35,000 ft)

1.1.2.2 Gateways

Table 1.4 Environmental conditions for Gateways

Environment	OfficeServ 7400/7200/7100/7070	Ubigate iBG 3026/2016/2006/1003/1004
Operating temperature	32 to 113°F (0 to 45°C)	32 to 104°F (0 to 40°C)
Storage temperature	14 to 122°F (-10 to 50°C)	-13 to 158°F (-25 to 70°C)
Humidity	10 to 90 %	5 to 95 %, non-condensing

1.2 Grounding Conditions

An equipment grounding conductor that is not smaller in size than the ungrounded branch-circuit supply conductors is to be installed as part of the circuit that supplies the product or system. Bare, covered, or insulated grounding conductors are acceptable. Individually covered or insulated equipment grounding conductors shall have a continuous outer finish that is either green or green with one or more yellow stripes. The equipment grounding conductor is to be connected to ground at the service equipment.

The attachment-plug receptacles in the vicinity of the product or system are all to be of a grounding type, and the equipment grounding conductors serving these receptacles are to be connected to earth ground at the service equipment.

> ⚠ WARNING
>
> **HIGH LEAKAGE CURRENT!**
>
> Earth connection is essential before connecting supply.

The SCM Servers and Gateways require that a supplementary earth ground be connected to the system. This is the preferred method of grounding the SCM Servers and Gateways. It should be noted that when the third wire ground becomes inferior, it many prevent the digital data bus from canceling out noise. This may result in erratic operation of the SCM Servers and Gateways. Another problem that has occurred is that some UPS battery systems do not pass the ground through to the power cord resulting in no ground to the system. The ground lug in the back of the cabinet must be connected to one of the following: bonded building steel, cold water pipe, or a ground rod using at least #16 AWG copper wire. Additionally, the ground between cabinets in a multiple cabinet system must also be at least #16 AWG copper wire. The third wire AC ground or field ground is connected to the system frame via the ground strap from the ground connector on the AC socket.

A supplementary equipment grounding conductor shall be installed between the system and ground that is in addition to the equipment grounding conductor in the power supply cord. The supplementary equipment grounding conductor shall not be smaller in size than the ungrounded branch-circuit supply conductors. The supplementary equipment grounding conductor shall be connected to the product at the terminal provided, and shall be connected to ground in a manner that will retain the ground connection when the product is unplugged from the receptacle. The connection to ground of the supplementary equipment grounding conductor shall be in compliance with the rules for terminating bonding jumpers in Part K of Article 250 of the National Electrical Code ANSI/NFPA 70. Termination of the supplementary equipment grounding conductor is permitted to be made to building steel, to a metal electrical raceway system, or to any grounded item that is permanently and reliably connected to the electrical service equipment ground.

Bare, covered, or insulated grounding conductors are acceptable. A covered or insulated grounding conductor shall have a continuous outer finish that is either green or green with one or more yellow stripes.

Failure to provide an adequate ground may cause a safety hazard, confusing trouble symptoms, or even circuit card failure.

> **WARNING**
>
> Unplug the power cord from the AC outlet before attempting to connect the ground. Hazardous voltage may cause death or injury. Observe extreme caution when working with AC power. Remove lines from trunk cards.

What the above paragraphs mean is that when conventional analog telephone circuits are connected to the SCM Servers and Gateways, under fault conditions (i.e. the tip and/or ring conductor is crossed with a power line, or the circuit is affected by lightning during a storm), it is possible for hazardous potentials to appear across the tip and ring wiring coming into the SCM Servers and Gateways from the outside plant (i.e. overhead cables, buried cables, cable head pedestal). These circuits are provided with both primary and secondary protection circuitry which will attempt to drain off these high voltages and currents to earth ground. Obviously, it is important to have a good source of ground connected to the SCM Servers and Gateways to drain this energy off. Again, a good earth ground source is required by the SCM Servers and Gateways.

The SCM Servers and Gateways have two ground reference points. One point is via the green wire in the power cord connected to the AC power outlet. This ground connection is provided to meet local electrical codes when the AC ground is required to be common with the earth ground. However, this can be disconnected either intentionally or unintentionally. Consequently, a more permanent ground connection is required by connecting a high current/voltage capacity ground wire which is bonded to ground at the electric service power entrance or via some other method approved by the National Electrical Code to the SCM Servers and Gateways ground lug. This is a more secure ground connection, which can only be disconnected intentionally. These precautions are taken for safety reasons to protect personnel working on the SCM Servers and Gateways and also for operational reasons to accommodate ground return and/or ground-referenced analog telephone circuits, which require this solid earth ground connection for normal functioning.

1.3 Power Conditions

1.3.1 SCM Server

The rating is as follows:

Dell R210 model

- AC Cord Rating: 15A @ 120 V, 10 A @ 240 V
- Input Voltage: AC 90-26 4V
- Line Frequency: 40-63H z
- Output Power: 250 W
- BTU: 1039 Btu/hr maximum

Dell R210-II model

- AC Cord Rating: 15 Amps @ 120 VAC, 10 Amps @ 240 VAC
- Input Voltage: 90-264 VAC
- Line Frequency: 47-63 Hertz
- Output Power: 250 W
- BTU: 1039 Btu/hr maximum

Dell R410 model

- Maximum Input Amps
  - Non-Redundant power supply: 7.5-3.8 A at 100-240 VAC, 50/60 Hz
  - Redundant power supply: 7-3.5 A at 100-240 VAC, 50/60 Hz
- Output Power
  - Non-Redundant power supply: 480 W
  - Redundant power supply: 500 W
- BTU: 1039 Btu/hr maximum
  - 1706 BTU/hr maximum (redundant power supply)
  - 1637 BTU/hr maximum (non-redundant power supply)

1.3.2 Gateway

Table 1.5 Power conditions for Gateways

Gateway	Rating	Power Consumption (each PSU)
OfficeServ 7400	AC 100-240 V, 50/60 Hz or DC 48 V	580 W
OfficeServ 7200	AC 100~120 V, 50/60 Hz or DC 48 V (USA) AC 220~240 V, 50/60 Hz or DC 48 V (non USA)	210 W
OfficeServ 7100	AC 100-240 V, 50/60 Hz or DC 48 V	120 W
OfficeServ 7070	AC 220~240 V, 50/60 Hz or DC 48 V (non USA)	135 W
iBG3026	AC 100-240 V, 50/60 Hz or DC 48 V	275 W (w/o POE)
iBG2016	AC 100-240 V, 50/60 Hz or DC 48 V	180 W
iBG2006	AC 100-240 V, 50/60 Hz or DC 48 V	100 W
iBG1003/1004	AC 100-240 V, 50/60 Hz or DC 48 V	72 W

1.4 UPS Considerations

We strictly recommend using uninterruptible power supply (UPS) to help protect your SCM Server (and Gateways) from sudden (transient) increases and decreases in electrical power.

Even a brief power outage could result in loss of unsaved data on a server/servers that was/were running. A UPS is an electronic device that continues to supply electricity for a certain period of time during a utility failure or when the line voltage varies outside the normal limits. UPS can be used for a server backup power and, large models can be used to feed entire machines in a room/building.

After the power gone, we recommend that a UPS keeps a server/servers alive for minimum 15 minutes. If it is important for a server/servers to survive hours without power, it should probably be a more robust power backup solution that includes a generator and other components.

If you get a UPS that's too big, then you've overpaid, but your equipment can survive a longer outage. If you get a UPS that's too small, your equipment might not be protected. Therefore, we recommend that you get advice from UPS vendors.

1.5 Network Requirements

We describe network requirements to provide general SCM services in network infrastructure examples shown in Figure 1.1, Figure 1.2, and Figure 1.3.

Our examples may not cover all conditions and requirements which are requested by clients. However we provide representative cases to deploy a network environment which is appropriate for SCM VoIP services.

For more detail information, you can see 'CHAPTER 2. Network Design Guide.'

1.5.1 Single Site Example

Following figure shows an example of network configuration for a single site. There is a SCM server which is an active-alone mode. O7400 Gateway is directly connected to PSTN. If needs, it can be connected to PSTN via a Legacy PBX. We recommend the voice network to be separated from the data network. For security, NAT and Firewall is also recommended.

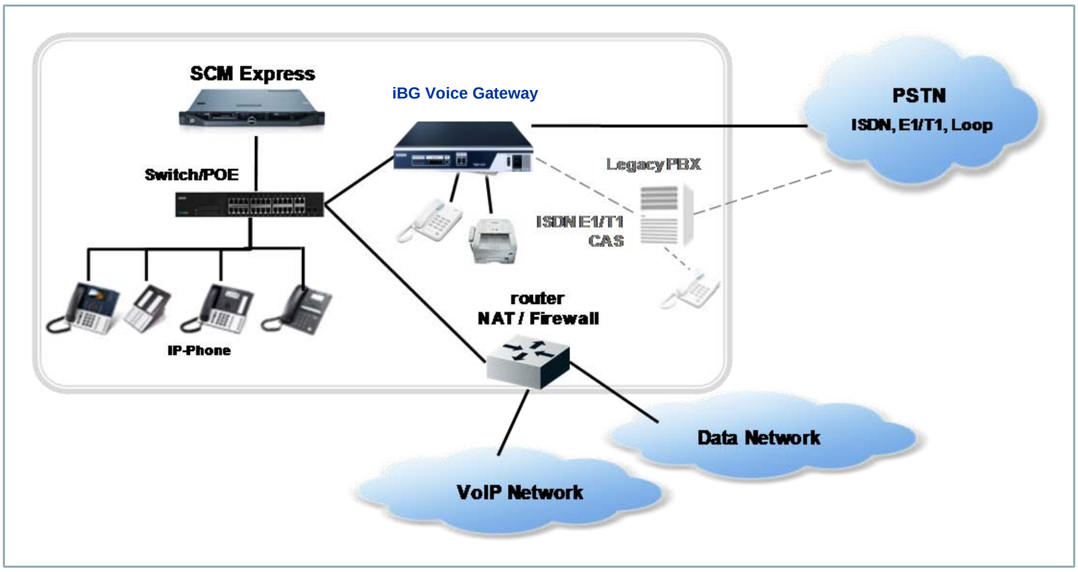


Figure 1.1 Configuration for a Stand Alone of SCM

Following figure shows an example of network configuration for an High Availability Service (Active-Standby) SCM. There two SCM servers where each SCM server is connected to both two switches. It is good to improve availability when one switch (network link) fails. OfficeServ 7400 Gateways can be duplicated too.

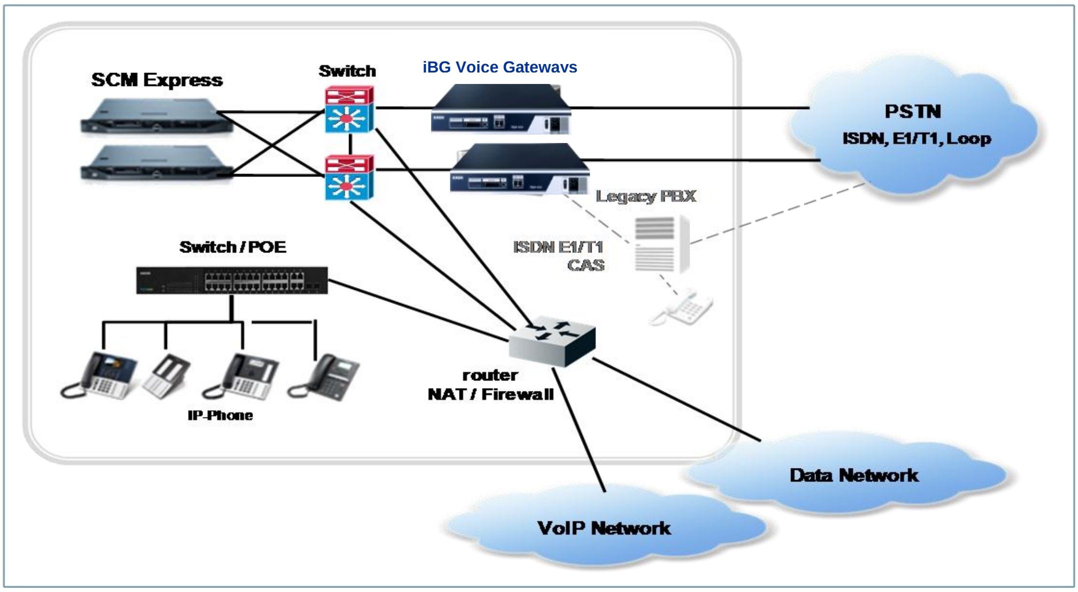


Figure 1.2 Configuration for Active-Standby of SCM

Following figure shows an example of network configuration for an High Availability Service (Active-Active) SCM.Two SCM servers set up a master node and a slave node. The master node using DB and Administrator can modify the information of the slave node. If one node of the two nodes is down or network is disconnected, Entire phones and gateways would be registered to other node and can continue to communicate.

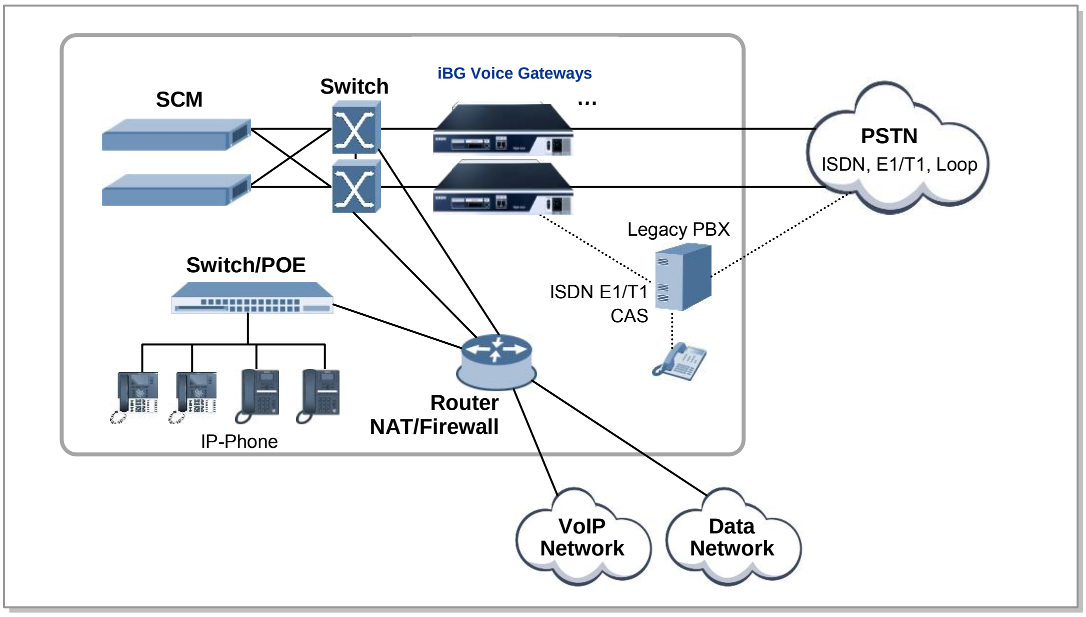


Figure 1.3 Configuration for Active-Standby of SCM

1.5.2 Headquarters and Branch Example

Following figure shows networks between a headquarters and a branch. The headquarters and the branch may have a dedicated link such as an E1 VPN or a MSPP tunnel.
The iBG2016 gateway in the branch may have a backup line which is connected to PSTN. The backup line is optional and it is used when the iBG2016 gateway loses a connection with SCM at the headquarters.

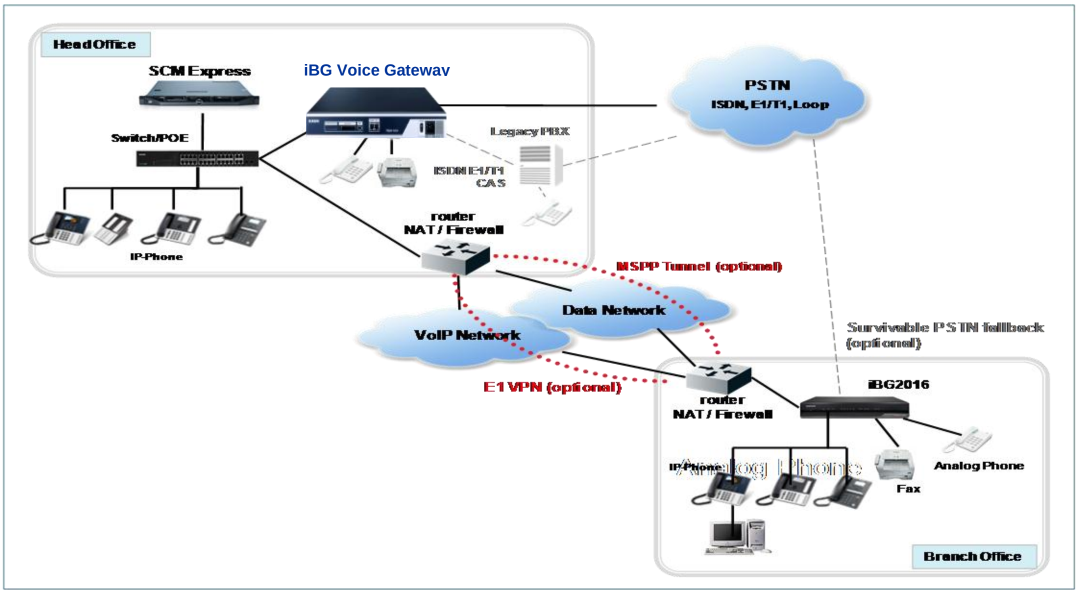


Figure 1.4 Configuration for Headquarter and branch

Following figure, there are multiple branches. Each branch is recommended to use NAT and Firewall to improve security. If there is no network node which supports the function of NAT and Firewall, you can configure iBG Gateways to provide the function of NAT and Firewall as well as the function of routing. The gateways in branches may have a connection to Local PSTN alternatively.

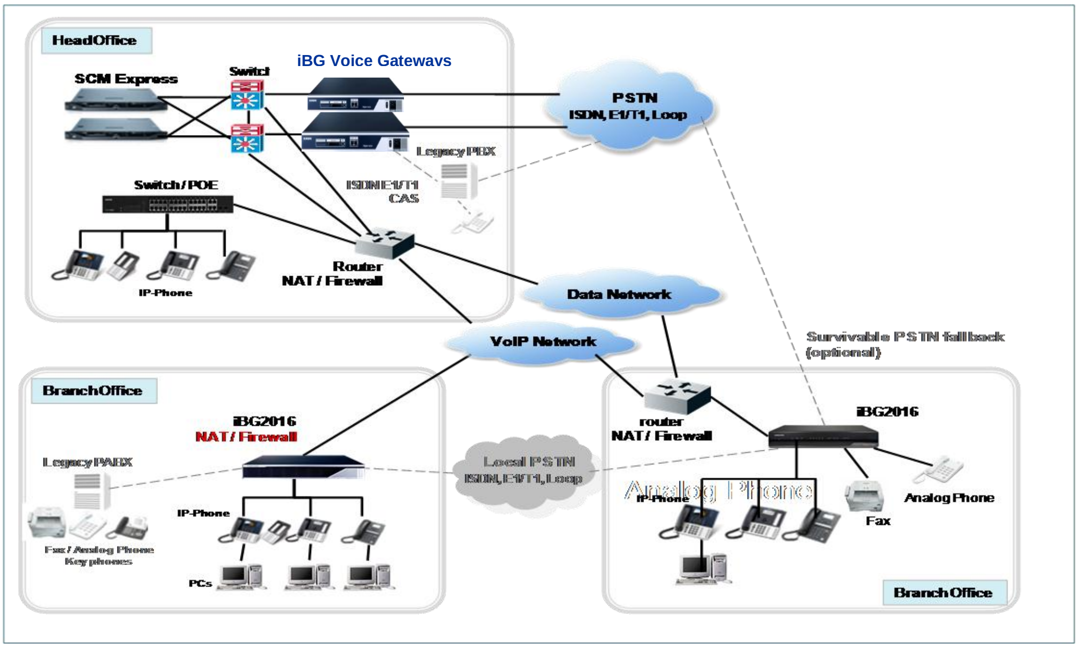


Figure 1.5 Configuration for Headquarter and multiple branches

Following figure, there are multiple branches. The SCM server of Active/Standby structure is configured as the master node and slave node. To work as one single network, NAT and firewall installation between nodes is not recommended

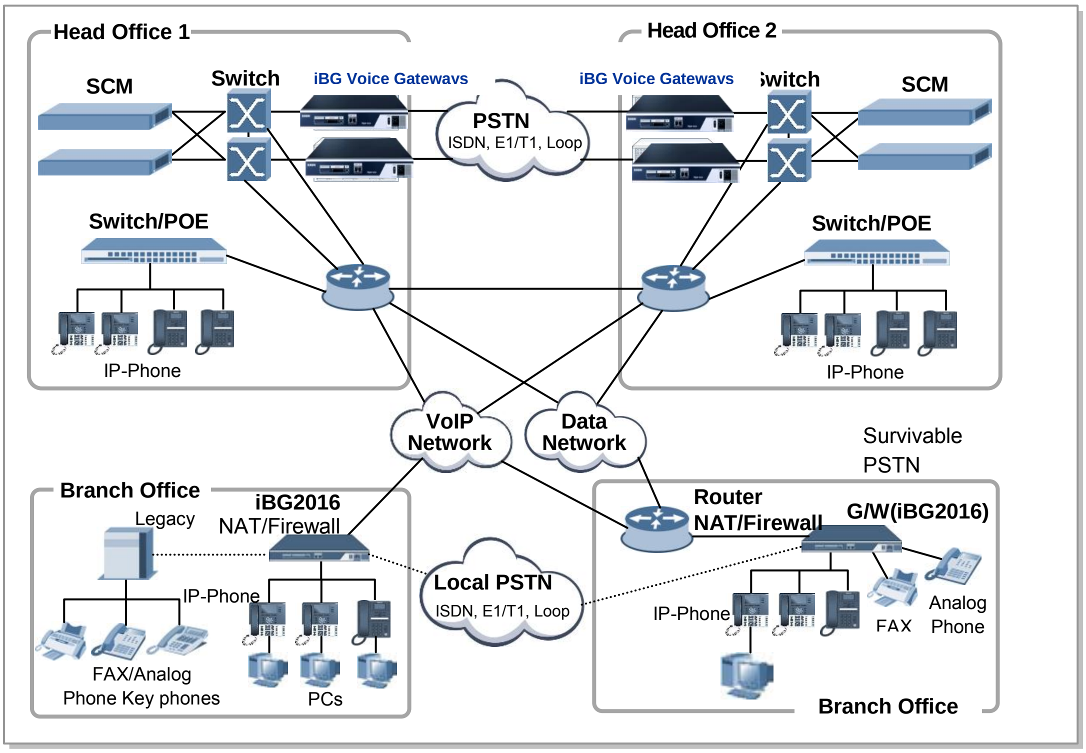


Figure 1.6 Configuration for Headquarter and multiple branches (Active-Active)

1.5.3 Network Considerations

Network Condition

- Packet loss rate < 0.1 %
- Packet delay < 100 ms (average)
  Packet delay < 200 ms (maximum)
- Jitter < 40 ms (maximum)

VLAN

1) Address space conservation and voice device protection from external networks: Private addressing of phones on the voice or auxiliary VLAN ensures address conservation and ensures that phones are not accessible directly via public networks. PCs and servers are typically addressed with publicly routed subnet addresses; however, voice endpoints should be addressed using RFC 1918 private subnet addresses.
2) Protection from malicious network attacks
   VLAN access control, 802.1Q, and 802.1p tagging can provide protection for voice devices from malicious internal and external network attacks such as worms, denial of service (DoS) attacks, and attempts by data devices to gain access to priority queues via packet tagging.
3) Ease of management and configuration
   Separate VLANs for voice and data devices at the access layer provide ease of management and simplified QoS configuration

NAT/Firewall

A NAT and firewall are recommended to prevent unauthorized Internet users from accessing SCM in private networks.

SCM has an embedded solution to provide Media Proxy. However SCM Enterprise does NOT provide it. If you want, you can deploy an additional network infrastructure such as Session Border Controller (SBC).

To access SCM from the public Internet, you need to configure NAT traversal and open several port numbers at NAT/Firewall. The port number list is in following tables.

Table 1.6 Port List for Management and Provisioning

Service	TCP Port	UDP Port	Description
General	20, 21	-	FTP Server
	22	-	Secure Shell
	23	-	Telnet
	80, 443	-	HTTP Web Server
	123	123	NTP

Table 1.6   Port List for Management and Provisioning (Continued)

Service	TCP Port	UDP Port	Description
Provisioning	69	-	TFTP Server
	8088	-	Gateway Provisioning
	-	6000	Phone upgrade from Proprietary to SIP
NMS	-	161	SNMP Agent
Personal Management	8080, 9500	-	Personal Assistant for Call Service
	4002, 4003, 4004	-	Single Sign-On, PWP for UMS/Conference
System Management	20001, 20002, 20003, 20005, 20006	-	SCM Administrator
	5432	-	PostGRE DBMS connection

Table 1.7   Port List for Telephony services

Service	TCP Port	UDP Port	Description
Call	5060, 5061	5060	SIP signaling
UMS	5080, 8624	5080	Call signaling for UMS
	-	14002~14130	RTP path for UMS
	25, 143, 993	-	Signaling for E-mail Server
	3681, 3683, 2001, 22001	-	Signaling for Outlook client
	2200	-	UMS File Server
Conference	3333	5090, 5098	Call signaling for Conference
	-	45000~49998	RTP path for Conference
MOH	-	35000~35999	RTP path for MOH/Announcement
MPS	-	40000~40799	RTP path for MPS (Media Proxy Service)
Others	6000~6127	-	CSTA link for each user group
	9050, 9052	-	PMS link
	9090, 9092	-	Proprietary Application server link
	9000, 9002	-	Voice Monitoring server link
	9011	-	MVS client link
	18122	-	mySingle link
	10306, 2300	-	CDR (Call Data Record)

CHAPTER 2. Network Design Guide

2.1 Overview

This document describes the design considerations and requirements for network infrastructure required when deploying the IPT service in a typical IPT network infrastructure as shown in following figure.

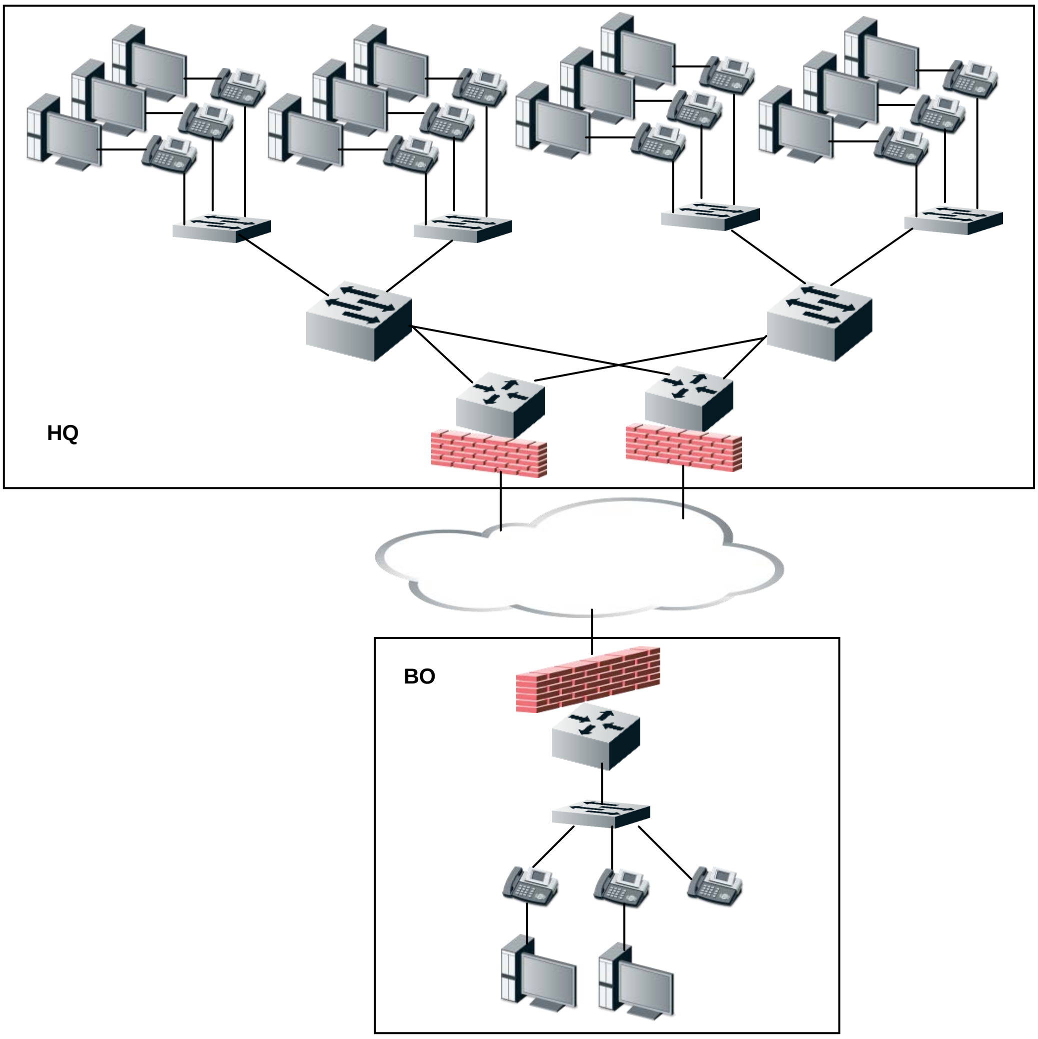


Figure 2.1 IPT Network Infrastructure

The IPT service is extremely sensitive to **IP packet loss, packet delay, and jitter**. Therefore, to deploy the IPT service, a network topology to which all available QoS and redundancy technologies are applied and in which convergence can be provided quickly when a network failure occurs, must be used.
That is, the network technology that will be described in the next chapter must be applied to the network infrastructure.

2.2 IP Network Considerations

2.2.1 Local Access Network (LAN)

For the IPT service in the LAN environment, the following should be considered: Setting up equipment so that basic communications can be performed properly, separating physically or logically the IPT network from the normal data network, and giving priorities by applying QoS-related concepts to the service.

The most common way to configure a logical domain in the LAN environment is to use the VLAN. For the IPT service, it is recommended in principle that the IPT network be configured with a separate VLAN and the QoS applied to it. The IPT network must also be configured so that quick connectivity to IP phones can be provided and the status of the link to be connected, including speed and duplex status, can be checked.

2.2.2 Virtual Local Access Network (VLAN)

The VLAN is a way to separate the physical switching ports into a logical broadcast domain. That is, the switching ports on the LAN are configured into one domain.

Within this single domain, multicast & broadcast traffic can be transmitted without limitations. On the IP data network, there exist many applications that generate multicast & broadcast traffic. Typical examples are ARP, RARP, VRRP, RIP, and OSPF. The VLAN is a technology that divides this multicast & broadcast domain to reduce unnecessary traffic.

Basically, to apply the VLAN to the IPT service properly, the VLAN for voice should be separated and the QoS should be configured to give a high priority to the VLAN for voice.

In the case of CISCO Ethernet switches, it is recommended to separate the voice VLAN due to the following reasons:

- Address space conservation and voice device protection from external networks

  Private addressing of phones on the voice or auxiliary VLAN ensures address conservation and ensures that phones are not accessible directly via public networks. PCs and servers are typically addressed with publicly routed subnet addresses; however, voice endpoints should be addressed using RFC 1918 private subnet addresses.

- QoS trust boundary extension to voice devices

  QoS trust boundaries can be extended to voice devices without extending these trust boundaries and, in turn, QoS features to PCs and other data devices.

- Protection from malicious network attacks.

  VLAN access control, 802.1Q, and 802.1p tagging can provide protection for voice devices from malicious internal and external network attacks such as worms, denial of service (DoS) attacks, and attempts by data devices to gain access to priority queues via packet tagging.

- Ease of management and configuration

  Separate VLANs for voice and data devices at the access layer provide ease of management and simplified QoS configuration.

2.2.3 Speed and Duplex Setup

Most recent devices providing an Ethernet interface have an auto-negotiation function. Auto-negotiation should first be enabled for the ports of the IP phones and PCs that will be connected to an Ethernet Switch. For old Ethernet switches or PCs or some IP phones, an auto-negotiation function is not provided. In this case, it may be that one party is set to half-duplex and the other party is set to full-duplex. Under these conditions, a packet loss occurs intermittently and has a major effect on the voice traffic's sound quality in the IPT environment. Therefore, it is absolutely essential to check that the speed and duplex options of the equipment to be connected are set to the same values. If the equipment at one end does not have auto-negotiation, the two pieces of equipment to be connected should be manually set to the same speed, and full-duplex if possible.

2.2.4 Spanning Tree-Related Setup

In the LAN environment, if the network is composed of Ethernet switches connected to each other, the spanning tree protocol should be enabled to prevent loops and provide a redundant path. When a new port is enabled or the root bridge changes, the spanning tree protocol raises a topology change event and requires a specific period of converged time to provide a stable network path. In the case of the IP phone, it is connected to an access port of an Ethernet switch and it is recommended to enable the following functions to make connections to IP phones smoothly:

2.2.4.1 PortFast

For the ports that do not generate BPDU and do not affect the network topology, such as ports of IP phones and PCs, the PortFast function should be enabled. If this function is enabled, when a port is connected to a switch, the port status is immediately changed so that data can be sent and received via the port, making the IP phones or PCs able to communicate immediately.

2.2.4.2 Root guard/BPDU guard

For the ports for which PortFast is enabled, it is also recommended to set a root guard and BPDU guard for them. This prevents those ports from becoming the root port (the port connected to the root bridge). Whenever the root port is changed, traffic is stopped for a certain period of time since the entire topology has to be re-calculated. This may cause a serious problem to user traffic. Moreover, when a BPDU guard is stably set, if a BPDU packet is received the BPDU guard makes the port change to blocking status to prevent potential dangers. When a BPUD packet is received, the port is changed to err-disable status. The port can be configured so that an administrator can re-enable it or it is enabled automatically after a specified period of time.

2.3 QoS (Quality of Service)

2.3.1 What Is QoS?

QoS refers to the quality of an application or service the end users of a network experience. For the IPT in particular, it frequently means call quality. To guarantee QoS, low latency and loss rates must be guaranteed for all voice packets in all paths through which they pass starting from an IP phone. To guarantee low delay and loss rates in a data network, such as LAN or WAN, where various types of packets are mixed, special measures must be taken for voice packets.

2.3.2 Basic Elements of QoS

To guarantee QoS for voice packets, the following basic technologies must be applied:

QoS setting (IP phone) or Marking:

When generating a voice packet in an IP phone or a soft phone running as a PC application, a marking or setting is made to indicate that it is a voice packet. Usually, a special value is set in the 802.1p field of the packet's Ethernet header or in the TOS byte field or DSCP field of the packet's IP header. According to Cisco's recommendations, the 802.1p or TOS byte field should be set to 5. The DSCP field should be set to 46 to configure the packet's class as Expedited Forwarding (EF) class.

- For not only voice packets but also voice signaling packets, video packets or the packets needed to run a voice application, QoS can ensure that their bandwidth is guaranteed. For these packets, it is also recommended that the packet generation application set an appropriate value in the 802.1p, TOS byte, and DSCP fields. Any value can be set for each traffic type. However they must be consistent within the same network environment (that is, connected Ethernet switches and routers) and be able to be recognized by all nodes. For example, if the DSCP field is set to 46 for voice packets in an IP phone, the connected Ethernet switches or routers should be able to recognize the voice packets for which the DSCP field is set to 46 and assign an appropriate bandwidth or priority to them.

Classification:

To guarantee QoS for each application's traffic (for example, voice packets, video packets, and voice signaling packets), the packets that belong to each application must be able to be recognized. The process that processes this operation is classification. For example, when an IP phone sends a voice packet for which the DSCP field is set to 46 and it reaches a LAN switch or WAN router, each node along the path the packet passes through checks the DSCP field value and, if it is 46, recognizes the packet as a voice packet. This process is called classification. Besides the 802.1p, TOS byte, and DSCP field values, network equipment provides another way to classify each application by using various data.

For example, if a special subnet address is assigned to voice equipment, the source or destination IP addresses are used for classification or the VLAN ID, protocol field, or application port can be used as the key for classification.
Classification refers to the process that classifies various mixed traffic into each application traffic type. A group of each of this classified traffic is called a class.

Action (Per-hop behavior):

The mechanism that provides QoS by applying a special rule to each of traffic groups classified by classification is called a policy or action. The following polices are required to guarantee the delay and loss rates for voice packets.

- Bandwidth Setup
- Priority Setup

For example, to compare the voice class with other classes and process it preferentially, the priority settings give a higher priority to the voice class and make it possible that when there are data traffic and voice traffic simultaneously, the voice traffic can be sent first. Alternatively, the following method can be used: When voice traffic and data traffic arrive at the same time, a specific bandwidth is assigned to voice traffic-regardless of the arrival order or the number of arrived packets-to guarantee the voice packets are sent at a specific transfer rate regardless of the amount of total traffic (bandwidth setup).

2.3.3 Applying the QoS Settings

IP Phone

IP Phone setting: Set the 802.1p, TOS byte, and IP DSCP values for the traffic generated by IP phones. All or some of these values can be set for each phone. The important point is that a field to which a value can be set should later be a standard for classification.
IP Phone’s Switch: An IP phone embeds a 3port Ethernet switch. The first port is connected to an upper PoE switch. The second is connected to the IP phone itself. The third is connected to a PC. The third is connected only if a PC is connected to an upper PoE switch via the IP phone. In the case of Samsung phones, this Ethernet switch is configured using their Configurations screen. Usually, for PC traffic and IP phone traffic, the 802.1p, DSCP, or TOS byte field can be set.

Soft Phone

Because a soft phone is a PC application, the 802.1p, DSCP and TOS byte settings cannot be configured in the PC’s Ethernet adapter and must be configured in the application itself.

Ethernet Switch or PoE Switch

For Ethernet switches, set a classification rule and action (policy), rather than a marking rule, for voice traffic. That is, classify voice traffic using the 802.1p, DSCP, and TOS byte fields and give priority and bandwidth to voice traffic to guarantee the delay or loss rate. For L3 switches with good specifications, besides those fields, provide an option in which voice, video, and voice signaling traffic can be classified using the source/destination IP address, application port, and protocol fields, etc. to guarantee QoS.

Wan Router

In case of the WAN Router, in general, the QoS settings are very important because the WAN link’s bandwidth is small. The QoS settings, classification and action should be configured for all WAN links though which voice traffic pass. Usually, for the WAN intervals, the 802.1p field is not used. Instead, set a classification rule so that voice packets are classified using the DSCP, TOS byte, source/destination IP address, application port, protocol fields, etc. Set an action so that priority and bandwidth are guaranteed for voice packets.

2.4 IP Applications

2.4.1 Domain Name System (DNS)

The DNS refers to the system that translates an Internet domain name into an IP address on a network. The DNS gives the advantage that a host can connect to another host on a network with only its domain name. A DNS server maintains a database in which domain names and their corresponding IP addresses are stored, and provides information when a host requests a translation. For example, if a host sends the domain name, www.sec.co.kr, to a DNS server, it sends an IP address like 201.57.66.216 to the host.

When using a DNS server to use domain names, each host requests a name to address translation from the DNS server to and performs the actual operation after receiving an IP address from it. However, if the connection to the DNS server is disconnected for any reason, the host cannot find out the IP address of other hosts it wants to connect to and thus cannot connect to them.

For this reason, it is better not to configure the DNS settings for the network elements on an IP telephony network. If the DNS settings, such as host name, domain name, DNS server address, etc. are not configured, the hosts on the network do not use the DNS and hence the disconnections due to a connection problem to the DNS server can be avoided.

2.4.2 Trivial File Transfer Protocol (TFTP)

TFTP is, like FTP, a protocol for transferring files, but which is designed to transfer files in a more simplified way than FTP. Since TFTP uses UDP as its transmission protocol, it has the disadvantage that it is unstable and, for example, data can be lost during data transmission. However, since it does not use such a complex protocol as FTP, it can be implemented simply. Because of this, it is frequently used when updating the firmware or configuration in an embedded system such as IP phones.

2.4.3 Network Time Protocol (NTP)

NTP is a protocol used to synchronize the clock times of the hosts connected to a network. NTP uses UTC to synchronize the system clock times up to 1/1000 seconds or less.

It is important to maintain an exact time all over the network, for several reasons. In the telephony service, a small difference in time can cause a problem. For example, the time stamps of the error logs, trace logs, and system reports for the errors that occur during network management must be synchronized.

NTP consists of NTP clients and a NTP server. An NTP client requests the server to exchange the exact current time. Through this, the client can calculate the link delay time using the difference with the server's time and adjust its clock to match it to the server's.

NTP supports clock synchronization by broadcasting as well as synchronizing by a client's request.

The routers and switches on an IP telephony network play the role of servers, set the exact time through time synchronization with an upper NTP server, and provide the clients with this time information.

IP phones or personal hosts play the role of clients, request time information from an NTP server, and synchronize their time with the received broadcast time information.

2.4.4 Dynamic Host Configuration Protocol (DHCP)

DHCP is a protocol that allows a network administrator to manage and assign the IP addresses of his organization's network from a central location. A DHCP server provides a way to dynamically assign the detailed configuration information, such as an IP address, default gateway information, and TFTP sever information, to the DHCP clients on the network. DHCP uses the concept of 'lease' in which an IP address assigned to a host is valid only for a specific period of time. The lease time can be varied depending on how long the Internet connection is needed at a specific location.

In an IP telephony network, there are many hosts to which an IP address has to be assigned since not only the user PCs but also IP phones exist on the network and it is inconvenient to manually assign IP addresses from an IP phone console. Therefore, it is better to use the dynamic assignment using DHCP.

The operation principle of DHCP is that, as shown in the figure below, a user (DHCP client) sends the DHCP DISCOVER message to obtain a DHCP lease. As the response to this message, the DHCP server sends the IP configuration information including an IP address and default gateway address. If the client accepts the information sent, it sends the REQUEST message to the server. The server then assigns the address and sends the ACK message to the client to complete the DHCP address assignment procedure.

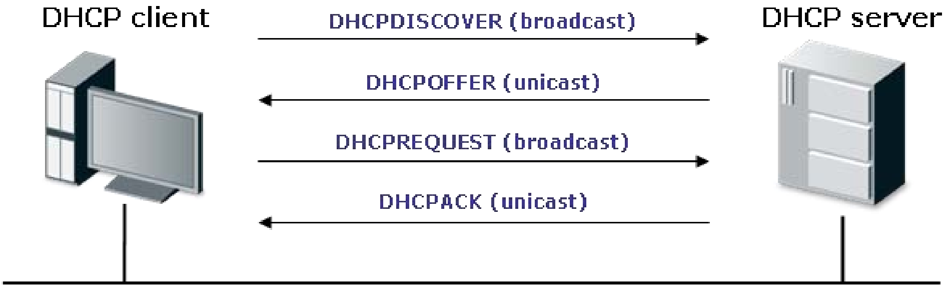


Figure 2.2 DHCP Request for an IP Address from a DHCP Server

Described below are the contents of the messages that are sent during the 4 step DHCP procedure above.

DHCP DISCOVER

The client sends the DISCOVER message to the server.

- Source port number: 68 (DHCP client port)
- Destination port number: 67 (DHCP server port)
- Source IP address: 0.0.0.0
- Destination IP address: 255.255.255.255 (broadcast address)

At this step, when receiving the DISCOVER message, the server searches the address pool for an available address and runs a ping test on the address found prior to assigning it to the client to avoid IP address duplication. If a ping response is received, it is recognized as an address being used and the server tries to assign another available address.

DHCP OFFER

The server sends the OFFER message to the client.

- Source port number: 67
- Destination port number: 68
- Source IP address: DHCP server's IP address
- Destination IP address: 255.255.255.255 or the IP address assigned by the DHCP server

DHCP REQUEST

The client sends the REQUEST message to the server.

- Source port number: 67
- Destination port number: 68
- Source IP address: The IP address assigned by the DHCP server
- Destination IP address: 255.255.255.255 (broadcast address)

DHCP ACK

The server sends the ACK message to the client.

- Source port number: 67
- Destination port number: 68
- Source IP address: DHCP server's IP address
- Destination IP address: The IP address assigned to the client by the DHCP server

2.5 Security (& Firewall)

A firewall serves to protect internal networks from external networks. To protect internal networks, a firewall blocks traffic that is not set in the firewall policy and allows only traffic that matches a service and IP address set in the policy. In the IPT operation environment, to communicate with an IP phone on an external network via a WAN interface, a firewall policy for IPT service must be set in each of the headquarters' and remote site's firewalls.

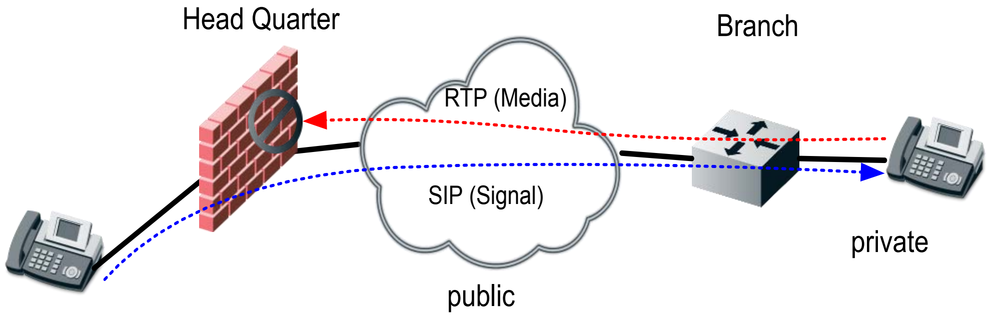


Figure 2.3 HQ-BO Network Diagram

In the previous firewall configurations, all outbound traffic is normally allowed and a policy is set to allow inbound traffic for the ports and IP addresses to be served. Recently, however, to protect against internal worm and virus propagations and block outflows of internal information, a policy is set to allow both of inbound and outbound traffic for specific services only.

When designing an IPT service network, the following items must be checked to add and modify the firewall policy.

- The firewall policy of the existing data communication network
- The service ports, protocols, and directions to be used in the IPT service
- The list of the IP addresses of the servers and IP phones to be operated for the IPT service

If the IPT service is operated at a single site or all VoIP nodes of the headquarters and branch offices are connected to a dedicated voice WAN network and use routable private IP addresses, no separate NAT configuration is needed. However, in a multiple site environment, if each of the headquarters and branch offices uses its own private IP addresses and the IPT is served via a public network, such as the Internet, the NAT function is required. The NAT function deployed in a router or firewall, through public to private IP address translations, not only supports a large number of private IP addresses with a small number of public IP addresses but also plays the role of hiding internal IP information from external networks. However, the NAT traversal problem can occur in the VoIP protocols, such as the SIP and H.323, for the following reasons:

- The IP address and port information is contained in the signaling packet's L7 payload.
- Different connections are being used for signaling and media (RTP).

The best method to solve the NAT traversal problem is to configure the network with only public IP addresses or to configure the network so that private IP addresses are used but they are made to be routable by using a dedicated network between the headquarters and branch offices.
However, if an existing data network is used and NAT must be used, the following technologies are available to solve the NAT traversal problem in present day network environments:

- Tunneling
- IPsec VPN, GRE over IPsec
- VoIP Aware Firewall NAT
- ALG (Application Level Gateway)
- SBC (Session Border Controller)
- STUN, TURN, ICE

This section describes the tunnel and SIP ALG.

IPSec VPN not only provides a secure encrypted communication channel between the headquarters and each branch office by connecting a virtual channel between them, but also provides a function allowing the users to use them as a same single site. If IPSec VPN is used in the Samsung IPT service environment, the same IPT service environment can be provided to a single site.

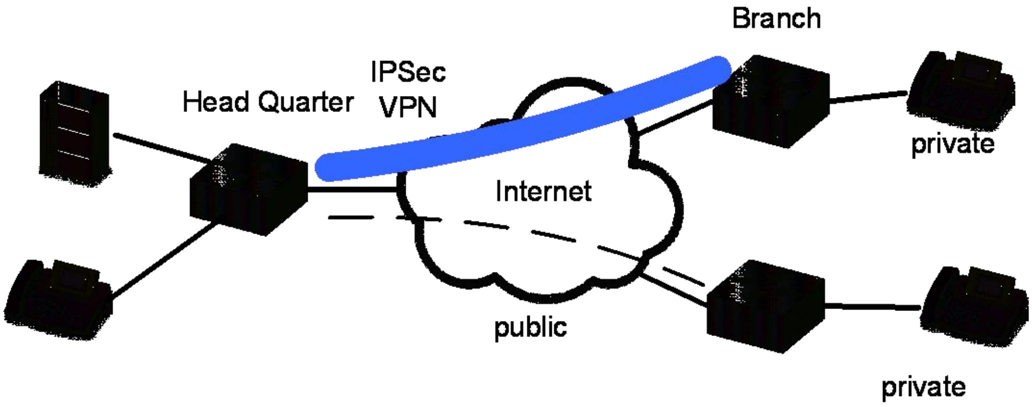


Figure 2.4 HQ-BO VPN Tunnel Configuration Example

The methods for configuring a tunnel between the headquarters and each branch office are divided into the following two types:

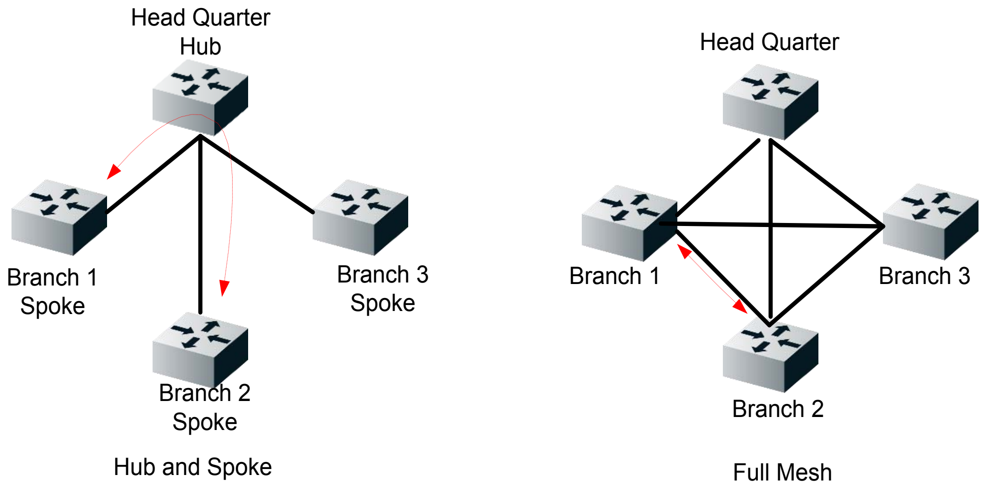


Figure 2.5 HQ-BO VPN Configuration Type

Hub and Spoke

- Each branch is tunneled to the headquarters only.
- Since the traffic between branches is transmitted via the headquarters, the delay and jitter are larger than in the Full Mesh type when supporting a VoIP service.

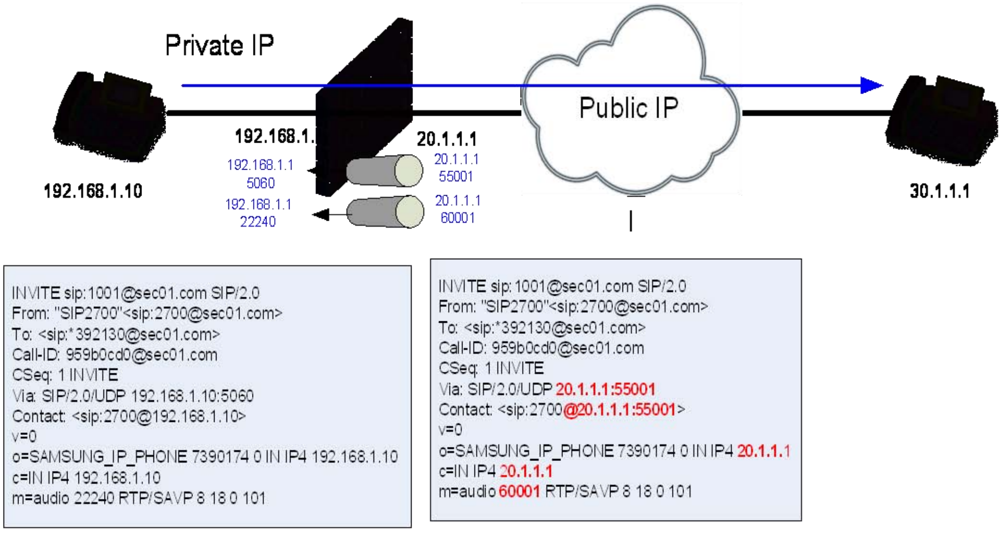
Full Mesh

- All branches and the headquarters are tunneled between themselves.
- The delay and jitter are smaller than in the Hub and Spoke type.
- As the number of branches increases, the configuration becomes more complex. When a new branch is added, the corresponding tunnel configurations must be added to other branches.

The VPN connection type should be determined by considering the IPI service’s traffic characteristics and the number of branches.

If the network is already connected between the headquarters and branch offices with an IPSec VPN, the QoS of the IPSec VPN must be considered to support the VoIP service via a tunnel.

Most of the firewalls and NAT equipment on the market not only change the L3 and L4 protocol header information during NAT but also recognize VoIP protocols, such as SIP and H.323, and change the IP address and port information for L7 VoIP packets. This is called the VoIP Aware Firewall/NAT or Application Level Gateway (ALG).



```
INVITE sip:1001@sec01.com SIP/2.0
From: "SIP2700"<sip:2700@sec01.com>
To: <sip:*392130@sec01.com>
Call-ID: 959b0cd0@sec01.com
CSeq: 1 INVITE
Via: SIP/2.0/UDP 192.168.1.10:5060
Contact: <sip:2700@192.168.1.10>
v=0
o=SAMSUNG_IP_PHONE 7390174 0 IN IP4 192.168.1.10
c=IN IP4 192.168.1.10
m=audio 22240 RTP/SAVP 8 18 0 101
```

```
INVITE sip:1001@sec01.com SIP/2.0
From: "SIP2700"<sip:2700@sec01.com>
To: <sip:*392130@sec01.com>
Call-ID: 959b0cd0@sec01.com
CSeq: 1 INVITE
Via: SIP/2.0/UDP 20.1.1.1:55001
Contact: <sip:2700@20.1.1.1:55001>
v=0
o=SAMSUNG_IP_PHONE 7390174 0 IN IP4 20.1.1.1
c=IN IP4 20.1.1.1
m=audio 60001 RTP/SAVP 8 18 0 101
```

Figure 2.6 ALG Configuration Example

The ALG carries out the following functions.

- Translates the internal IP address and port information for SIP and H.323 packets.
- Generates pin holes for RTP packets.

When operating the IPT, the firewall policy should be set after checking whether the firewall installed supports SIP ALG.
If the ALG function, which changes the content of SIP packets in the NAT equipment or firewall which is an intermediate node through which they pass, is implemented incorrectly or is not tested fully in interoperation with other VoIP systems, this may affect existing VoIP processing. Therefore, it is better to disable ALG supporting in the firewall or NAT equipment when using other NAT traversal functions, such as an SBC or tunnel.

2.6 IPT Service Deployment Guide

This chapter describes step by step the check points and configurations for each node on an IP network when deploying the IPT service. Therefore, the site engineers taking charge of the IPT service should check the check points for each node according to the procedure below and add a configuration to a node if a recommendation in this chapter is not set for it.

2.6.1 Workgroup Switch

2.6.1.1 Cisco Catalyst 3750 LAN Setup Guide

1) Voice VLAN Setup
For most Catalyst switches providing, such as Catalyst 2950/3750, the VLAN for voice is separated and the QoS function is operated for that VLAN automatically in order to provide the voice VLAN function and thus acquire a quality for voice packets. Therefore, by using the voice VLAN function, the protection function can be provided for the voice packets for IPT service.
For example, if an IP phone and a PC are connected to Fast Ethernet 0/1, the VLAN for voice set to 112, and the VLAN for data set to 12, configure the voice VLAN as follows:

```
CAT2950(config)# interface interface-id
CAT2950(config-if)# switchport mode access
CAT2950(config-if)# switchport voice vlan 112
CAT2950(config-if)# switchport access vlan 12
CAT2950(config-if)# exit
```

2) Speed and Duplex Setup
It is recommended to set the speed and duplex values to auto. You only have to set them as shown below. If you have to set the speed and duplex values manually, you can set them easily using the help on the speed command.

```
interface FastEthernet0/1
speed auto
```

3) Spanning Tree-Related Setup
If a host device, such as a PC or IP phone, is connected to the corresponding port, it is recommended that the convergence time required in the spanning tree protocol be minimized to make communication possible immediately. By using the Portfast command, you can change the port to the state that it is ready to communicate as soon as the link is set up. For a port that uses Portfast, it is assumed that a host device is used. Therefore, a problem may occur if a hub or switch is connected to the bottom end. To prevent this, it is recommended that a stabilization mechanism be provided by applying bpduguard and rootguard. Below is a spanning tree-related setup example.

```
interface FastEthernet0/1
spanning-tree portfast
spanning-tree portfast bpduguard
spanning-tree portfast rootguard
```

2.6.1.2 Cisco Catalyst 3750 QoS Setup Guide

In the Catalyst 3750, you can automatically generate the QoS configuration for protecting voice traffic using auto-QoS. Below is an example in which auto-QoS is enabled in the gigabitethernet2/0/1.

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# auto qos voip trust
```

You can view the Auto-QoS configuration using the ‘show auto qos interface gigabitethernet2/0/1’ command.
When auto-QoS is enabled, the content described in the highlighted descriptions below is applied, which you should be aware of.

- It is assumed that, for voice packets, the DSCP field is marked as 46 and the CoS field is marked as 5. The related configuration should be set in the IP phone. Voice packets are assigned to the strict priority queue, that is, queue 2.
- It is assumed that, for VoIP control packets, the DSCP field is marked as 24 or 26 and the CoS field is marked as 3. The related configuration should be set in the IP phone and soft phone. If there is no configuration made, packets are considered as All other traffic in Table 1 below and the corresponding QoS configuration is applied.
  VoIP control packets are assigned to the strict priority queue, that is, queue 2.
- It is assumed that, for real-time video traffic, the DSCP field is marked as 34 and the CoS field is marked as 4. The source generating real-time video traffic must set the values above. Real-time video traffic is assigned to the strict priority queue, that is, queue 2.

When auto-QoS is enabled, it uses the ingress packet label to categorize traffic, to assign packet labels, and to configure the ingress and egress queues as shown in following three tables.

Table 2.1 Traffic Types, Packet Labels, and Queues

<table>
<tr><th></th><th>VoIP Data Traffic</th><th>VoIP Control Traffic</th><th>Routing Protocol Traffic</th><th>STP BPDU Traffic</th><th>Real-Time Video Traffic</th><th colspan="2">All Other Traffic</th></tr>
<tr><td>DSCP</td><td>46</td><td>24, 26</td><td>48</td><td>56</td><td>34</td><td colspan="2">-</td></tr>
<tr><td>CoS</td><td>5</td><td>3</td><td>6</td><td>7</td><td>4</td><td colspan="2">-</td></tr>
<tr><td>CoS-to-Ingress Queue Map</td><td colspan="5">2, 3, 4, 5, 6, 7
(queue 2)</td><td colspan="2">0, 1
(queue 1)</td></tr>
<tr><td>CoS-to-Egress Queue Map</td><td>5
(queue 1)</td><td colspan="2">3, 6, 7
(queue 2)</td><td colspan="2">4
(queue 3)</td><td>2
(queue 3)</td><td>0, 1
(queue 4)</td></tr>
</table>

Table 2.2 Auto-QoS Configuration for the Ingress Queues

Ingress Queue	Queue Number	CoS-to-Queue Map	Queue Weight (Bandwidth)	Queue (Buffer) Size
SRR shared	1	0, 1	81 percent	67 percent
Priority	2	2, 3, 4, 5, 6, 7	19 percent	33 percent

Table 2.3 Auto-QoS Configuration for the Egress Queues

Egress Queue	Queue Number	CoS-to-Queue Map	Queue Weight (Bandwidth)	Queue (Buffer) Size for Gigabit-Capable Ports	Queue (Buffer) Size for 10/100 Ethernet Ports
Priority (shaped)	1	5	10 percent	16 percent	10 percent
SRR shared	2	3, 6, 7	10 percent	6 percent	10 percent
SRR shared	3	2, 4	60 percent	17 percent	26 percent
SRR shared	4	0, 1	20 percent	61 percent	54 percent

When you enable the auto-QoS feature on the first port, these automatic actions occur:

- QoS is globally enabled (mls qos global configuration command), and other global configuration commands are added.
- When you enter the **auto qos voip trust interface** configuration command on a port connected to the interior of the network, the switch trusts the CoS value for nonrouted ports or the DSCP value for routed ports in ingress packets (the assumption is that traffic has already been classified by other edge devices). The switch configures the ingress and egress queues on the port according to the settings in the above tables.

Besides the configurations above, the auto qos voip Cisco-phone command and the auto qos voip Cisco-softphone command can be used. However, these are applicable only if a Cisco phone or Cisco softphone is used. It is advisable to enable auto-QoS using the **auto qos voip trust interface** command.
When auto-QoS is enabled using the **auto qos voip trust interface** command, the QoS configuration shown in the following table is automatically generated in the switch.

Table 2.4 Generated Auto-QoS Configuration

Description	Automatically Generated Command
The switch automatically enables standard QoS and configures the CoS-to-DSCP map (maps CoS values in incoming packets to a DSCP value).	Switch (config)# mls qos Switch (config)# mls qos map cos-dscp 0 8 16 26 32 46 48 56
The switch automatically maps CoS values to an ingress queue and to a threshold ID.	Switch (config)# no mls qos srr-queue input cos-map Switch (config)# mls qos srr-queue input cos-map queue 1 threshold 3 0 Switch (config)# mls qos srr-queue input cos-map queue 1 threshold 2 1 Switch (config)# mls qos srr-queue input cos-map queue 2 threshold 1 2 Switch (config)# mls qos srr-queue input cos-map queue 2 threshold 2 4 6 7 Switch (config)# mls qos srr-queue input cos-map queue 2 threshold 3 3 5
The switch automatically maps CoS values to an egress queue and to a threshold ID.	Switch (config)# no mls qos srr-queue output cos-map Switch (config)# mls qos srr-queue output cos-map queue 1 threshold 3 5 Switch (config)# mls qos srr-queue output cos-map queue 2 threshold 3 3 6 7 Switch (config)# mls qos srr-queue output cos-map queue 3 threshold 3 2 4 Switch (config)# mls qos srr-queue output cos-map queue 4 threshold 2 1 Switch (config)# mls qos srr-queue output cos-map queue 4 threshold 3 0
The switch automatically maps DSCP values to an ingress queue and to a threshold ID.	Switch (config)# no mls qos srr-queue input dscp-map Switch (config)# mls qos srr-queue input dscp-map queue 1 threshold 2 9 10 11 12 13 14 15 Switch (config)# mls qos srr-queue input dscp-map queue 1 threshold 3 0 1 2 3 4 5 6 7 Switch (config)# mls qos srr-queue input dscp-map queue 1 threshold 3 32 Switch (config)# mls qos srr-queue input dscp-map queue 2 threshold 1 16 17 18 19 20 21 22 23

Table 2.4 Generated Auto-QoS Configuration (Continued)

Description	Automatically Generated Command
The switch automatically maps DSCP values to an ingress queue and to a threshold ID.	Switch (config)# mls qos srr-queue input dscp-map queue 2 threshold 2 33 34 35 36 37 38 39 48 Switch (config)# mls qos srr-queue input dscp-map queue 2 threshold 2 49 50 51 52 53 54 55 56 Switch (config)# mls qos srr-queue input dscp-map queue 2 threshold 2 57 58 59 60 61 62 63 Switch (config)# mls qos srr-queue input dscp-map queue 2 threshold 3 24 25 26 27 28 29 30 31 Switch (config)# mls qos srr-queue input dscp-map queue 2 threshold 3 40 41 42 43 44 45 46 47
The switch automatically maps DSCP values to an egress queue and to a threshold ID.	Switch (config)# no mls qos srr-queue output dscp-map Switch (config)# mls qos srr-queue output dscp-map queue 1 threshold 3 40 41 42 43 44 45 46 47 Switch (config)# mls qos srr-queue output dscp-map queue 2 threshold 3 24 25 26 27 28 29 30 31 Switch (config)# mls qos srr-queue output dscp-map queue 2 threshold 3 48 49 50 51 52 53 54 55 Switch (config)# mls qos srr-queue output dscp-map queue 2 threshold 3 56 57 58 59 60 61 62 63 Switch (config)# mls qos srr-queue output dscp-map queue 3 threshold 3 16 17 18 19 20 21 22 23 Switch (config)# mls qos srr-queue output dscp-map queue 3 threshold 3 32 33 34 35 36 37 38 39 Switch (config)# mls qos srr-queue output dscp-map queue 4 threshold 1 8 Switch (config)# mls qos srr-queue output dscp-map queue 4 threshold 2 9 10 11 12 13 14 15 Switch (config)# mls qos srr-queue output dscp-map queue 4 threshold 3 0 1 2 3 4 5 6 7
The switch automatically sets up the ingress queues, with queue 2 as the priority queue and queue 1 in shared mode. The switch also configures the bandwidth and buffer size for the ingress queues.	Switch (config)# no mls qos srr-queue input priority-queue 1 Switch (config)# no mls qos srr-queue input priority-queue 2 Switch (config)# mls qos srr-queue input bandwidth 90 10 Switch (config)# mls qos srr-queue input threshold 1 8 16 Switch (config)# mls qos srr-queue input threshold 2 34 66 Switch (config)# mls qos srr-queue input buffers 67 33

Table 2.4 Generated Auto-QoS Configuration (Continued)

Description	Automatically Generated Command
The switch automatically configures the egress queue buffer sizes. It configures the bandwidth and the SRR mode (shaped or shared) on the egress queues mapped to the port.	Switch (config)# mls qos queue-set output 1 threshold 1 138 138 92 138 Switch (config)# mls qos queue-set output 1 threshold 2 138 138 92 400 Switch (config)# mls qos queue-set output 1 threshold 3 36 77 100 318 Switch (config)# mls qos queue-set output 1 threshold 4 20 50 67 400 Switch (config)# mls qos queue-set output 2 threshold 1 149 149 100 149 Switch (config)# mls qos queue-set output 2 threshold 2 118 118 100 235 Switch (config)# mls qos queue-set output 2 threshold 3 41 68 100 272 Switch (config)# mls qos queue-set output 2 threshold 4 42 72 100 242 Switch (config)# mls qos queue-set output 1 buffers 10 10 26 54 Switch (config)# mls qos queue-set output 2 buffers 16 6 17 61 Switch (config-if)# srr-queue bandwidth shape 10 0 0 0 Switch (config-if)# srr-queue bandwidth share 10 10 60 20
If you entered the auto qos voip trust command, the switch automatically sets the ingress classification to trust the CoS value received in the packet on a nonrouted port by using the mls qos trust cos command or to trust the DSCP value received in the packet on a routed port by using the mls qos trust dscp command.	Switch (config-if)# mls qos trust cos Switch (config-if)# mls qos trust dscp
After creating the class maps and policy maps, the switch automatically applies the policy map called *AutoQoS-Police-SoftPhone* to an ingress interface on which auto-QoS with the Cisco SoftPhone feature is enabled.	Switch (config-if)# service-policy input AutoQoS-Police-SoftPhone

Effects of Auto-QoS on the Configuration

When auto-QoS is enabled, the auto qos voip interface configuration command and the generated configuration are added to the running configuration.

The switch applies the auto-QoS-generated commands as if the commands were entered from the CLI. An existing user configuration can cause the application of the generated commands to fail or to be overridden by the generated commands. These actions occur without warning. If all the generated commands are successfully applied, any user-entered configuration that was not overridden remains in the running configuration. Any user-entered configuration that was overridden can be retrieved by reloading the switch without saving the current configuration to memory. If the generated commands fail to be applied, the previous running configuration is restored.

2.6.2 Core Switch

2.6.2.1 Cisco Catalyst 6500/4500 LAN-related Setup Guide

1) **auxiliary VLAN**

For most Catalyst switches providing CatOS, such as Catalyst 6500/4500, the VLAN for voice is separated and the QoS function is operated automatically for that VLAN in order to provide the auxiliary VLAN function and thus acquire a quality for voice packets. Therefore, by using the auxiliary VLAN function, the protection function can be provided for the voice packets for IPT service.

For example, if an IP phone and a PC are connected to Fast Ethernet 0/1, the VLAN for voice set to 112, and the VLAN for data set to 12, configure the voice VLAN as follows:

```
cat6k-access> (enable) set vlan 12 name 10.1.10.0_data
cat6k-access> (enable) set vlan 112 name 10.1.110.0_voice
cat6k-access> (enable) set vlan 12 5/1-48
cat6k-access> (enable) set port auxiliaryvlan 5/1-48 112
```

2) **Speed and Duplex Setup**

It is recommended to set the speed and duplex values to auto. You have only to set them as shown below. If you have to set the speed and duplex values manually, you can set them easily using the help on the speed command.

```
cat6k-access> (enable) set port inlinepower 5/1-48 auto
cat6k-access> (enable) set port speed 5/1-48 auto
```

3) **Spanning Tree-Related Setup**

In the CatOS, you can optimize the properties of the port that is connected to a host device, such as a PC or IP phone, by using the 'set port host' command.

This command enables the portfast function, turns off trunk mode, and automatically turns off the link aggregation function, such as channel mode.

To prevent loops due to an abnormal hub or switch connection from a port to which Portfast is applied, it is recommended that a stabilization mechanism be provided by applying bpduguard to all ports to which Portfast is applied.

```
cat6k-access> (enable) set port host 5/1-48
cat6k-access> (enable) spanning-tree portfast bpduguard default
```

2.6.2.2 Cisco Catalyst 6000/6500 Port Scheduling

The Cisco Catalyst 6000/6500 supports two operating systems, IOS and CatOS.
This sections describes port scheduling for IOS.
Output Queueing Capability of Different Line Cards on the Catalyst 6500/6000
To enable QoS in the Catalyst 6000/6500, you should configure the following:

```
cosmos#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
cosmos(config)#mls qos
```

The Catalyst 6500/6000 provides a different queuing mechanism depending on the type of line card, that is, interface card. To check this, you should run the 'show interface capabilities' command. Below is an example.

```
cosmos #show interface gigabitethernet 6/2 capabilities
GigabitEthernet6/2
  Model                 : WS-SUP720-BASE
  Type                  : No GBIC
  Speed                 : 1000
  Duplex                : full
  Trunk encap. Type     : 802.1Q,ISL
  Trunk mode            : on,off,desirable,nonegotiate
  Channel               : yes
  Broadcast suppression : percentage(0-100)
  Flowcontrol           : rx-(off,on,desired),tx-(off,on,desired)
  Membership            : static
  Fast Start            : yes
  QOS scheduling        : rx-(1p1q4t), tx-(1p2q2t)
  CoS rewrite           : yes
  ToS rewrite           : yes
  Inline power          : no
  SPAN                  : source/destination
  UDLD                  yes
  Link Debounce         : yes
  Link Debounce Time    : yes
  Ports on ASIC         : 1-2
```

In the example above, the output queuing type of this port is 1p2q2t. The input queuing type is 1p1q4t.

The queuing type of each module can be found in this document.
http://www.cisco.com/en/US/products/hw/switches/ps700/products_tech_note09186a008015bf98.shtml

Receive Interface

To prevent voice packets from being dropped at the receive interface due to a congestion, they should be protected using queuing. It is assumed that the CoS, that is, 802.1p value of voice packets is set to 5 by the IP phone.

The following queuings are provided by default for each interface card type.

- rx-(1p1q4t)-one strict-priority queue and one wrr (Weighted Round Robin) queue with four thresholds
- rx-(1q4t)-one wrr queue with four thresholds
- rx-(1p1q0t)-one strict-priority queue and one wrr queue with no configurable thresholds.

The strict-priority queue is served first before other wrr queues. That is, when the strict-priority queue has a packet, it is served first before all of other queues.
1q4t port has the following drop-threshold configuration:

- Receive-queue drop threshold 1: When the buffer is filled 50 % or more, the switch drops the packets of CoS 0 or 1.
- Receive-queue drop threshold 2: When the buffer is filled 60 % or more, the switch drops the packets of CoS 2 or 3.
- Receive-queue drop threshold 3: When the buffer is filled 80 % or more, the switch drops the packets of CoS 4 or 5.
- Receive-queue drop threshold 4: When the buffer is filled 100 %, the switch drops the packets of CoS 6 or 7.

1P1Q4T is composed of one priority queue and one wrr queue. It has the following characteristics:

Queue #	% of Buffer Capacity	Drop CoS Value
1	50 %	0-1
1	60 %	2-3
1	80 %	4
1	100 %	6-7
2	100 %	5

That is, Queue 2 is the priority queue and receives packets for which CoS (Class of Service), that is, 802.1P is set to 5. It is processed preferentially before Queue 1.

Moreover, it does not drop packets until its buffer is filled 100 %. Queue 1 is a common queue. It receives other traffic. In the table above, the packets for which CoS is 4 are processed by a common queue. When the buffer is filled 80 %, packets start to be dropped. 1p1q0t port has the following drop-threshold configuration by default:

- The packets of CoS 0, 1, 2, 3, 4, 6 or 7 are filled in the wrr receive-queue. When the receive-queue buffer is filled 100 %, packets are dropped.
- The packets of CoS 5 are filled in the strict receive-queue. When the strict receive-queue buffer is filled 100 %, packets are dropped.

To use the queuing engine of the receive interface using the packets' CoS set already in the IP phone, the trust state of the port should be set to trust CoS using the following commands:

```
cosmos#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
cosmos(config)#interface gigabitethernet 1/1
cosmos(config-if)# mls qos trust cos
```

Transmit Queues

To prevent voice packets from being dropped at the transmit interface due to congestion, they should be protected using queuing. It is assumed that the CoS, that is, 802.1p value of voice packets is set to 5 by the IP phone.
You can check the queue structure of the port using the 'show interface capabilities' command. Check whether one of the following transmit queue sets is displayed:

- tx-(2q2t)-Two wrr queues and two drop thresholds for each wrr queue.
- tx-(1p2q2t)-One strict priority queue, two wrr queues and two drop thresholds or each wrr queue.
- tx-(1p3q1t)-One strict priority queue, three wrr queues and two drop thresholds for each wrr queue.

2q2t Ports
For the 2q2t port, each of the two wrr queues supports two drop thresholds as follows:

- The packets of CoS 0, 1, 2 or 3 are served by being filled in Queue 1.
- transmit queue 1, drop-threshold 1: When the queue buffer is filled 80 % or more, the packets of CoS 0 or 1 are dropped.
- transmit queue 1, drop-threshold 2: When the queue buffer is filled 100 % or more, the packets of CoS 2 or 3 are dropped.
- The packets of CoS 4, 5, 6 or 7 are served by being filled in Queue 2.
- transmit queue 2, drop-threshold 1: When the queue buffer is filled 80 % or more, the packets of CoS 4 or 5 are dropped.
- transmit queue 2, drop-threshold 2: When the queue buffer is filled 100 % or more, the packets of CoS 6 or 7 are dropped.

1p2q2t Ports

For the 1p2q2t port, one strict priority queue and two wrr queues are provided Each of wrr queues supports two drop thresholds as follows.

- The packets of CoS 0, 1, 2 or 3 are served by being filled in Queue 1.
- transmit queue 1, drop-threshold 1: When the queue buffer is filled 80 % or more, the packets of CoS 0 or 1 are dropped.
- transmit queue 1, drop-threshold 2: When the queue buffer is filled 100 % or more, the packets of CoS 2 or 3 are dropped.
- The packets of CoS 4, 6 or 7 are served being filled in Queue 2.
- transmit queue 2, drop-threshold 1: When the queue buffer is filled 80 % or more, the packets of CoS 4 are dropped.
- transmit queue 2, drop-threshold 2: When the queue buffer is filled 100 % or more, the packets of CoS 6 or 7 are dropped.
- The packets of CoS 5 are served by being filled in Queue 3, that is, a strict-priority queue. They are dropped when the queue buffer is filled 100 %.

To use QoS in the Catalyst 6500/6000, QoS should be configured with the following steps:

- Enable QoS.
- (This step is optional) Map CoS values to the queues and drop thresholds.

1) Enable QoS. Follow this example:

```
cosmos#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
cosmos(config)#mls qos

QoS is enabled globally
   Microflow policing is enabled globally

QoS global counters:
    Total packets: 552638
    IP shortcut packets: 0
    Packets dropped by policing: 0
    IP packets with TOS changed by policing: 0
    IP packets with COS changed by policing: 0
    Non-IP packets with CoS changed by policing: 0
```

2) Map CoS values to the queues and drop thresholds.
For example, for the 1p2q2t ports, Queue 1 is a wrr queue with the lowest priority. Queue 2 is a wrr queue with high-priority. Queue 3 is a strict-priority queue. If the CoS value of voice packets is not 5, you should map the value to the priority queue by applying the example below:

```
cosmos#configure terminal
cosmos(config)#interface gigabitethernet 1/1
cosmos(config-if)#priority-queue cos-map 1 5  !--- Assign a CoS of 5 to
priority queue.  cos-map configured on:  Gi1/1 Gi1/2
cosmos(config-if)#wrr-queue cos-map 1 1 0 1  !--- Assign CoS 0 and 1 to
the first threshold of low-priority WRR queue.
  cos-map configured on:
Gi1/1 Gi1/2
cosmos(config-if)#wrr-queue cos-map 1 2 2 3  !--- Assign CoS 2 and 3 to
the second threshold of low-priority WRR queue.
 cos-map configured on: Gi1/1 Gi1/2
cosmos(config-if)#wrr-queue cos-map 2 1 4 6  !--- Assign CoS 4 and 6 to
the first threshold of high-priority WRR queue.
  cos-map configured on:  Gi1/1 Gi1/2
cosmos(config-if)#wrr-queue cos-map 2 2 7  !--- Assign CoS 7 to the
first threshold of high-priority WRR queue.
  cos-map configured on:
Gi1/1 Gi1/2Check the configuration:

cosmos#show queueing interface gigabitethernet 1/1

!--- Output suppressed.

Queue  thresh   cos-map
    ---------------------------------------
    1    1     0 1
    1    2     2 3
    2    1     4 6
    2    2     7
    3    1     5
!--- Output suppressed.
```

You can check QoS information using the following commands: You can check that CoS 5 is assigned to the priority queue.

```
cosmos#show queueing interface gigabitethernet 1/1
Interface GigabitEthernet1/1 queueing strategy:  Weighted Round-Robin
  Port QoS is enabled
  Port is untrusted
  Default COS is 0
  Transmit queues [type = 1p2q2t]:
    Queue Id    Scheduling  Num of thresholds
    -----------------------------------------
       1       WRR low           2
       2       WRR high          2
       3       Priority          1
    WRR bandwidth ratios:   20[queue 1]  80[queue 2]
    queue-limit ratios:    70[queue 1]  15[queue 2]
    queue random-detect-max-thresholds
    ----------------------------------
      1   50[1] 80[2]
      2   40[1] 60[2]
    queue thresh cos-map
    ---------------------------------------
    1     1      0 1
    1     2      2 3
    2     1      4 6
    2     2      7
    3     1      5

  Receive queues [type = 1p1q4t]:
    Queue Id    Scheduling  Num of thresholds
    -----------------------------------------
       1         Standard          4
       2         Priority          1

    queue tail-drop-thresholds
    --------------------------
    1    100[1] 100[2] 100[3] 100[4]

    queue thresh cos-map
    ---------------------------------------
    1     1      0 1
    1     2      2 3
    1     3      4
    1     4      6 7
    2     1      5

  Packets dropped on Transmit:
    BPDU packets:  0

    queue thresh    dropped  [cos-map]
    ---------------------------------------------------
    1     1             0    [0 1 ]
    1     2             0    [2 3 ]
    2     1             0    [4 6 ]
    2     2             0    [7 ]
    3     1             0    [5 ]

  Packets dropped on Receive:
    BPDU packets:  0

    queue thresh    dropped  [cos-map]
    ---------------------------------------------------
    1     1             0    [0 1 ]
    1     2             0    [2 3 ]
    1     3             0    [4 ]
    1     4             0    [6 7 ]
    2     1             0    [5 ]
```

For more information on QoS configuration for the Catalyst 6500/6000, visit the link below. http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps708/prod_white_paper0900aecd80233956.html

2.6.3 DHCP Server

In an IP telephony network, since user PCs and IP phones are mixed on it and it is very inconvenient to assign IP addresses to IP phones manually, from the standpoint of network management, it is better to use DHCP to manage IP addresses smoothly. Moreover, if the network is managed with the data and voice networks divided logically, IP address management becomes more convenient and the management of IP address and IP phone configurations through DHCP also becomes simpler.

The figure below shows an example in which a network is divided into voice and data networks. This section describes the procedure to configure the DHCP service using the DHCP server contained in the CISCO router based on the network architecture below.

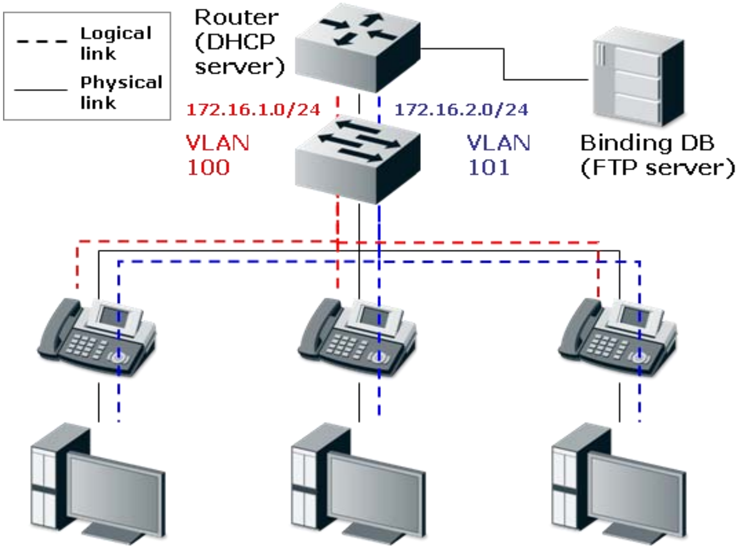


Figure 2.7 DHCP Deployment Configured with Voice and Data VLANs

1) Enabling the DHCP Service

```
Router(config)# service dhcp
```

Enable the DHCP service. (default enable)

2) Configuring the DHCP Database Agent and DHCP Conflict Logging

Set the database agent that will periodically store the DHCP binding information in a permanent storage device. In DHCP, the binding information in which lease information is contained should be maintained between the server and client.

To do this, the binding database is stored in an external storage device so that binding information can be preserved even when an unexpected reboot or shutdown occurs. Generally, binding information can be stored in a file at a remote location via a protocol, such as FTP or TFTP. Even if the system has been rebooted, the lease information for the client can be recovered by loading binding information from the database.

Below is an example in which the database agent is configured to store binding information at the 172.16.4.253 host via FTP. In this example, the server records the changes of the database with an interval of 120 seconds.

```
Router(config)# ip dhcp database
ftp://user:password@172.16.4.253/router-dhcp write-delay 120
```

When an address conflict is detected through the ICMP echo or DHCPDECLINE message, the DHCP conflict logging function transmits the conflict information using a syslog message and thus ensures the address remains unused. It is disabled by default. By doing so, even if a conflict occurs temporarily, when it is cleared afterward, the address can be reused.

```
Router(config)# no ip dhcp conflict logging
```

3) Selecting Addresses to Exclude from Dynamic Assignment

By default, the DHCP server is configured to assign sequentially all addresses in the subnet that the address pool has. If a network administrator does not want to assign some addresses dynamically, an exclusion setting should be made for them. To do so, set the address band not to be assigned to DHCP clients using the excluded-address command, which operates in the global configuration mode, as follows:

```
Router(config)# ip dhcp excluded-address low-address [high-address]
```

4) Configuring a DHCP Address Pool

In the DHCP server, an address to be assigned to a client can be selected from an address pool. Each address pool has a name of string type. You can configure an address pool by setting the pool name and pool parameters as shown in the procedure below:

- Configuring the DHCP Address Pool Name and Entering DHCP Pool Configuration Mode
- Set the DHCP address pool name. You then enter the DHCP pool configuration mode.

```
Router(config)# ip dhcp pool name
Router(config-dhcp)#
```

- Configuring the DHCP Address Pool Subnet and Mask
- Configure the subnet address and netmask for the newly created DHCP address pool. By default, all addresses within the subnet address band configured at this step can be assigned to clients.

```
Router(config-dhcp)# network network-number [mask | /prefix-length]
```

- Configuring the Address Lease Time
- By default, each address has a lease period of one day. The lease period can be changed using the following lease command:

```
Router(config-dhcp)# lease {days [hours][minutes] | infinite}
```

- The lease time can be varied depending on how long the Internet connection is needed at a specific location. If more hosts than the number of available IP addresses exist, the network should be made to be reconfigured dynamically and continually by shortening the lease period of IP addresses. However, in the IP telephony network environment, it is better that once an address is assigned to an IP phone, it is not changed frequently. If the address of an IP phone changes because the information configured for the IP telephony service using the previous address is also changed, a service synchronization operation is required. It is therefore better that the DHCP lease period is set to one week or longer for an IP telephony network in which the network architecture or configuration does not change frequently once it is deployed.
- Configuring the Pool Parameters
- Configure the network settings, such as the domain name, DNS server IP address, NetBIOS server address, and default router to be used by the clients.
- In the example below, a DHCP address pool is configured for each address band when VLAN 100 and 101 exist as shown in the figure above. The pool data and pool voice are the address pool for each VLAN, respectively. Each of them is an address pool for the network 172.16.1.0/24 and 172.16.2.0/24. The domain name and DNS server information are set for each pool. The addresses, except those set as excluded-address, are assigned to the clients and the lease period is set to 30 days.

```
ip dhcp excluded-address 172.16.1.100 172.16.1.103
ip dhcp excluded-address 172.16.2.100 172.16.2.103
!
ip dhcp pool data
      network 172.16.1.0 /24
      domain-name sec.com
      dns-server 172.16.1.102 172.16.2.102
      default-router 172.16.1.100 172.16.1.101
      lease 30
!
ip dhcp pool voice
      network 172.16.2.0 /24
      domain-name sec.com
      dns-server 172.16.1.102 172.16.2.102
      default-router 172.16.2.100 172.16.2.101
      lease 30
```

5) Viewing the DHCP Server Information

```
Router# show ip dhcp binding [address]
```

- Check a list of binding information with clients created in the DHCP server.

```
Router# show ip dhcp conflict [address]
```

- Check a list of conflict addresses recorded in the DHCP server.
- Check the statistics information related to the DHCP server and the message transmission reception statistics information.

```
Router# show ip dhcp server statistics
```

2.6.4 Security device

Table 7 shows a list of the service, protocol and port pairs used in the OfficeServ IPT service environment. Referring to this, you should set a firewall for a service which is transmitted between the headquarters and a branch via a WAN network. The tables and configurations below show an example of configuring a Cisco firewall for the headquarters and branch offices in the SIP-based IPT operation environment.

Table 2.5 Firewall Configurations for the Headquarters

Priority	Dir	Service	Port	Source	Destination
1	In	SIP	UDP 5060 TCP 5060	IP address area for branches	SCM
2	In	SIP TLS	TCP 5061	Branch IP address area	SCM
3	Out	SIP	UDP 5060 TCP 5060	SCM	Branch IP address area
4	Out	SIP TLS	TCP 5061	SCM	Branch IP address area
5[1]	In	RTP	Any	External branch IP address area	Internal IP phone IP address area
6	Out	RTP	Any	Internal IP phone IP address area	External branch IP address area
7	Out	NTP	TCP 123 UDP 123	SCM Server	External NTP server
8	Out	SNMP	UDP 161	NMS server	Branch IP phone area
9	In	SNMPTrap	UDP 162	Branch IP phone area	NMS server
10	In	HTTP	TCP 80	External branch IP address area	SCM Server
11	In	NTTPS	TCP 443	External branch IP address area	SCM Server
12	In	TFTP	UDP 69	External branch IP address area	SCM Server

1) For the firewalls and NAT equipment that support the ALG function, a policy for RTP does not need to be set since the firewall policy is generated by dynamic pin-hole connection.

Table 2.6 Firewall Configurations for Branch Offices

Priority	Dir	Service	Port	Source	Destination
1	In	SIP	UDP 5060 TCP 5060	Headquarters/other branch IP addresses	Internal IP phone IP addresses
2	In	SIP TLS	TCP 5061	Headquarters/other branch IP addresses	Internal IP phone IP addresses
3	Out	SIP	UDP 5060 TCP 5060	Internal IP phone IP addresses	Headquarters/other branch IP addresses
4	Out	SIP TLS	TCP 5061	Internal IP phone IP addresses	Headquarters/other branch IP addresses
5	In	RTP	UDP ANY	External branch IP address area	Internal IP phone IP addresses
6	Out	RTP	UDP A NY	Internal IP phone IP addresses	External branch IP address area
7	Out	TFTP	UDP 69	IP phone address	TFTP Server
8	Out	NTP	TCP 123 UDP 123	IP phone address	External NTP server
9	In	SNMP	UDP 161	NSM server	IP phone address
10	Out	SNMPTrap	UDP 162	IP phone address	NSM server
11	Out	HTTP	TCP 80	Internal IP phone IP addresses	SCM

You should configure the IPT policy for the firewalls operating in the data network in accordance with the tables above. Below is an example of how to configure the IPT service in a Cisco firewall:

Set the Access-list.

Set the ACL with the ports and IP addresses for which the IPT service is to be allowed. Below is an example of how to configure a firewall for the headquarters based on Table 2.5 Firewall Configurations for the Headquarters.

```
ip access-list extended HQ_out_access_list
permit udp any host <<ntp_server_ip>> eq ntp
permit udp any host <<dns_server_ip >> eq dns
permit udp any <<branch_ip_range>> eq sip
permit tcp any <<branch_ip_range>> eq sip
permit tcp any <<branch_ip_range>> eq 5061
deny ip any any
!
ip access-list extended HQ_in_access_list
permit udp <<nms_server_ip>> any eq snmp
permit udp any host <<tft_server_ip>> eq tftp
permit tcp any host <<http_server_ip> eq http
permit udp any <<branch_ip_range>> eq sip
permit tcp any <<branch_ip_range>> eq sip
deny ip any any
```

The firewalls for branch offices should also be configured referring to table. Firewall Configurations for Branch Offices.

Create the Cisco Inspect Rule.

The inspect command sets the Stateful Packet (SPI) function for a Cisco ACL. When the inspect command with timeout 180 is executed for the SIP protocol, the firewall creates and manages the SIP response messages and pin-hole connections to RTP.

```
ip inspect name IPT_INSPECT_1 sip timeout 180
ip inspect name IPT_INSPECT_1 tftp timeout 30
ip inspect name IPT_INSPECT_1 http timeout 60
ip inspect name IPT_INSPECT_1 dns timeout 10
ip inspect name IPT_INSPECT_1 ssh timeout 3600
ip inspect name IPT_INSPECT_1 snmp timeout 60
ip inspect name IPT_INSPECT_1 icmp timeout 60
ip inspect name IPT_INSPECT_1 tcp timeout 3600
ip inspect name IPT_INSPECT_1 udp timeout 60
```

Cisco inspect is an ALG function. If a firewall from another vendor besides Cisco’s is used, you should check whether it supports the ALG function and then determine whether to enable the ALG function.

If the ALG function is not used, the firewall policy for RTP traffic should be set separately. Generally, because the RTP traffic used by VoIP peers uses a wide area of UDP ports, if the inbound and outbound firewall permission policy is set explicitly for RTP traffic, internal security may become weak.

Set the ACL and Inspect Rule for Network Interface

```
interface FastEthernet0/0
  ip access-group HQ_in_access_list in
ip inspect IPT_INSPECT_1 in
!
interface FastEthernet0/1
  ip access-group HQ_out_access_list out
ip inspect IPT_INSPECT_1 out
```

IPSec VPN not only provides a secure encrypted communication channel between the headquarters and each branch office by connecting a virtual channel between them, but also provides a function allowing the users to use them as a same single site.

If IPSec VPN is used in the Samsung IPT service environment, the same IPT service environment can be provided to a single site.
Cisco VPN equipment also support QoS for encrypted ESP and AH packets. For more information on Cisco IPSec VPN and QoS supporting, visit the URL below.

- Configuring Per Site QoS with IPsec VPN
- PIX/ASA 7.x: QoS for VoIP Traffic on VPN Tunnels Configuration Example

In the network environment for which the IPT needs to be supported using NAT without connecting tunnels between single sites or multiple sites, a plan for solving the NAT traversal problem is required. If a dedicated system for solving the NAT traversal problem, such as SBC, cannot be used in that network environment, the firewall and NAT equipment should support NAT traversal. The SIP ALG function of the firewall and NAT equipment analyzes SIP packets and then performs public/private IP address and port translation for SIP packet payloads and creates pin hole connections for RTP packets. In the NAT environment, with Cisco products, the inspection function described previously performs the ALG function.

Below is an example of how to configure the NAT in the Cisco IOS.
Define the IP area to apply NAT to using the ACL.
Define the IP area of LAN environment to which NAT will be applied using ACL.

```
access-list 7 permit 192.168.1.0 0.0.0.24
access-list 7 permit 192.168.2.0 0.0.0.24
```

Create a NAT pool and configure the ACL for NAT.

```
ip nat pool ovrld 172.16.10.1 172.16.10.1 prefix 24
 !
ip nat inside source list 7 pool ovrld overload
 !
```

Configure NAT for network interfaces.

```
interface ethernet 1
 ip address 10.10.20.1 255.255.255.0
 ip nat inside

interface serial 0
 ip address 172.16.10.64 255.255.255.0
 ip nat outside
```

2.6.5 WAN Router

2.6.5.1 An example for configuring a Cisco WAN router (2800, 3800, 7200)

You should configure QoS for each link at the Cisco WAN router. To provide the best voice quality, it is better to configure QoS for outbound traffic from the interface.

Defining the voice traffic

First, define the voice traffic as follows:

```
access-list 100 permit ip any any precedence 5
access-list 100 permit ip any any dscp ef
```

Define the voice control traffic as follows:

```
! MGCP Control Traffic
access-list 101 permit udp any host 10.1.10.20 2427
access-list 101 permit tcp any host 10.1.10.20 2428
!
! H.323 Control Traffic
access-list 101 permit tcp any host 10.1.10.20 1720
access-list 101 permit tcp any host 10.1.10.20 range 11000 11999
```

For SIP or OSPP, the access-list should be defined using the proper port range information.

```
class-map VoIP-RTP
match access-group 100
class-map VoIP-Control
match access-group 101
```

Defining the class-map for voice traffic/voice control traffic

```
policy-map QoS-Policy
class VoIP-RTP
priority 100       # 100 means 100 kbps for a single call. If there are
# multiple voice calls, you should increase this value
class VoIP-Control
bandwidth 8        # 8 means 8 kbps for a single call. If there are
multiple
# voice calls, you should increase this value
class class-default
fair-queue         # Other traffic is processed in the round robin
method.
# for each flow.
```

Setting the policy for each class-map

```
interface FastEthernet1/0
service-policy output QoS-Policy
```

Applying the policy to all interfaces

```
show service-policy interface FastEthernet1/0
```

Checking the applied policy

2.7 IPT Requirements and Measurement

Below are the requirements for a smooth IPT service.

- Packet loss rate: 0.1 % or less
- Packet delay: Average 100 ms or less, maximum 200 ms or less
- Jitter: Maximum 40 ms or less

If the IPT service has been deployed in accordance with the directions in Chapter 3, using the following criteria and tool measure whether the IP network where the IPT service is deployed meets the requirements above. If it does not meet the requirements above, it is recommended that the IPT service be deployed after it is made to meet the requirements above by optimizing it in accordance with the directions in the 'IP Network Infrastructure' section.

1) Measurement Criteria
   - When measuring data, make sure to include the time when the most IP network traffic occurs.
   - Measure 8 times or more a day for at least one week.
   - Measure data including the longest path through which the IPT service is provided.

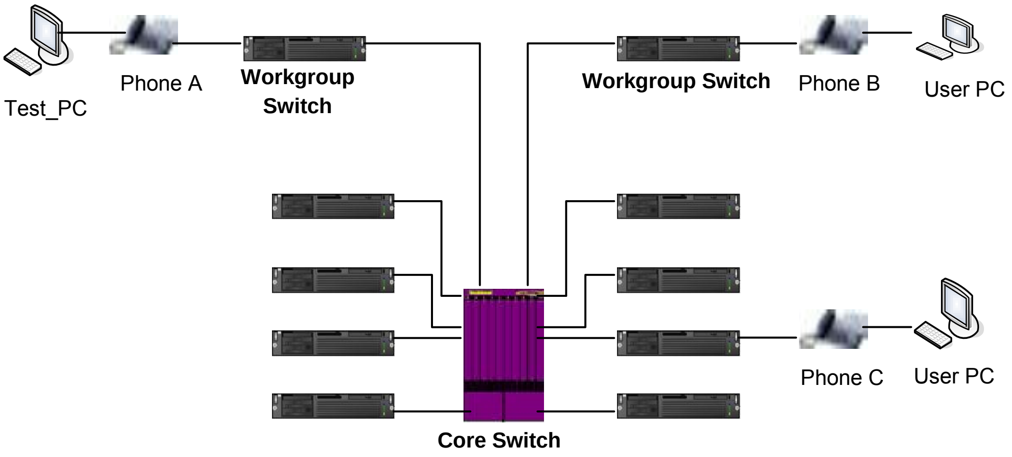
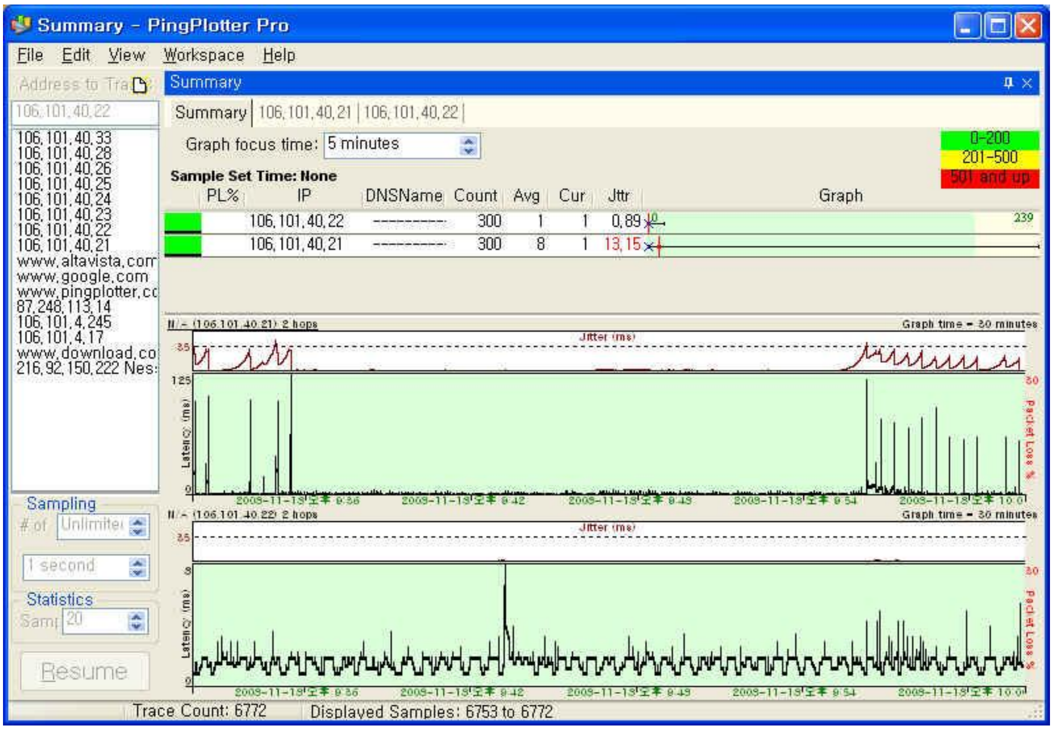


Figure 2.8 Test Network Architecture

2) Measurement Tool
   - Ping Plotter: Loss rate, delay time and jitter time between network nodes can be measured using ping tests unlimitedly and simultaneously. Measurement results are displayed and categorized into green, yellow, and red according to delay time. The delay time and jitter time are displayed graphically.

Below are the measurement results obtained when a ping plotter was installed into the test_PC and the network status from phone B to phone C was measured in the IPT network topology as shown in the figure above.



Summary - PingPlotter Pro

Graph focus time: 5 minutes

Sample Set Time: None

PL%	IP	DNSName	Count	Avg	Cur	Jttr
🟩	106.101.40.22	----------	300	1	1	0.89
🟩	106.101.40.21	----------	300	8	1	13.15

Trace Count: 6772 Displayed Samples: 6753 to 6772

Figure 2.9 Ping Plotter Test Results

2.8 IPT Service Deployment Example

In this section, we have listed the problems that occurred when deploying the Samsung IPT service in a real life example so that they can be used as a reference for future IPT service deployments.

2.8.1 German Samsung Corporation

- The IPT service was stopped because a broadcast storm occurred in the IPT service network.
- It was cleared by dividing the network into the IPT service network and IP data network logically.
- In more detail, because the versions of the workgroup switch (Sermit1, Extreme) and core switch (Black Diamond 6808, Extreme) images being used by the Unified German Corporation were early, we divided the network into the IPT service network and IP data network using VLAN. However, because the network was configured so that all STPs operated as a subnet, a broadcast storm on the IP data network flowed into the IPT service network. Therefore, we first separated logically the broadcast domain from the IP data network by removing the VLAN for IPT service from all STPs.
- The low S/W versions have now been completely upgraded to versions that can enable RSTP for each VLAN of all switches, and the RSTP is being enabled for each Per VLAN.

A time mismatch occurred due to a packet sending/receiving error between the SCM and NTP server.
This problem occurred because a private address for the SCM was blocked by the ACL (packet filter type) in the gateway switch. It was cleared by modifying the ACL.
The Internet access speed of a PC connected to the IP phone of a subscriber of SCG slowed down.
A large quantity of CRC errors occurred due to a fault in the cable between the workgroup switch and IP phone. The cable was replaced.
Measures were put in place so that the same action could be taken if a similar problem occurs in the future (when a Tx CRC error occurs in a workgroup switch).
This problem is related to a slowing down of the Internet connection speed; the speed and duplex options for the workgroup switch port connected to the IP phone should always be operated in auto negotiation mode.
The IP address received by a specific IP phone via DHCP conflicted.
This problem occurred because a user used an IP address in the DHCP pool as a static IP address. Measures were taken so that he could not use the static IP address.
To prevent similar problems from occurring during future operation, we strongly recommended that a notice should be sent to all employees and that this kind of problem be managed continually.

CHAPTER 3. License Guide

3.1 License Key Type

3.1.1 System

This describes the number of subscribers, generally thought of as users.

Licensed items are:
Samsung SIP Phones, Samsung Soft Phones, Samsung Mobile Phones, Samsung PC Attendants, 3rd Party SIP Phones, Analog Phones (Gateway)

3.1.2 Embedded Application

This describes the number of embedded application channels

Licensed items are:
Meet-Me Conference Channels, UMS Channels

3.1.3 External Application

This describes the number of external application channels

Licensed items are:
Total CSTA Applications, Communicator (Desktop), Other CSTA Applications, SIP Application Channels

3.1.4 Wireless Enterprise Future Feature

This describes the number of wireless service channel

License items are:
FMS Phones, MVS Phones

3.2 License Policy

3.2.1 Evaluation Period

If you didn't install the license, the evaluation license will work for 30 days.

3.2.2 Active-Active Validation (Future Feature)

If license is for active-active system and link down occur for 30 days continuously, the license will not work.

3.2.3 License Status Notification

If evaluation work or active-active system is link-down, the elapsed time will be notified at 9:00.
If the states of active-active system changed to normal, elapsed time will reset and be notified on time.
If evaluation license is expired, this information will be notified. But, if you already installed the license, system will work normally.

CHAPTER 4. Installing SCM Server

4.1 SCM Server Hardware

4.1.1 Preparing the SCM Hardware

The table below lists the minimum hardware requirements for installing the SCM.

Table 4.1 Minimum hardware requirements for SCM server

Category	SCM
CPU	2.4 GHz or higher (Quad Core, at least 1 CPU)
RAM	4 GB or more (DDR3, 1333 MHz or higher)
HDD	160 GB or more
ODD	1 DVD-ROM
Network Interface	3 Gigabit Ethernet

4.1.2 Unpacking and Inspection

To install the SCM software the server must meet the above the minimum requirements. SAMSUNG supplies the Dell's R210 model for SCM server. Samsung branded name is IPX-S500

For additional hardware installation of the IPX-S500, please refer to the 'IPX-S500 Hardware Owner's Manual'.

4.1.3 Preparing Peripherals

Following peripherals should be preparing for operating of SCM server. Preparing peripherals are different between stand alone system and twin system (high availability service system).

Table 4.2 Minimum peripherals for SCM server

Category	Stand Alone	Twin System
KVM (keyboard, video, mouse) switch (USB Type)	Not Need	1
Keyboard (USB type)	1	1
Mouse (USB type)	1	1
Monitor	1	1
L2 Switch	1 (Recommend 2)	2
UPS (Uninterruptible Power Supply)	Recommend	Recommend

4.1.4 Cabinet Mounting

NOTE

This section referenced on the Dell's R210 installation guide by Dell.

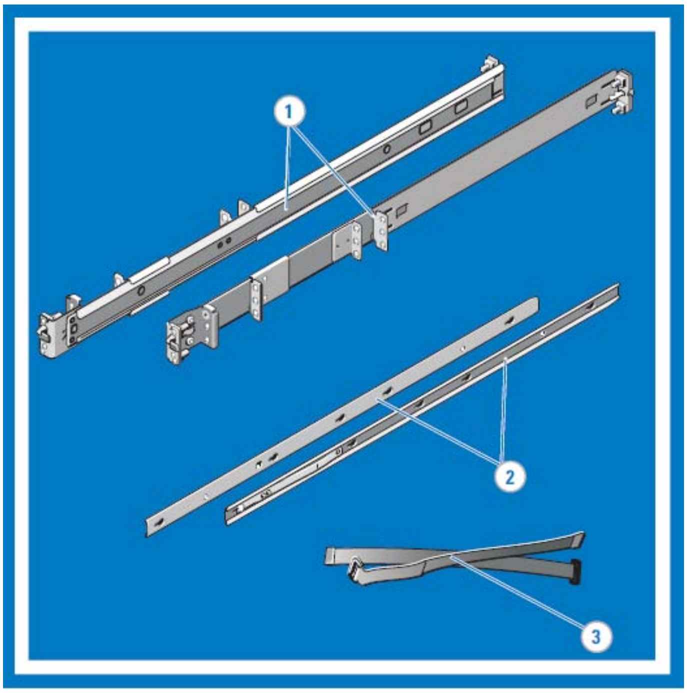
For additional information about installing to cabinet, see www.dell.com.

4.1.4.1 Installing with Static Rail

Identifying the Static Rail Kit Contents

Locate the components for installing the rail kit assembly:

- Two Dell™ ReadyRails™ static rails (1)
- Two chassis rail members (2)
- Two Velcro straps (3)

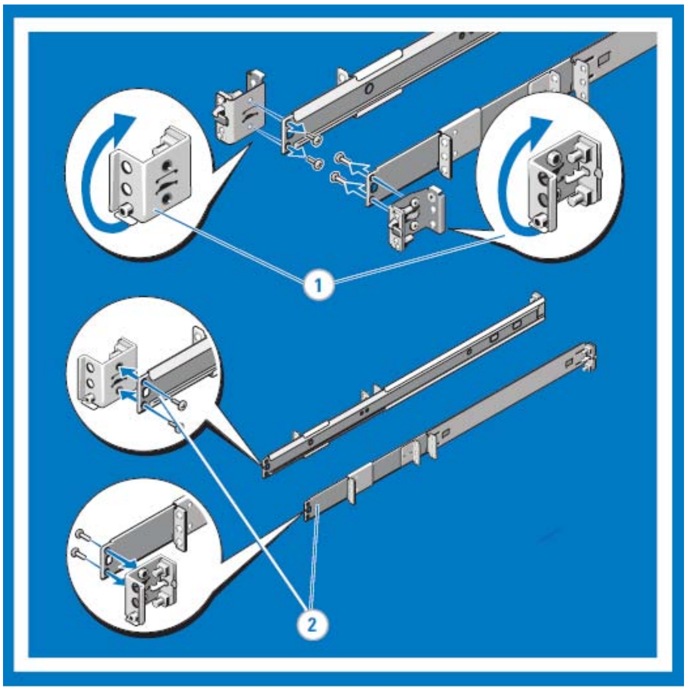


Configuring Flush-Mount Static Rails (Two- or Four-Post)

Lay both rails flat with both end pieces facing up. Remove the Remove the two screws on the front end pieces and rotate each piece 180 degrees (1). Reattach both end pieces with the two pairs of screws (2).

NOTE

The rails as they are shipped must be converted to tooled rails to install in a flush-mounted rack.

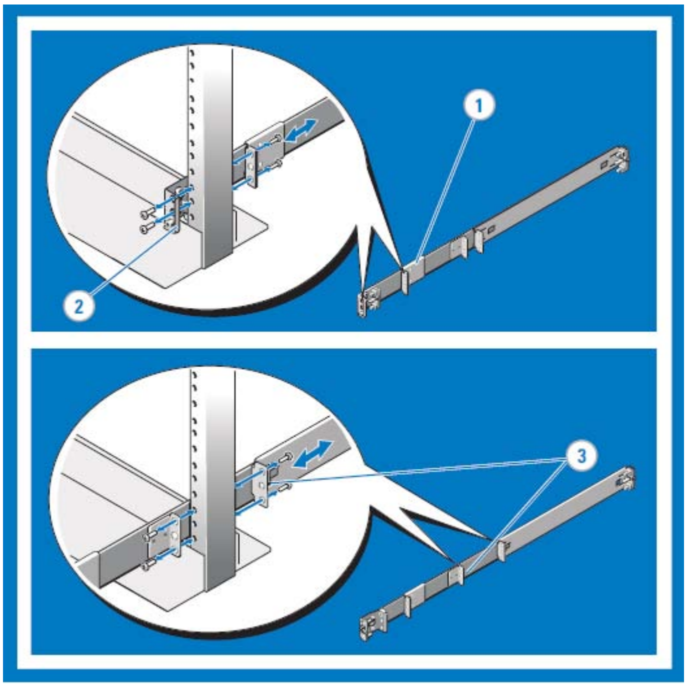


Installing Flush-Mount or Center-Mount Static Rails (Two-Post)

Attach right and left mounting rails to the front mounting flanges with two pairs of screws (1). Slide each flush-mount adjustable bracket forward against the two-post rack. Secure each side to the mounting flange with two pairs of screws (2). For a center-mount installation, push the adjustable rear mounting brackets toward the back of the right and left mounting rails. Attach the fixed center mount brackets to the front mounting flanges with two pairs of screws. Slide both the adjustable rear-mounting brackets forward against the two-post rack. Secure each side to the mounting flange with two screws (3).

NOTE

To configure your rails for a tooled flush-mount installation, refer to PANEL 3.

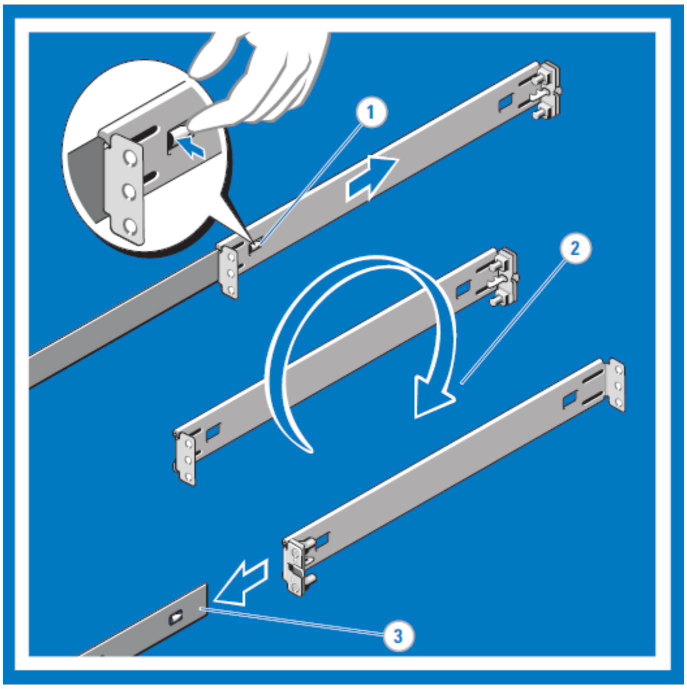

1
2
3

Configuring Four-Post Threaded Static Rails

Press the rail release button on each rail to disengage the rear segments (1). Rotate the rear segments 180 degrees so that the tooled end piece is in the rear position (2). With the end pieces positioned outward, align and rejoin the midsections and slide the rear segments into place until the release button engages (3).

NOTE

To configure the front end pieces of your rails for a tooled installation, refer to PANEL 3. To configure the rear end pieces of your rails for a tooled installation, perform the following steps.

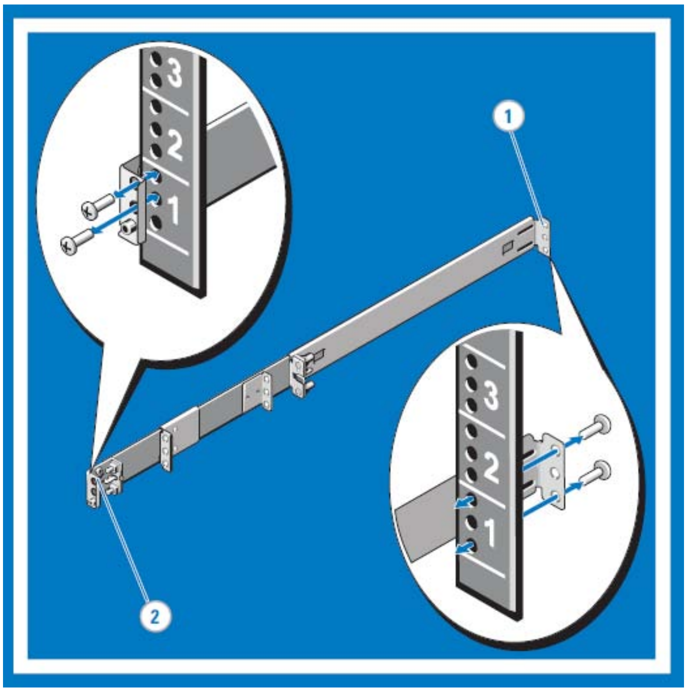


Installing and Removing Four-Post Threaded Static Rails

Attach the right and left mounting rails to the front mounting flanges with two pairs of screws (1). Repeat the preceding step for the rear mounting flanges (2).

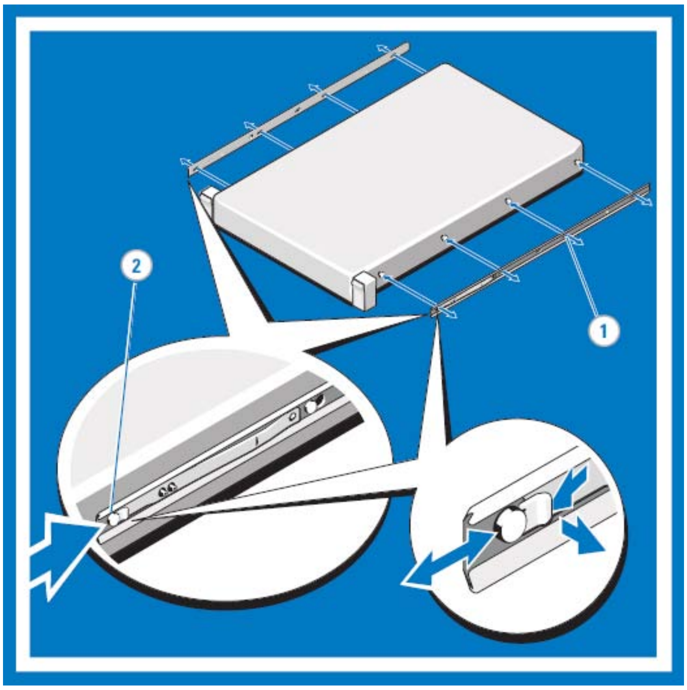
NOTE

To your rails for a tooled installation, refer to PANEL 3 and PANEL 5.



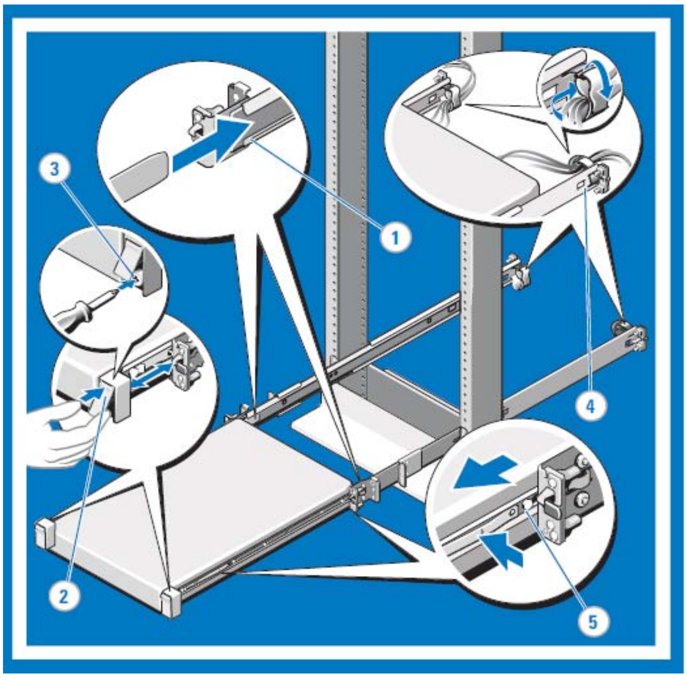
Installing and Removing Chassis Rail Members

Place the system on a level surface and align the keyhole slots on the chassis rail members with the pins on the system (1). Slide the chassis rail members toward the back of the system until they lock into place. To remove the chassis rail members, lift the lock spring until it clears the head of the pin (2). Slide the chassis rail member towards the front of the system until the pins slip through the keyhole slots.



Installing, Removing, Cabling, and Securing the System in the Rack

Insert the ends of the chassis rail members into the front of the static rails and push the system into the rack (1). For tool-less four-post racks and center-mount two-post configurations, the slam latches engage automatically as the system is pushed into the rack (2). To secure the system for shipment in the rack or for other unstable environments, locate and tighten the hard-mount screw under each latch (3). Bundle the system cables, pulling them clear of the system connectors to the left and right sides. Secure the bundles by threading the Velcro straps through the tooled rail slots (4). To remove the system from the rack, pull the system out of the rack until the rails lock into place. The lock position is intended to provide the opportunity to reposition the grip for removal, it is not intended for service. Locate the blue tabs on the sides of the chassis rail members. Push the tabs inward and continue pulling the system until the chassis rail members are completely clear of the rails (5).

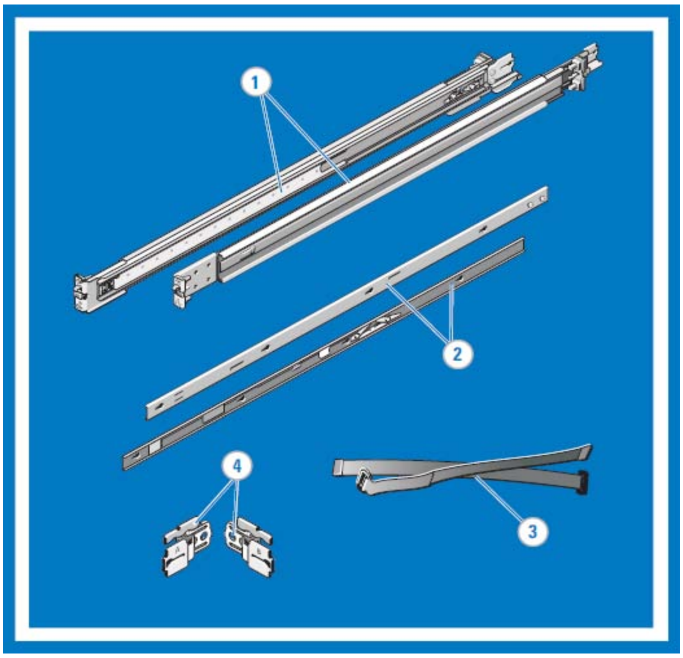


4.1.4.2 Installing with Sliding Rail

Identifying the Rail Kit Contents

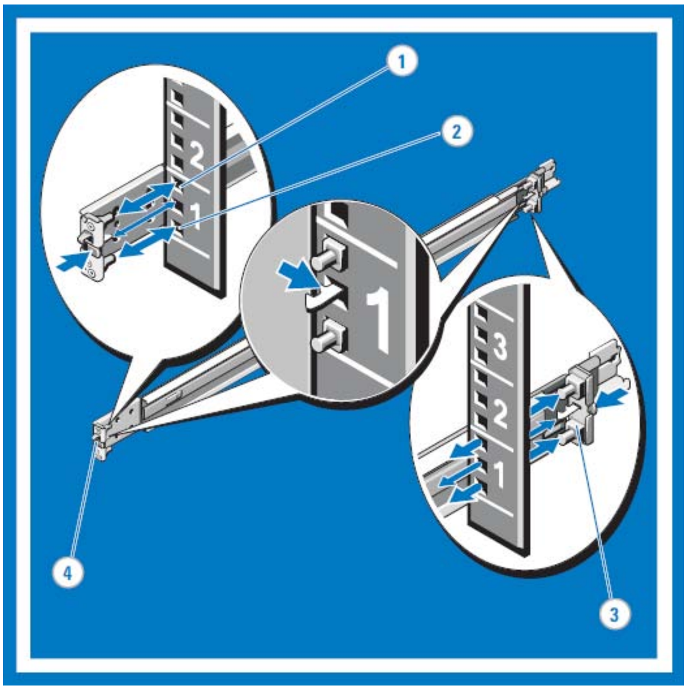
Locate the components for installing the rail kit assembly:

- Two A3 Dell™ ReadyRails™ sliding rails (1)
- Two chassis rail members (2)
- Two Velcro straps (3)
- Two cable management arm (CMA) attachment brackets (4)



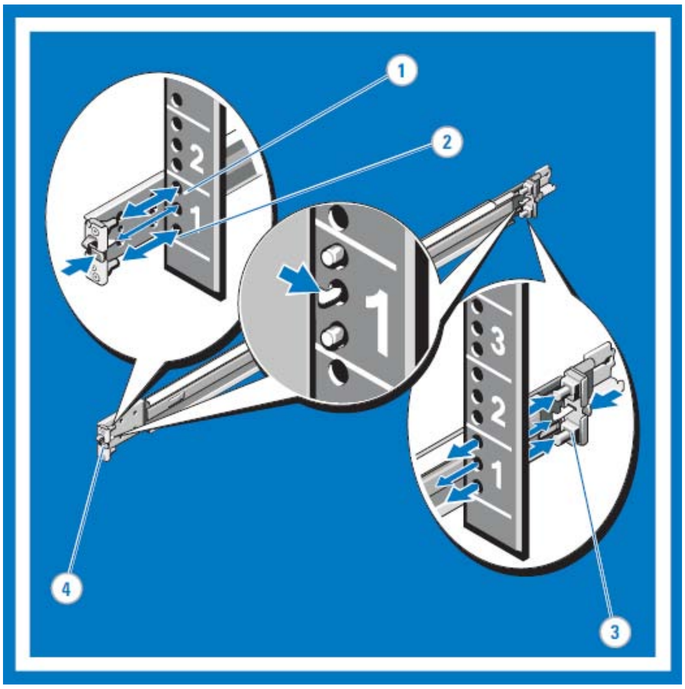
Installing and Removing the Rails (square-hole racks)

Position the left and right rail end pieces of the sliding rail labeled FRONT facing inward and orient each end piece to seat in the square holes on the front side of the vertical rack flanges (1). Align each end piece to seat the pegs in the bottom hole of the first U and the top hole of the first U (2). Engage the back end of the rail until it fully seats on the vertical rack flange and the second ‘tooth’ on the latch locks in place. Repeat these steps to position and seat the front end piece on the vertical flange (3). To remove the rails, pull on the latch release button on the end piece midpoint and unseat each rail (4).



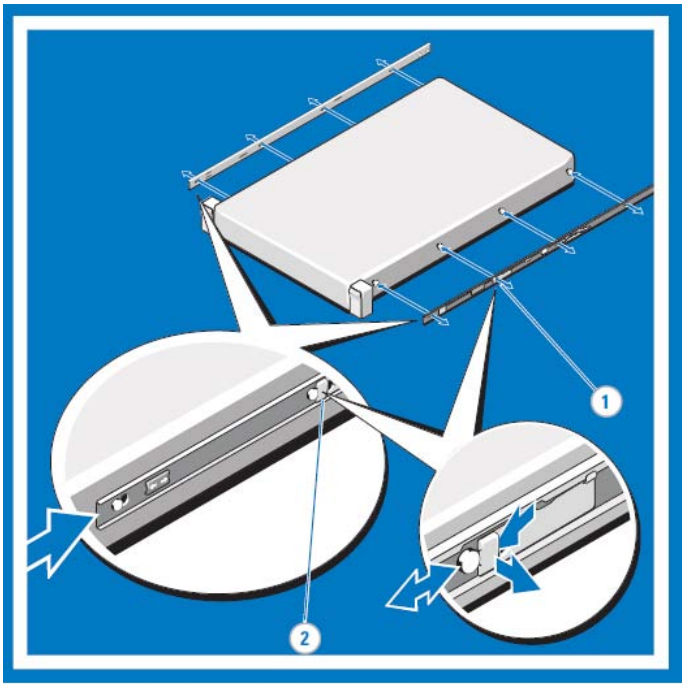
Installing and Removing the Rails (round-hole racks)

Position the left and right rail end pieces of the sliding rail labeled FRONT facing inward and orient each end piece to seat in the round holes on the front side of the vertical rack flanges (1). Align each end piece to seat the pegs in the bottom hole of the first U and the top hole of the first U (2). Engage the back end of the rail until it fully seats on the vertical rack flange and the first ‘tooth’ on the latch locks in place. Repeat these steps to position and seat the front end piece on the vertical flange (3). To remove the rails, pull on the latch release button on the end piece midpoint and unseat each rail (4).



Installing and Removing the Chassis Rail Members

Place the system on a level surface and align the four keyhole slots on the chassis rail members with the corresponding pins on the system (1). Slide the chassis rail members towards the back of the system until each one locks into place. To remove the chassis rail members, lift the lock spring until it clears the head of the pin (2). Slide the chassis rail member toward the front of the system until the pins slip through the keyhole slots.

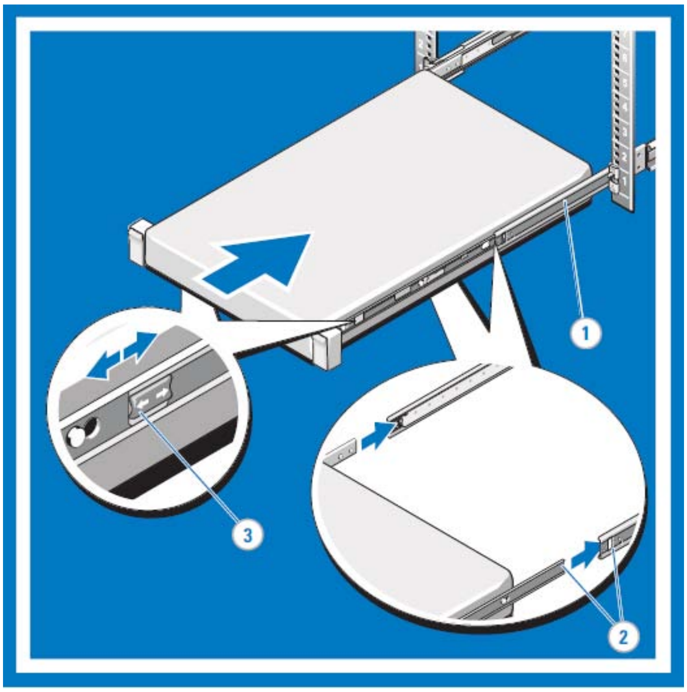


Installing the System in the Rack

Pull the sliding rails out of the rack until they lock into place (1). Align and insert the ends of the chassis rail members into the ends of the rails (2). Push the system inward until the chassis rail members lock into place. Push or pull the blue tab located near the front of the system and slide the system into the rack (3).

NOTE

Ensure that the system is properly supported until the chassis rail members are locked into the slide rails on both sides.

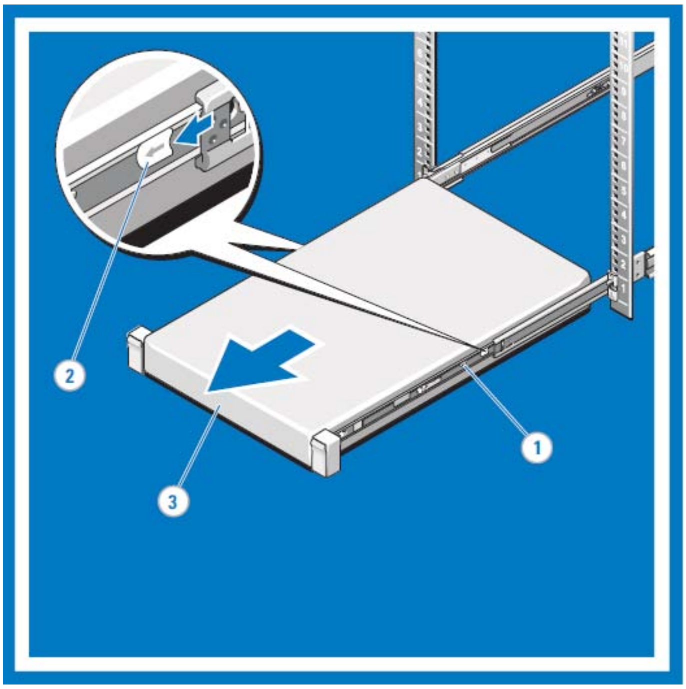


Removing the System from the Rack

Pull the system out of the rack until the sliding rails lock into place (1). Locate the white tabs on the sides of the chassis rail members (2). Pull the tabs towards the front of the system to release the chassis rail members from the rails. Continue pulling the system until the chassis rail members are completely clear of the rails and place the system on a level surface (3).

NOTE

To remove the chassis rail members from the system, refer to PANEL 4.

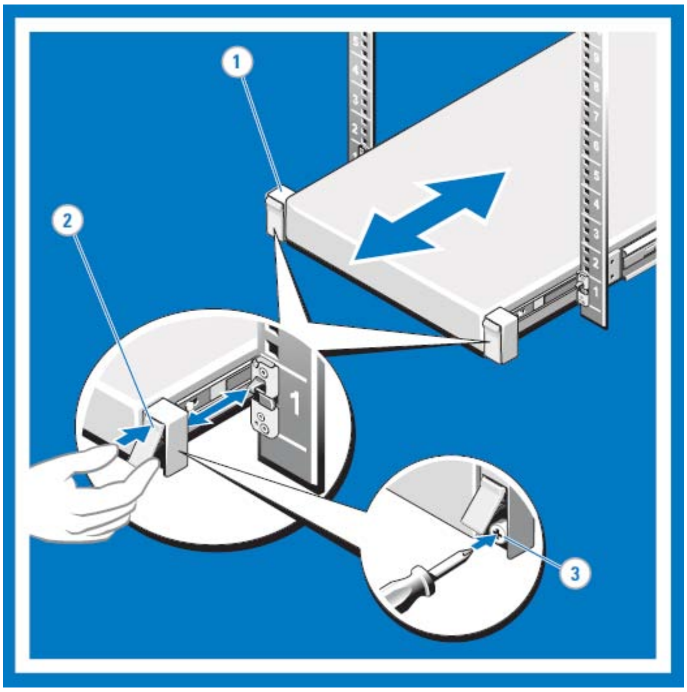


Engaging and Releasing the Slam Latch

Facing the front, locate the slam latch on either side of the system (1). The latches engage automatically as the system is pushed into the rack and are released by pulling up on the latches (2). To secure the system for shipment in the rack or for other unstable environments, locate the hard-mount screw under each latch and tighten each screw with a #2 Phillips screwdriver (3).

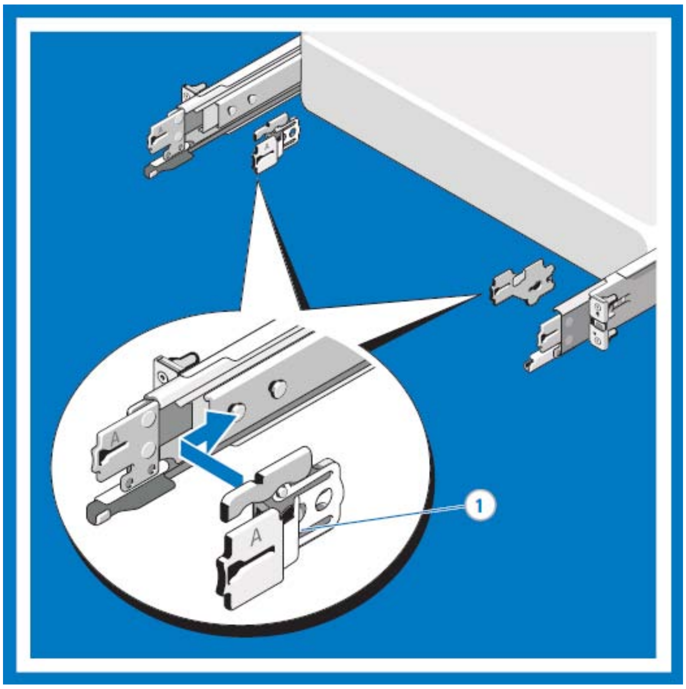
NOTE

For systems not equipped with slam latches, you can secure the system using screws, as described in Step 3.



Installing the CMA Attachment Brackets

Locate the CMA attachment bracket marked A and install it at the back of the slide rail marked with a corresponding A (1). Align the holes on the bracket with the pins on the slide rail and push the bracket forward until it locks into place. Repeat the same process for the CMA attachment bracket marked B.

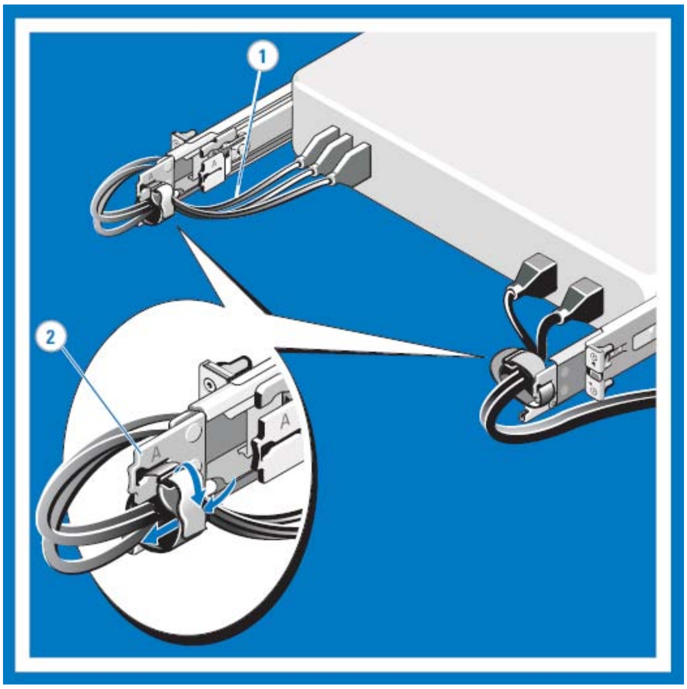


4.1.4.3 Routing the Cables

Bundle the cables gently, pulling them clear of the system connectors to the left and the right sides (1). Thread the Velcro straps through the tooled slots on the outer or inner CMA brackets on each side of the system to secure the cable bundles (2).

NOTE

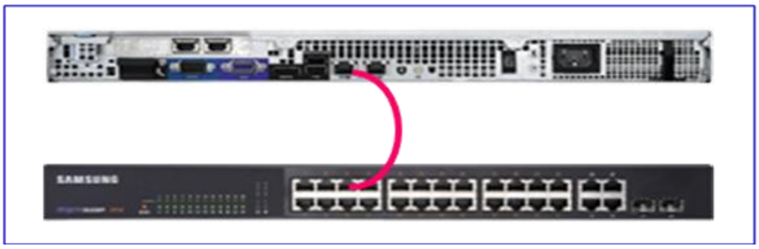
If you did not order the optional CMA, use the two Velcro straps provided in the rail kit to help route the cables at the back of your system. To allow proper fit in racks that do not accommodate the CMA, the outer CMA brackets can be removed using a #2 Phillips screwdriver.



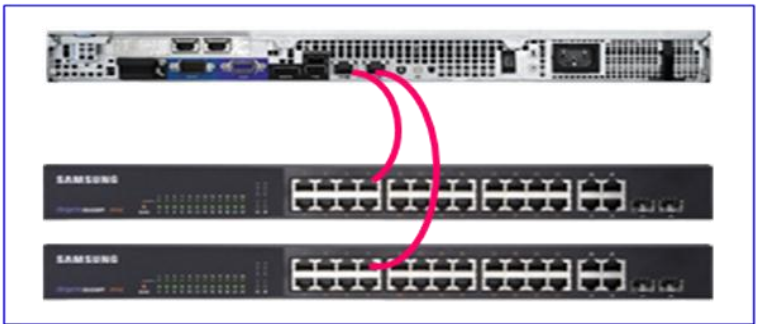
4.1.5 Connecting to Network

Stand Alone SCM

Following figure is connecting to IP network diagram for Stand Alone SCM without network redundancy.

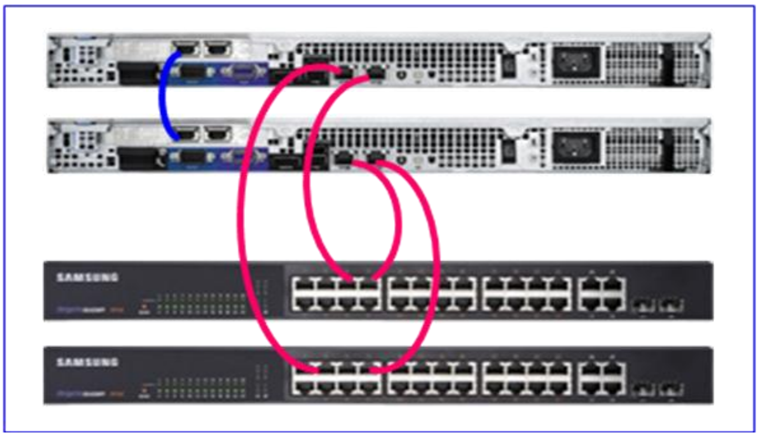


Following figure is connecting to IP network diagram for Stand Alone SCM with network redundancy.
When using network redundancy, the SCM network cables should be connecting to different switches.



High Availability Service SCM

Following figure is connecting to IP network diagram for High Availability service SCM with network redundancy.



When SCM using High Availability service, should be used network redundancy. The SCM network cables should be connecting to different switches.
The network cable of connecting between active and standby SCM, should be used Category E5 or more.

4.2 SCM Server Software

4.2.1 Preparing the SCM Software

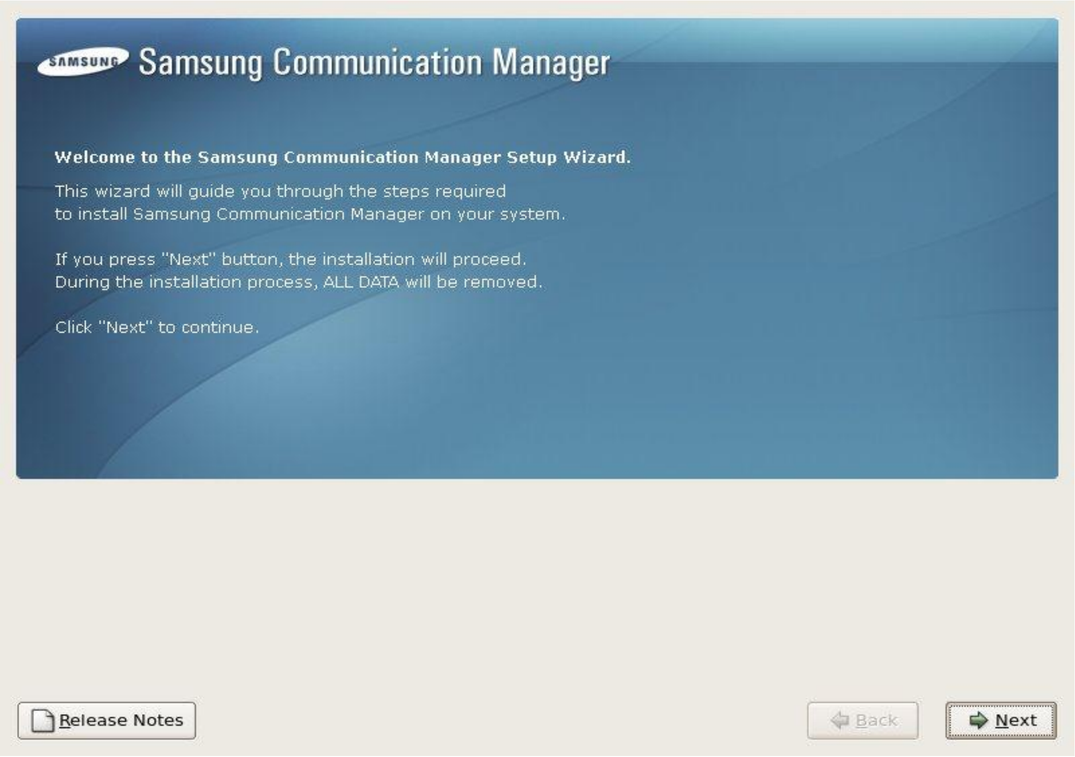
The IPX-S500 server comes with the SCM software and Linux OS already installed.

However if you need to reinstall the SCM application contact Technical Support for a copy of the software.

To reinstall the SCM software, the installation DVD is required. It does not require the Linux operating system to be reinstalled. You need to install the SCM software on the device with a valid software license.

4.2.2 SCM Software Installation Procedure

To install the SCM:
Insert the installation DVD into your DVD-ROM drive and run the setup program.



Samsung Communication Manager

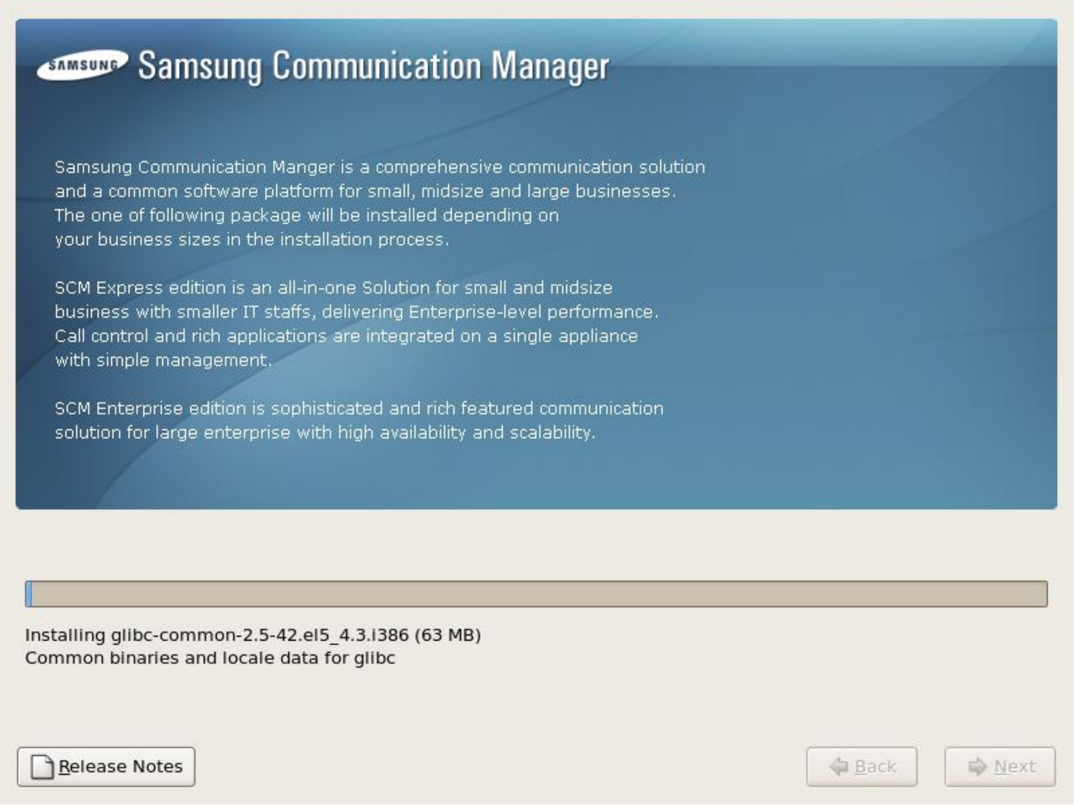
Welcome to the Samsung Communication Manager Setup Wizard.

This wizard will guide you through the steps required
to install Samsung Communication Manager on your system.

If you press "Next" button, the installation will proceed.
During the installation process, ALL DATA will be removed.

Click "Next" to continue.

Click the **Next** button to start the installation.



Samsung Communication Manger is a comprehensive communication solution
and a common software platform for small, midsize and large businesses.
The one of following package will be installed depending on
your business sizes in the installation process.

SCM Express edition is an all-in-one Solution for small and midsize
business with smaller IT staffs, delivering Enterprise-level performance.
Call control and rich applications are integrated on a single appliance
with simple management.

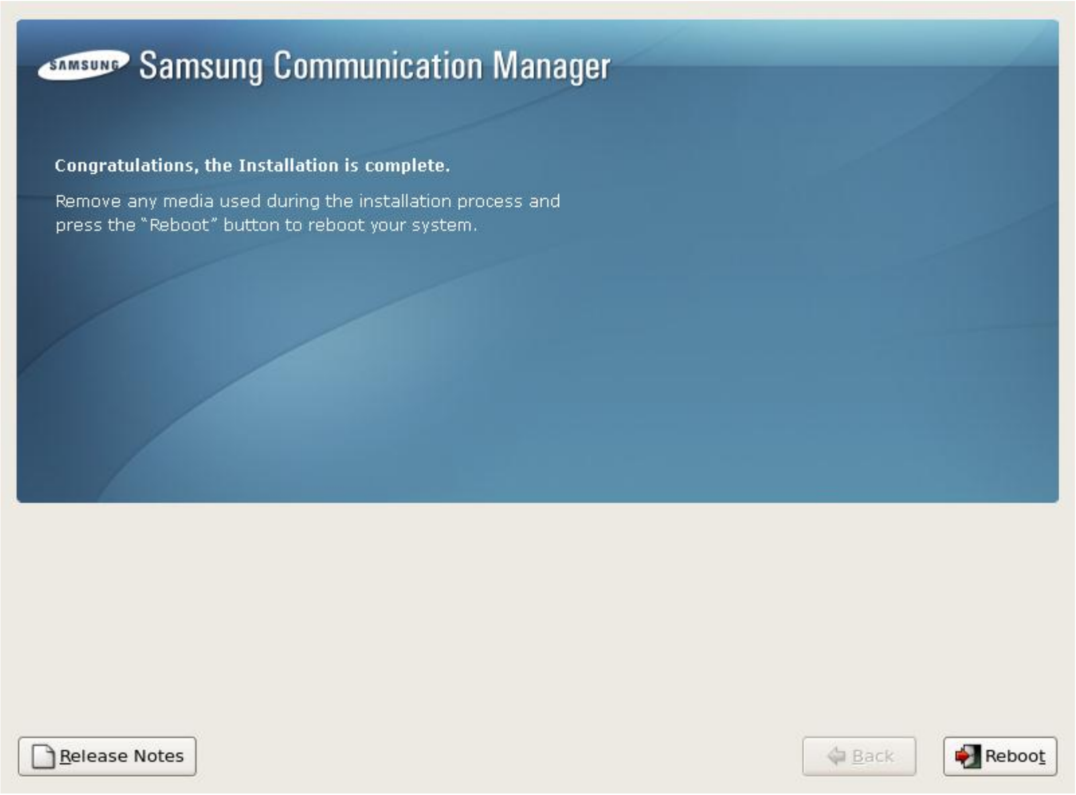
SCM Enterprise edition is sophisticated and rich featured communication
solution for large enterprise with high availability and scalability.

Installing glibc-common-2.5-42.el5_4.3.i386 (63 MB)
Common binaries and locale data for glibc

CAUTION

All the data stored in the HDD will be deleted when installing the SCM software.

When the installation is complete, eject the DVD and click the **Reboot** button to restart your computer.



Congratulations, the Installation is complete.

Remove any media used during the installation process and press the "Reboot" button to reboot your system.

The following directories are created under the /DI directory after installing the SCM.

- BASE: Base components
- CM: The components related to the SIP and the supplementary services
- etc: The shell scripts and other utilities for supporting installation
- HA: The components for redundancy processing
- MP: The components for announcement and mixing processing
- WEBCLI: The components for operation management

After rebooting, should be configured following 3.3 or 3.4 section.

4.3 Configuring Stand Alone Server

After the installation, if you log in with the default administrator account (ID: admin, Password: samsung*#), the setup wizard runs automatically.
The configuration procedure consists of the following steps in sequential order:

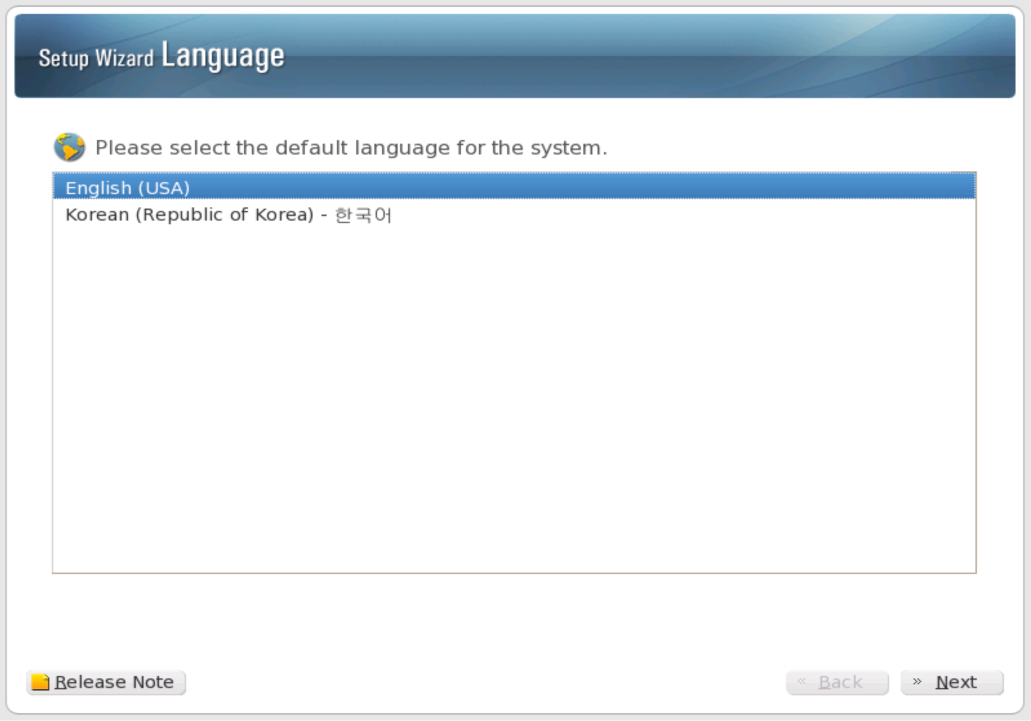
- Server Basic Configuration
  - Language setting
  - Keyboard setting
  - Time zone setting
  - Date and time setting
- SCM Software Configuration
  - Database setting
  - IP address setting

4.3.1 Server Basic Configuration

Configure language, keyboard, time zone, and date & time.

4.3.1.1 Language Setting

Select the language to use.



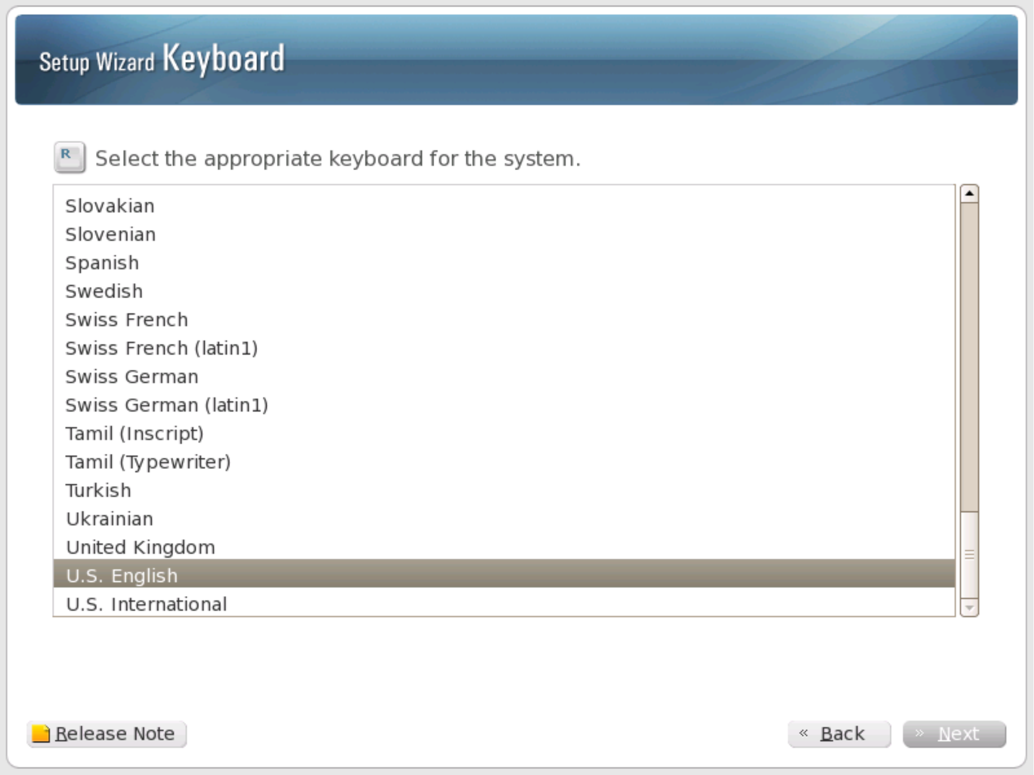
Setup Wizard Language

Please select the default language for the system.

English (USA)
Korean (Republic of Korea) - 한국어

4.3.1.2 Keyboard Setting

Select the keyboard to use.

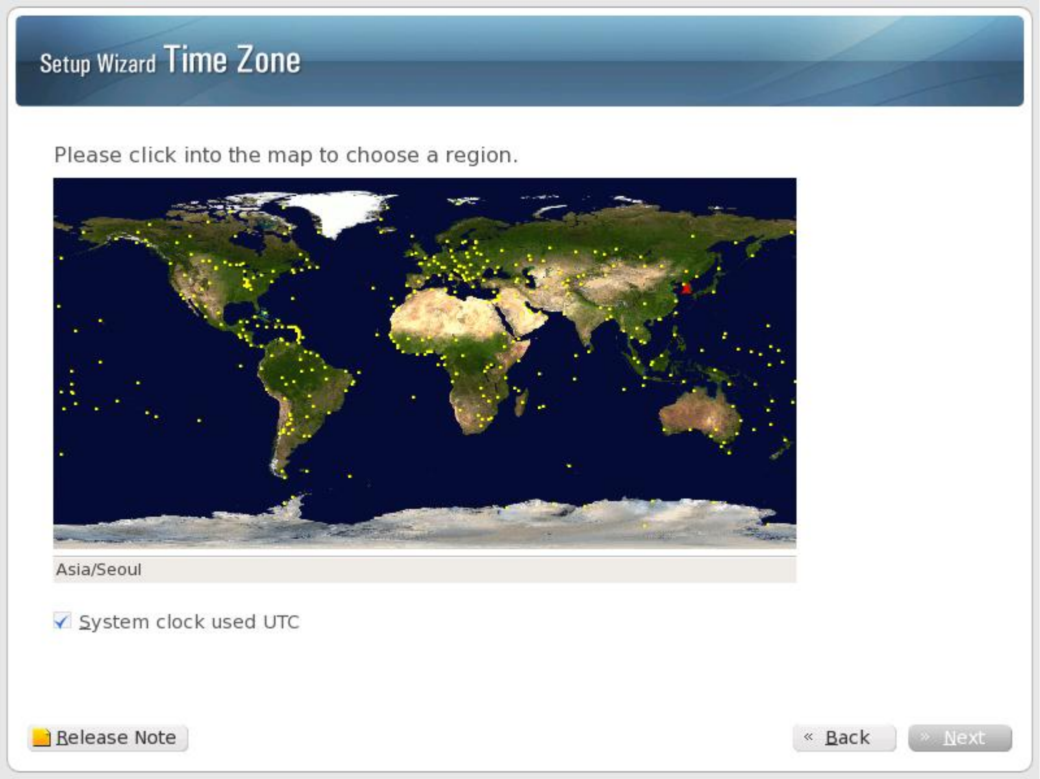


Select the appropriate keyboard for the system.

Slovakian
Slovenian
Spanish
Swedish
Swiss French
Swiss French (latin1)
Swiss German
Swiss German (latin1)
Tamil (Inscript)
Tamil (Typewriter)
Turkish
Ukrainian
United Kingdom
U.S. English
U.S. International

4.3.1.3 Time Zone Setting

Select the time zone where you are located.



Setup Wizard Time Zone

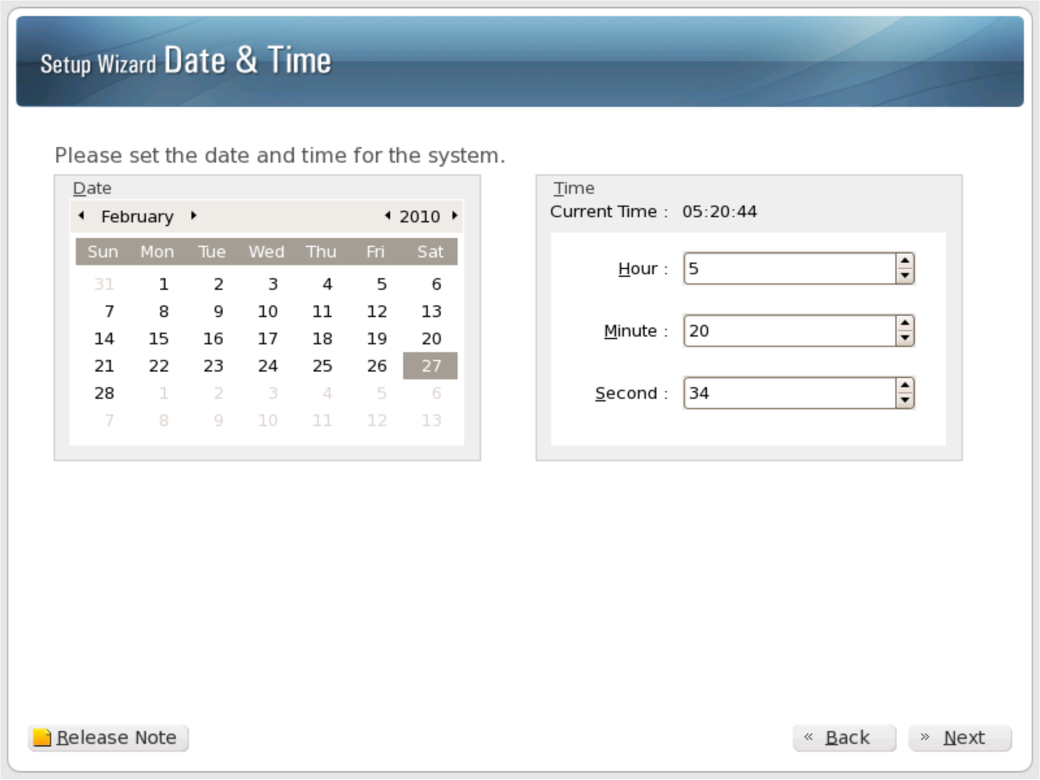
Please click into the map to choose a region.

Asia/Seoul

☑ System clock used UTC

4.3.1.4 Date and Time Setting

Set the date and time.



Setup Wizard Date & Time

Please set the date and time for the system.

Date

February 2010

Sun	Mon	Tue	Wed	Thu	Fri	Sat
31	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	1	2	3	4	5	6
7	8	9	10	11	12	13

Time

Current Time : 05:20:44

Hour : 5

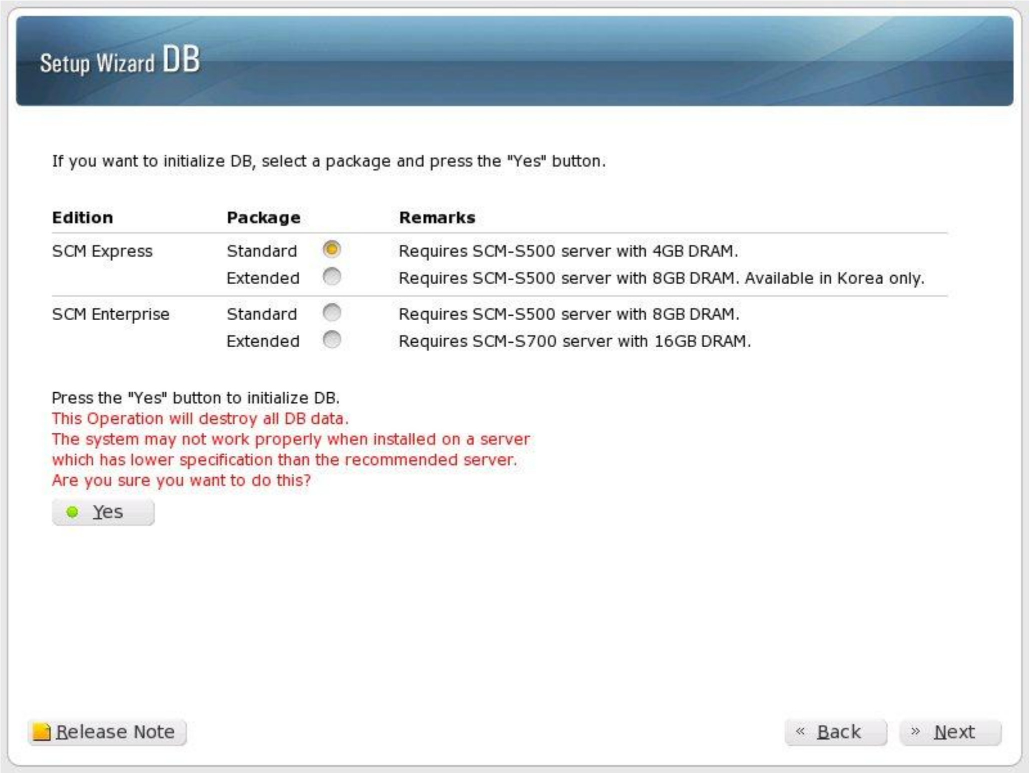
Minute : 20

Second : 34

4.3.2 SCM Software Configuration

Configure the database and IP addresses for the SCM Software.

4.3.2.1 Database Setting



If you want to initialize DB, select a package and press the "Yes" button.

Edition	Package		Remarks
SCM Express	Standard	●	Requires SCM-S500 server with 4GB DRAM.
	Extended	○	Requires SCM-S500 server with 8GB DRAM. Available in Korea only.
SCM Enterprise	Standard	○	Requires SCM-S500 server with 8GB DRAM.
	Extended	○	Requires SCM-S700 server with 16GB DRAM.

Press the "Yes" button to initialize DB.
This Operation will destroy all DB data.
The system may not work properly when installed on a server which has lower specification than the recommended server.
Are you sure you want to do this?

- **In North America always select SCM Express - Standard**

NOTE

If you select the edition not appropriate to your license, the system does not operate.

- Select the country to use. (The system capacity changes depending on the selected country.)
- Click the Yes button to initialize the database.

CAUTION

All the existing data will be deleted when initializing the database.

4.3.2.2 IP Address Setting

To set the IP addresses, you must have the ones assigned by the network administrator.

NOTE

Before the installation of the SCM, the correct network address must be assigned by the network administrator, and each port (eth0, eth1, and eth2) must be ready to connect to the LAN.

The table below lists the number of IP addresses that need to be assigned on the standalone system configuration.

Category	Need IP Address
Data Link IP	2
System IP	1
Heartbeat IP	None
Component IP	None

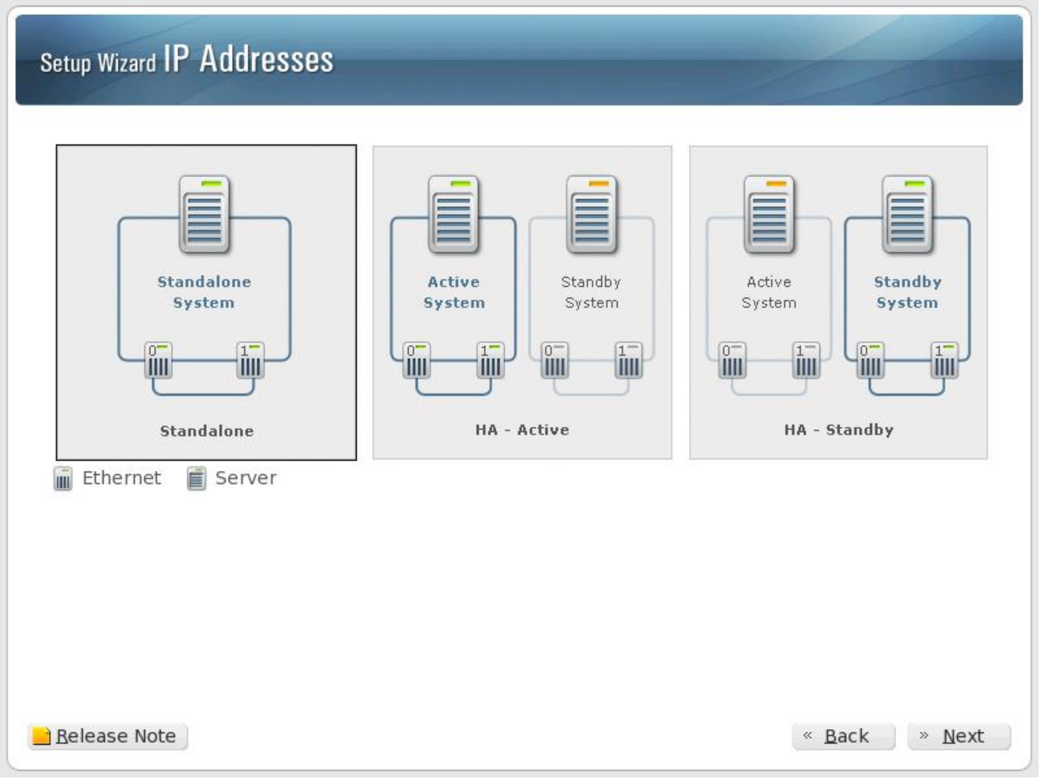
CAUTION

When assigning IP addresses to configure the system, their subnet addresses should be set carefully.

- For the data link IP addresses (eth0, eth1), their subnet addresses must be identical.
- For the data link IP addresses of the active and standby systems, their subnet addresses must be also identical.
- For the system IP addresses of the active and standby systems, their subnet addresses must be identical.
- For the heartbeat IP addresses of the active and standby systems, their subnet addresses must be identical.
- For the data link IP address, system IP address, and heartbeat IP address, their subnet addresses must be different from each other.

4.3.2.3 Selecting the Installation Mode

Select the SCM installation mode appropriate for your system configuration. You can select either a standalone or high availability (HA-Active, HA-Standby) configuration.

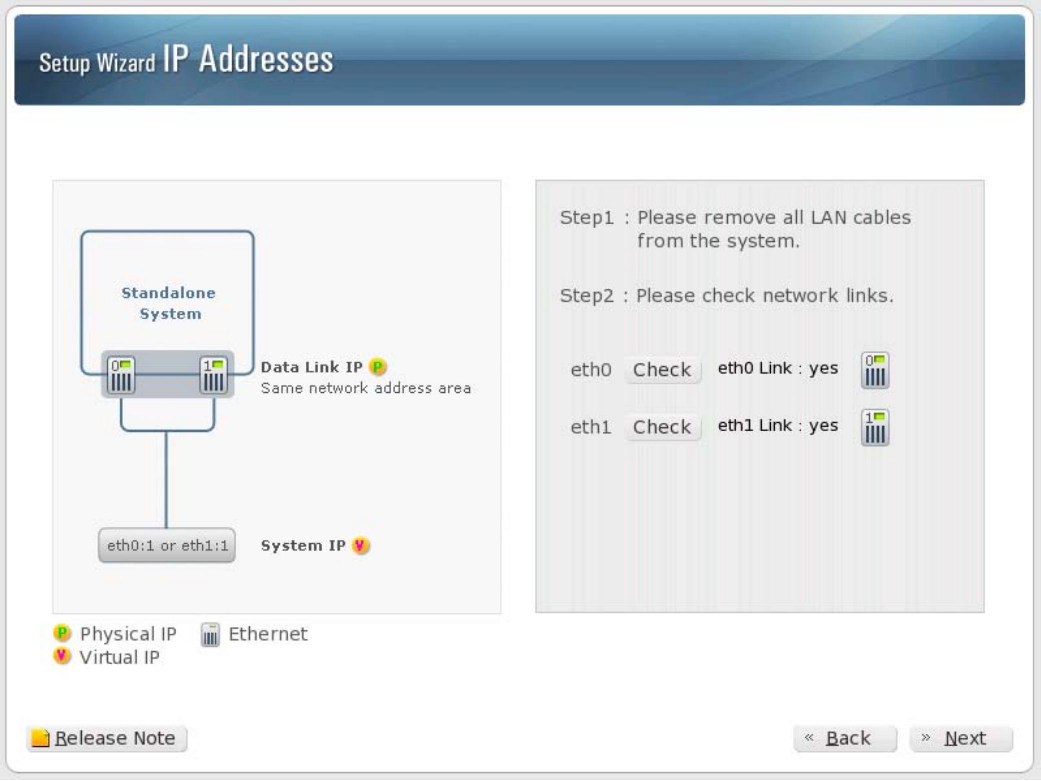


NOTE

If you select the edition not appropriate to your license, the system does not operate.

4.3.2.4 Checking the LAN Ports

Remove all LAN cables from the system. Then connect one at a time and click the **Check** button. Through this process, you can identify port connections for the LAN cards.



Step1 : Please remove all LAN cables from the system.

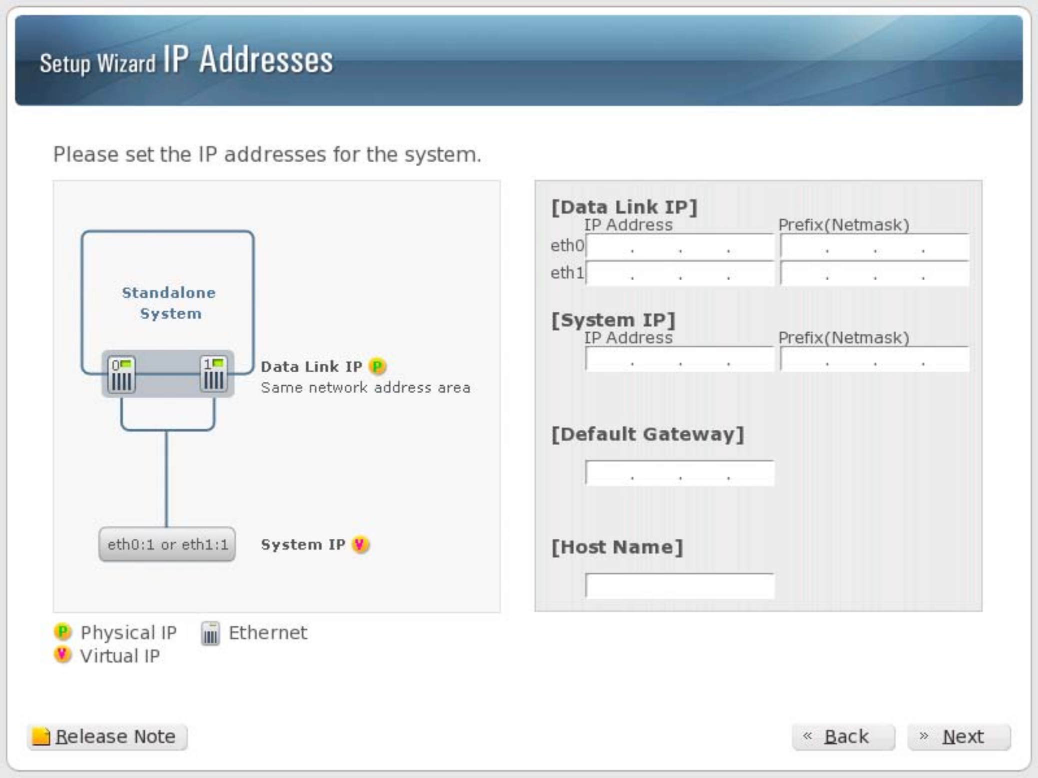
Step2 : Please check network links.

eth0 Check eth0 Link : yes

eth1 Check eth1 Link : yes

4.3.2.5 Entering IP Addresses

Enter the network information for your system configuration.

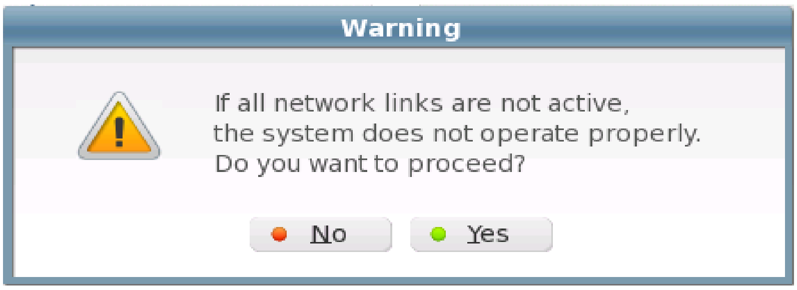


Please set the IP addresses for the system.

Item	Description
Data Link IP	- eth0: Enter the IP address of eth0. - eth1: Enter the IP address of eth1. - Netmask: Enter ‘255.255.255.0’. The subnet addresses of eth0 and eth1 must be identical.
System IP	- IP Address: Enter the IP address that the SCM will use. - Netmask: Enter the netmask that the SCM will use.
Default Gateway	Enter the gateway address.
Host Name	Enter the host name of the SCM.

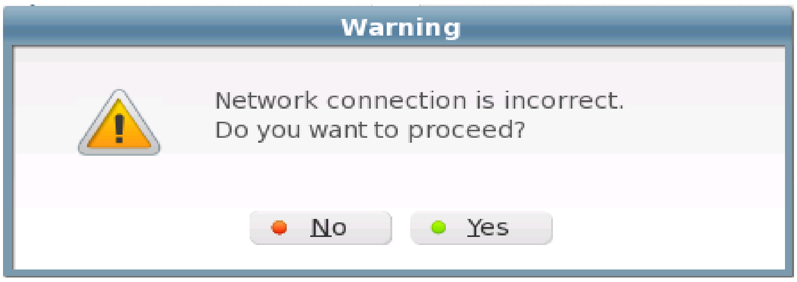
CHECK

- If you install the SCM without checking the LAN ports, an error may occur when operating the system. Make sure to check the LAN ports and then proceed to the installation.



If all network links are not active,
the system does not operate properly.
Do you want to proceed?

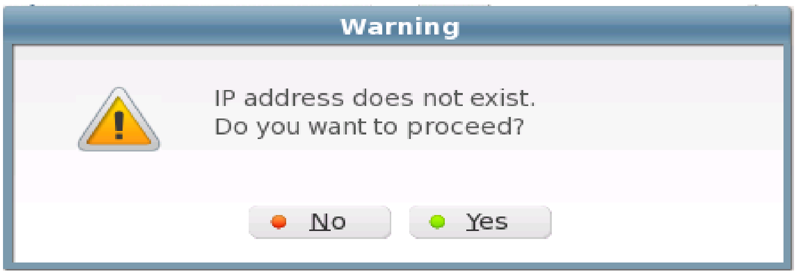
- If you install the SCM when there is an error in the LAN port, the warning message appears as shown below. Correct the port error and then proceed to the next step.



Network connection is incorrect.
Do you want to proceed?

NOTE

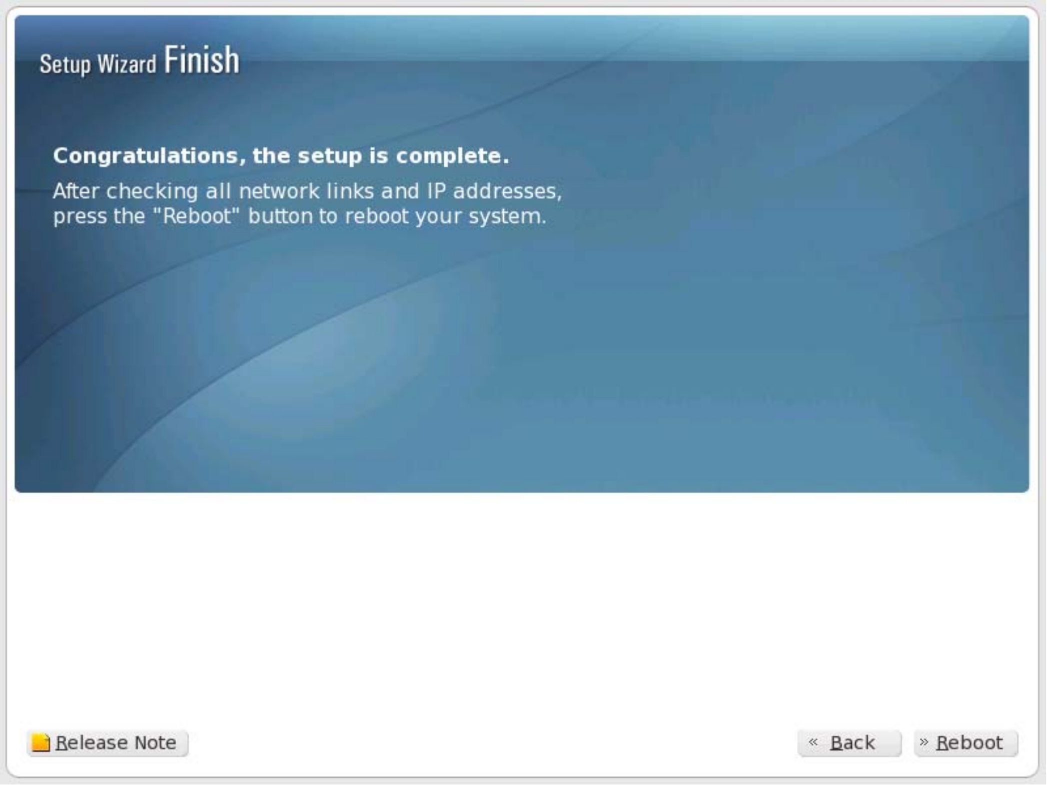
If the network information is not provided, the warning message appears as shown in the figure below. If the network information is configured incorrectly, the system may not operate properly.



IP address does not exist.
Do you want to proceed?

4.3.2.6 Finishing the Configuration

When the configuration is completed, click the **Reboot** button to restart your computer. If a configuration value is incorrect, you can click the **Back** button to correct it.



Setup Wizard Finish

Congratulations, the setup is complete.

After checking all network links and IP addresses, press the "Reboot" button to reboot your system.

4.4 Configuring High Availability Service

After the installation, if you log in with the initial administrator account (ID: admin, Password: samsung*#), the setup wizard runs automatically.
The configuration procedure consists of the following steps in sequential order:

- Server Basic Configuration
  - Language setting
  - Keyboard setting
  - Time zone setting
  - Date and time setting
- SCM Software Configuration
  - Database setting
  - IP address setting

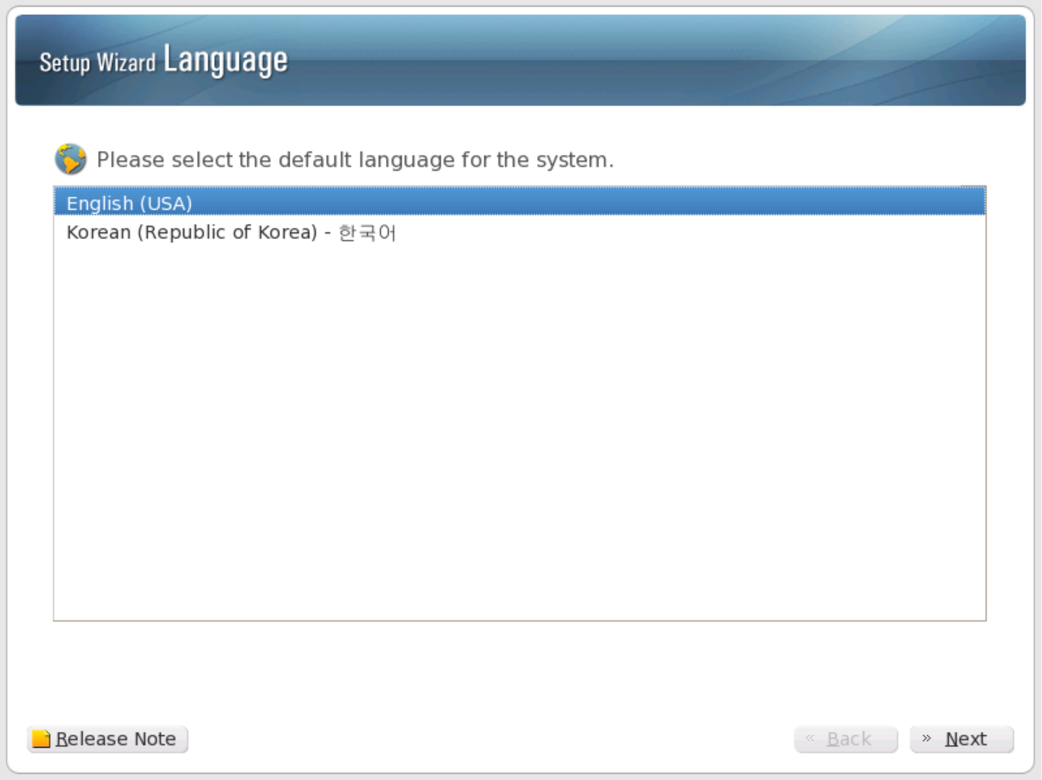
In case of High Availability Service System, each Active system and Standby system will be configure following above courses.

4.4.1 Server Basic Configuration

Configure language, keyboard, time zone, and date & time.

4.4.1.1 Language Setting

Select the language to use.



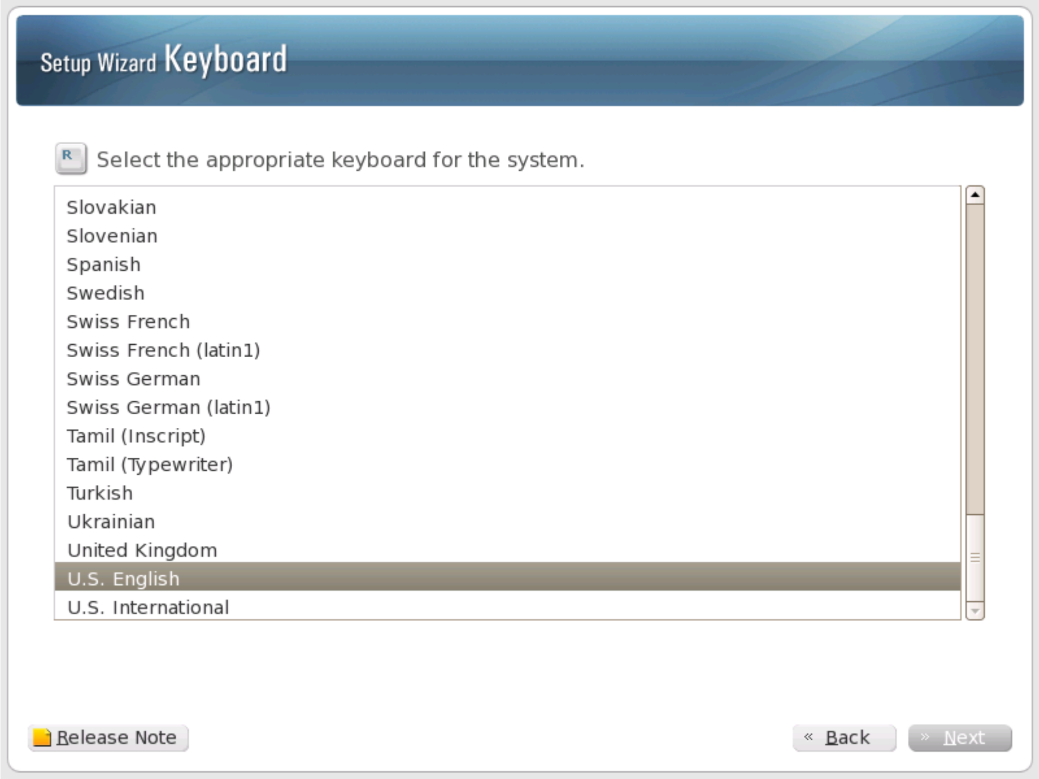
Setup Wizard Language

Please select the default language for the system.

English (USA)
Korean (Republic of Korea) - 한국어

4.4.1.2 Keyboard Setting

Select the keyboard to use.

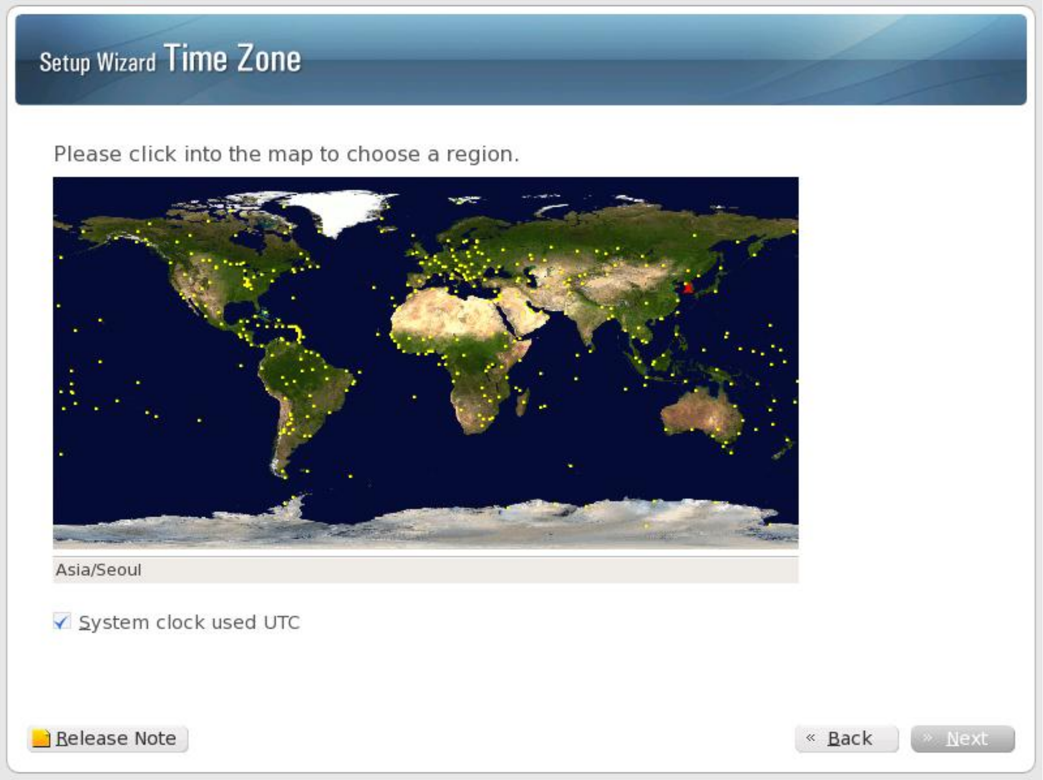


Select the appropriate keyboard for the system.

- Slovakian
- Slovenian
- Spanish
- Swedish
- Swiss French
- Swiss French (latin1)
- Swiss German
- Swiss German (latin1)
- Tamil (Inscript)
- Tamil (Typewriter)
- Turkish
- Ukrainian
- United Kingdom
- U.S. English
- U.S. International

4.4.1.3 Time Zone Setting

Select the time zone where you are located.



Setup Wizard Time Zone

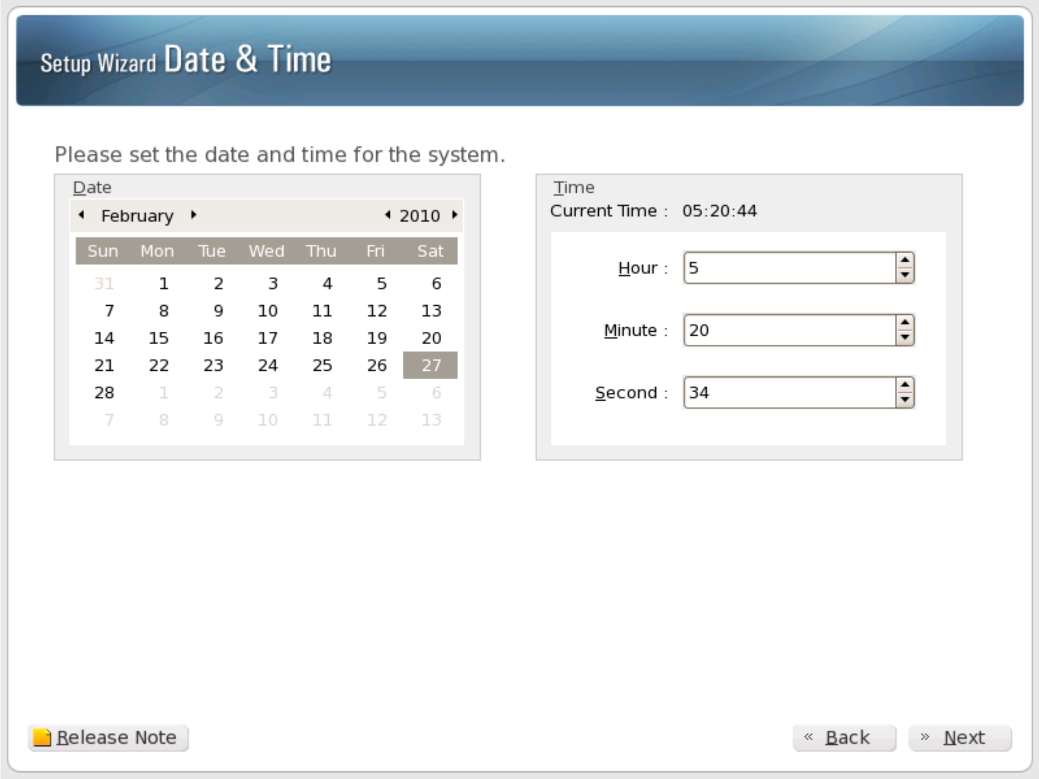
Please click into the map to choose a region.

Asia/Seoul

☑ System clock used UTC

4.4.1.4 Date and Time Setting

Set the date and time.



Please set the date and time for the system.

Date

◂ February ▸ ◂ 2010 ▸

Sun	Mon	Tue	Wed	Thu	Fri	Sat
31	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	1	2	3	4	5	6
7	8	9	10	11	12	13

Time

Current Time : 05:20:44

Hour : 5

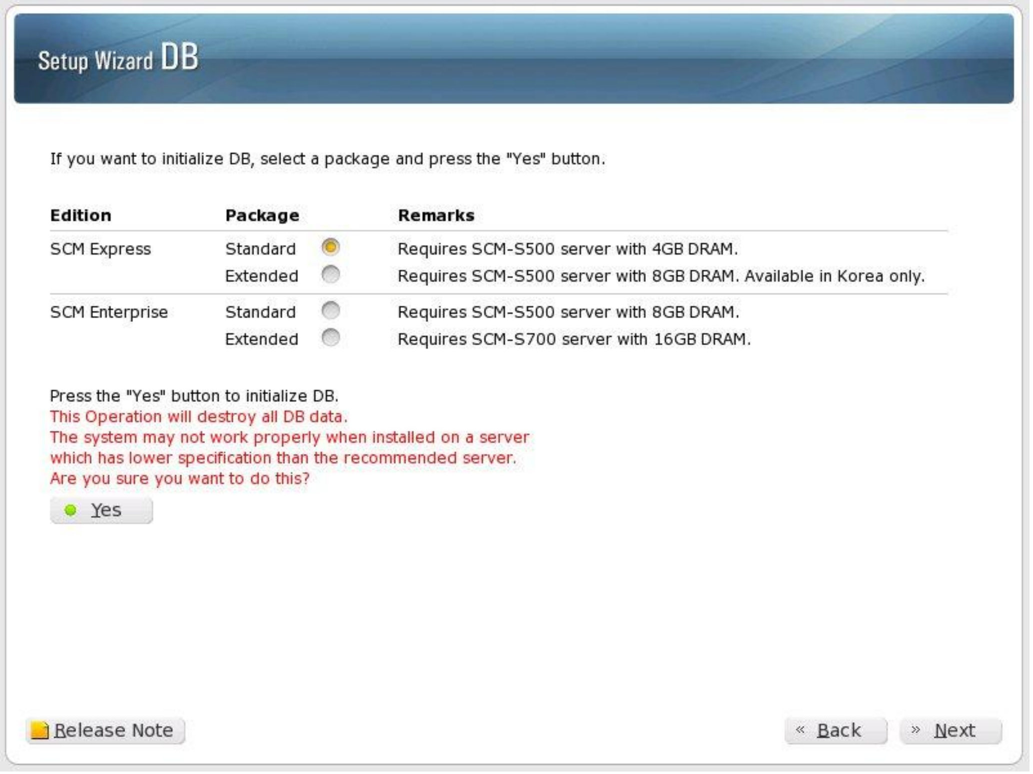
Minute : 20

Second : 34

4.4.2 SCM Software Configuration

Configure the database and IP addresses for the SCM Software.

4.4.2.1 Database Setting



If you want to initialize DB, select a package and press the "Yes" button.

Edition	Package		Remarks
SCM Express	Standard	●	Requires SCM-S500 server with 4GB DRAM.
	Extended	○	Requires SCM-S500 server with 8GB DRAM. Available in Korea only.
SCM Enterprise	Standard	○	Requires SCM-S500 server with 8GB DRAM.
	Extended	○	Requires SCM-S700 server with 16GB DRAM.

Press the "Yes" button to initialize DB.
This Operation will destroy all DB data.
The system may not work properly when installed on a server
which has lower specification than the recommended server.
Are you sure you want to do this?

- 1) **In North America always select SCM Express - Standard**

NOTE

If you select the edition not appropriate to your license, the system does not operate.

2) Select the country to use. (The system capacity changes depending on the selected country.)

3) Click the Yes button to initialize the database.

CAUTION

All the existing data will be deleted when initializing the database.

4.4.2.2 IP Address Setting

To set the IP addresses, you must have the ones assigned by the network administrator.

NOTE

Before the installation of the SCM, the correct network address must be assigned by the network administrator, and each port (eth0, eth1, and eth2) must be ready to connect to the LAN.

The table below lists the number of IP addresses that need to be assigned on the high availability system configuration.

Category	High Availability (HA)	
	Active	Standby
Data Link IP	2	2
System IP	1	1
Heartbeat IP	1	1
Component IP	1	

CAUTION

When assigning IP addresses to configure the system, their subnet addresses should be set carefully.

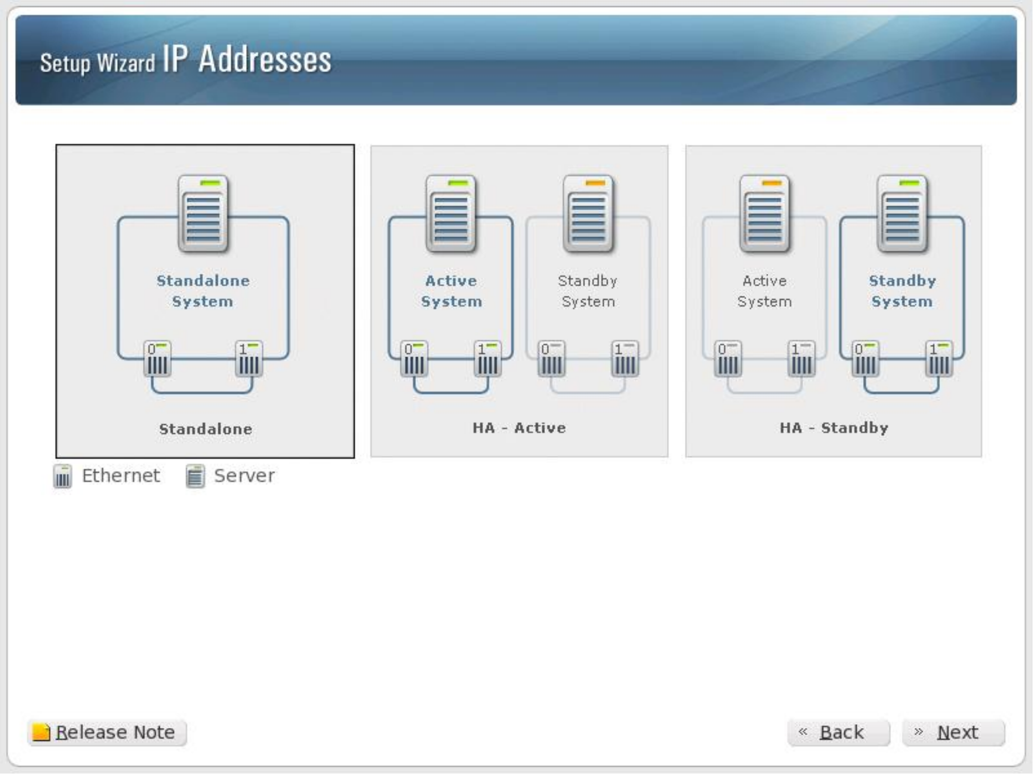
- For the data link IP addresses (eth0, eth1), their subnet addresses must be identical.

  For the data link IP addresses of the active and standby systems, their subnet addresses must be also identical.
- For the system IP addresses of the active and standby systems, their subnet addresses must be identical.
- For the heartbeat IP addresses of the active and standby systems, their subnet addresses must be identical.
- For the data link IP address, system IP address, and heartbeat IP address, their subnet addresses must be different from each other.

4.4.3 Configuring HA-Active Server

4.4.3.1 Selecting the Installation Mode

Select the SCM installation mode appropriate for your system configuration. You can select either a standalone or high availability (HA-Active, HA-Standby) configuration.

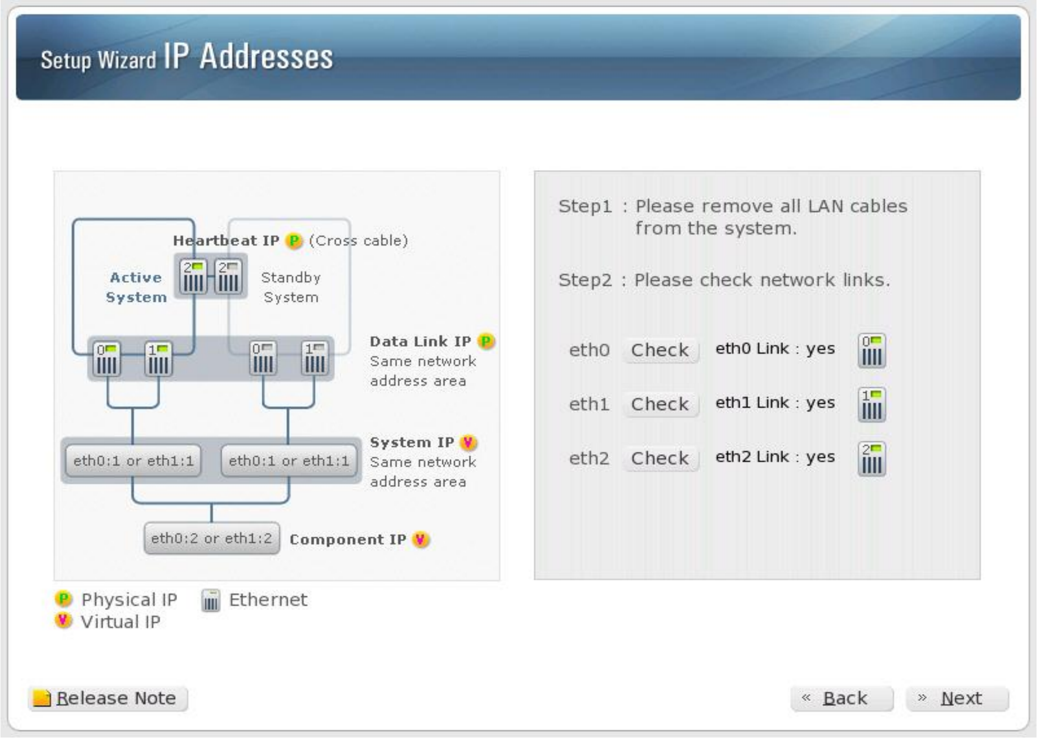


If you select the edition not appropriate to your license, the system does not operate.

NOTE

4.4.3.2 Checking the LAN Ports

Remove all LAN cables from the system. Then connect one at a time and click the **Check** button. Through this process, you can identify port connections for the LAN cards.



Setup Wizard IP Addresses

Step1 : Please remove all LAN cables from the system.

Step2 : Please check network links.

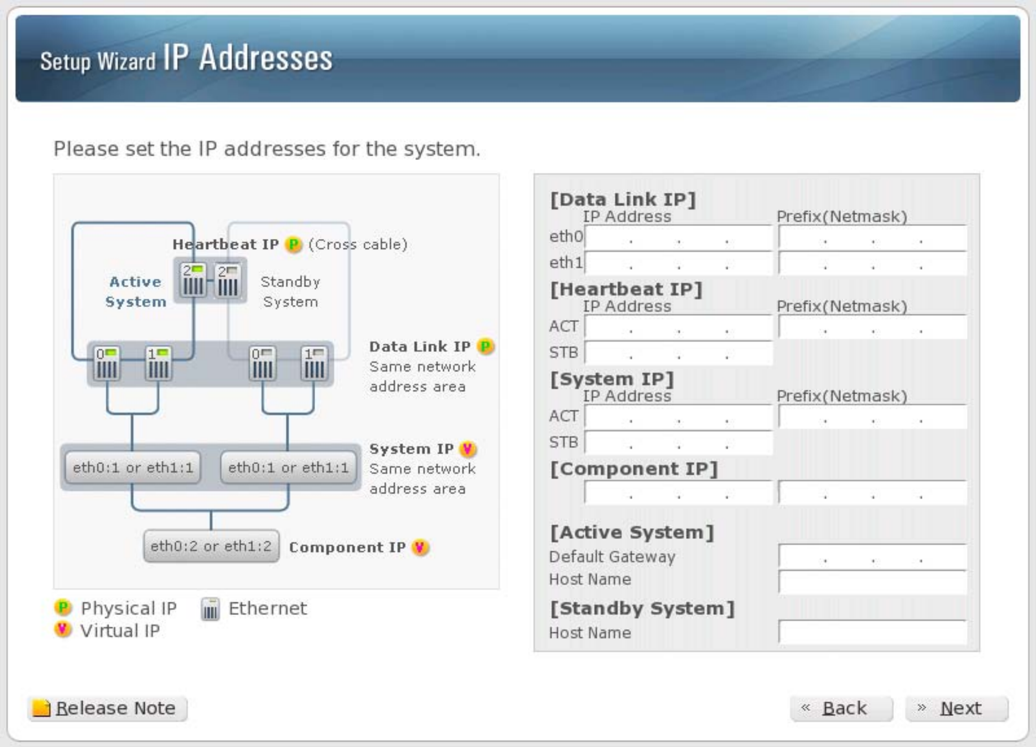
eth0 Check eth0 Link : yes

eth1 Check eth1 Link : yes

eth2 Check eth2 Link : yes

4.4.3.3 Entering IP Addresses

Enter the network information for your system configuration.



Setup Wizard IP Addresses

Please set the IP addresses for the system.

[Data Link IP]

IP Address / Prefix(Netmask)

eth0

eth1

[Heartbeat IP]

IP Address / Prefix(Netmask)

ACT

STB

[System IP]

IP Address / Prefix(Netmask)

ACT

STB

[Component IP]

[Active System]

Default Gateway

Host Name

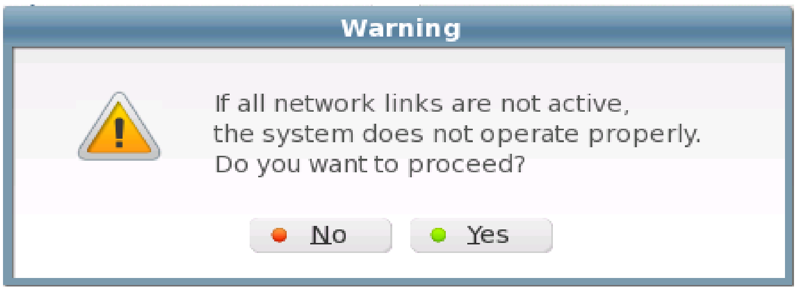
[Standby System]

Host Name

Item	Description
Data Link IP	- eth0: Enter the IP address of eth0. - eth1: Enter the IP address of eth1. - Netmask: Enter ‘255.255.255.0’. The subnet addresses of eth0 and eth1 must be identical.
Heartbeat IP	- ACT: Enter the heartbeat IP address of the active system. - STB: Enter the heartbeat IP address of the standby system. - Netmask: Enter ‘255.255.255.0’. The subnet addresses of the active and standby systems must be identical.
System IP	- ACT: Enter the system IP address of the active system. - STB: Enter the system IP address of the standby system. - Netmask: Enter ‘255.255.255.0’. The subnet addresses of the active and standby systems must be identical.
Component IP	IP Address: Enter the IP address that the SCM will use. Netmask: Enter ‘255.255.255.0’.
Active System	Default Gateway: Enter the gateway address. Host Name: Enter the host name of the active system.
Standby System	Enter the host name of the standby system.

CHECK

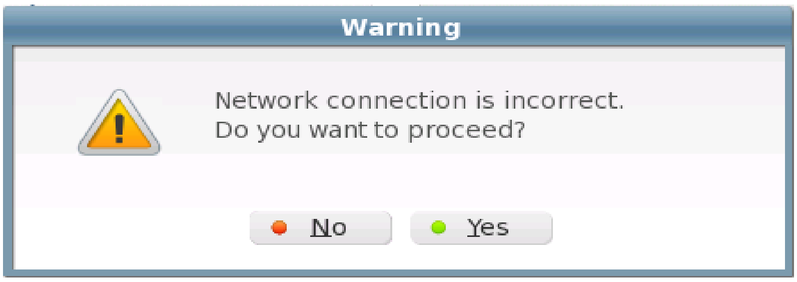
- If you install the SCM without checking the LAN ports, an error may occur when operating the system. Make sure to check the LAN ports and then proceed to the installation.



Warning

If all network links are not active,
the system does not operate properly.
Do you want to proceed?

- If you install the SCM when there is an error in the LAN port, the warning message appears as shown below. Correct the port error and then proceed to the next step.

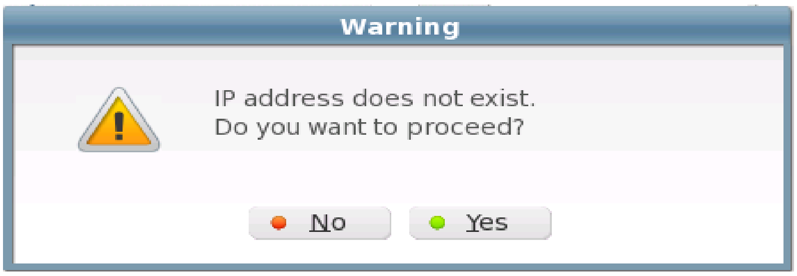


Warning

Network connection is incorrect.
Do you want to proceed?

NOTE

If the network information is not provided, the warning message appears as shown in the figure below. If the network information is configured incorrectly, the system may not operate properly.

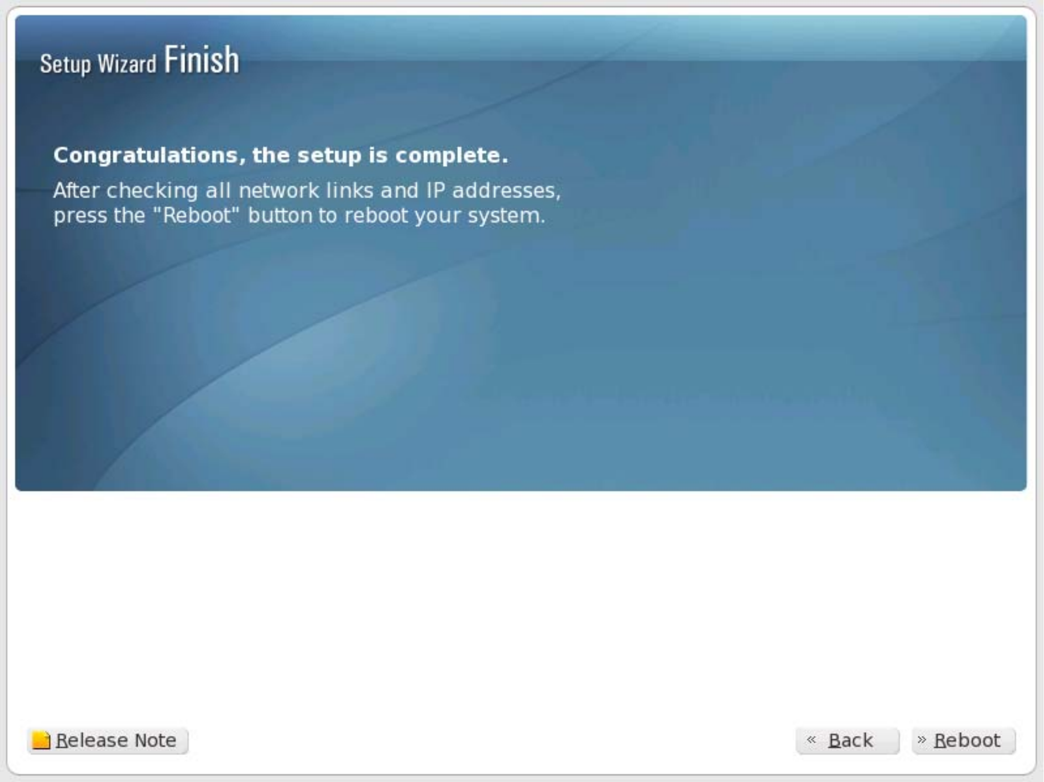


Warning

IP address does not exist.
Do you want to proceed?

4.4.3.4 Finishing the Configuration

When the configuration is completed, click the **Reboot** button to restart your computer. If a configuration value is incorrect, you can click the **Back** button to correct it.



Setup Wizard Finish

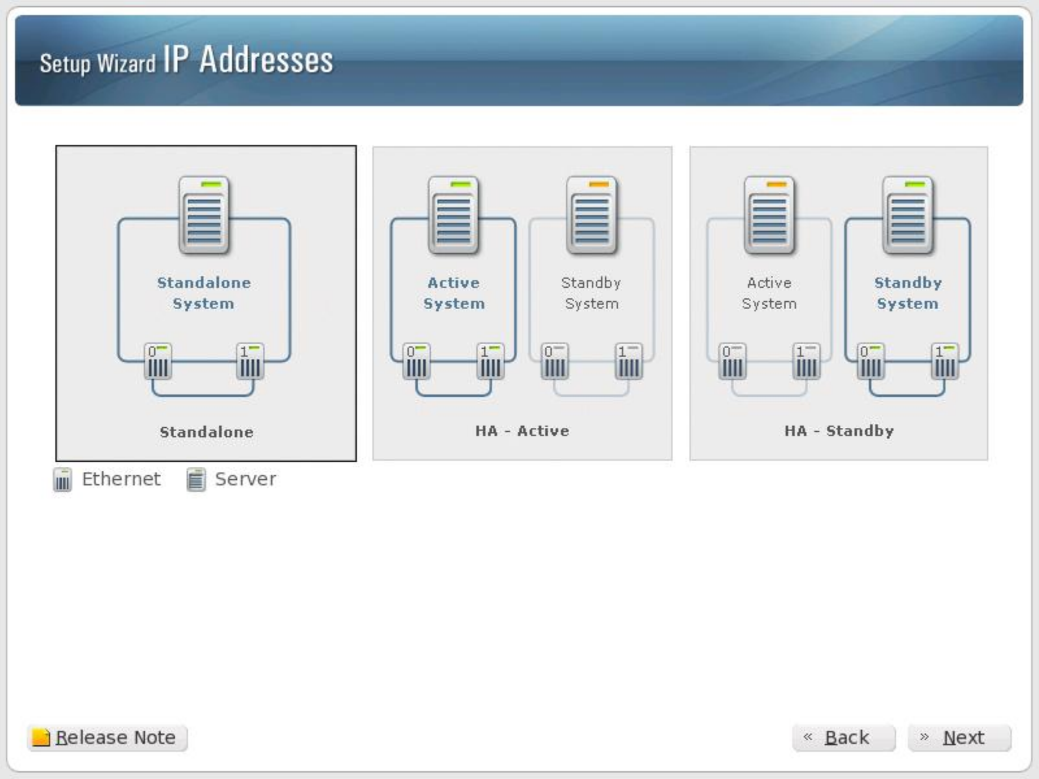
Congratulations, the setup is complete.

After checking all network links and IP addresses, press the "Reboot" button to reboot your system.

4.4.4 Configuring HA-Standby Server

4.4.4.1 Selecting the Installation Mode

Select the SCM installation mode appropriate for your system configuration. You can select either a standalone or high availability (HA-Active, HA-Standby) configuration.

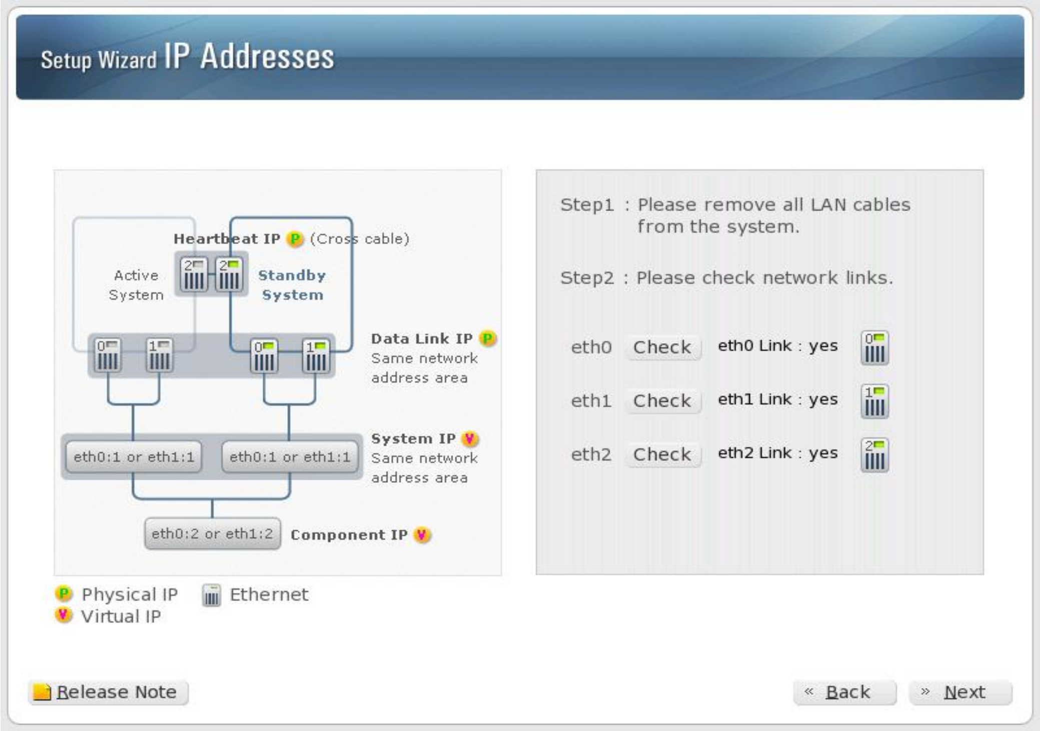


NOTE

If you select the edition not appropriate to your license, the system does not operate.

4.4.4.2 Checking the LAN Ports

Remove all LAN cables from the system. Then connect one at a time and click the **Check** button. Through this process, you can identify port connections for the LAN cards.



Setup Wizard IP Addresses

Step1 : Please remove all LAN cables from the system.

Step2 : Please check network links.

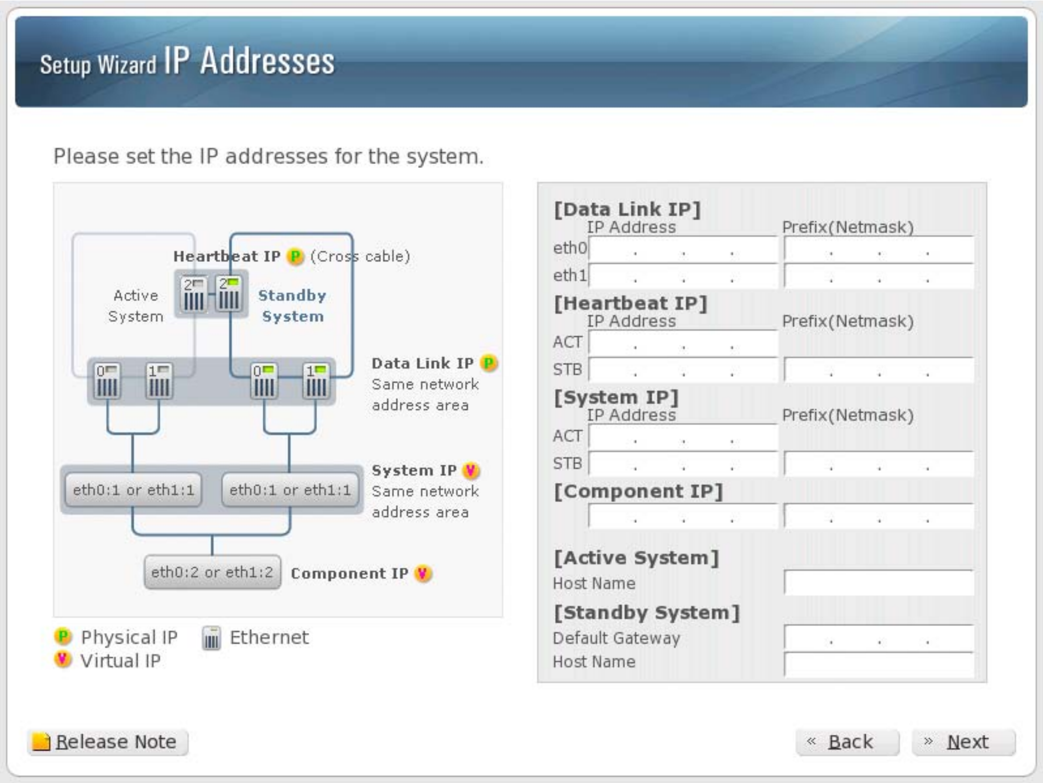
eth0 Check eth0 Link : yes

eth1 Check eth1 Link : yes

eth2 Check eth2 Link : yes

4.4.4.3 Entering IP Addresses

Enter the network information for your system configuration.



Setup Wizard IP Addresses

Please set the IP addresses for the system.

[Data Link IP]

	IP Address	Prefix(Netmask)
eth0	. . .	. . .
eth1	. . .	. . .

[Heartbeat IP]

	IP Address	Prefix(Netmask)
ACT	. . .	
STB	. . .	. . .

[System IP]

	IP Address	Prefix(Netmask)
ACT	. . .	
STB	. . .	. . .

[Component IP]

. . .   . . .

[Active System]

Host Name

[Standby System]

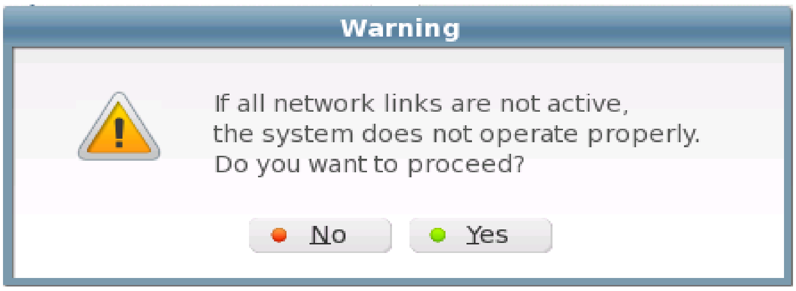
Default Gateway . . .

Host Name

Item	Description
Data Link IP	- eth0 IP Address: Enter the IP address of eth0. - eth1 IP Address: Enter the IP address of eth1. - Netmask: Enter ‘255.255.255.0’. The subnet addresses of eth0 and eth1 must be identical.
Heartbeat IP	- ACT IP Address: Enter the heartbeat IP address of the active system. - STB IP Address: Enter the heartbeat IP address of the standby system. - Netmask: Enter ‘255.255.255.0’. The subnet addresses of the active and standby systems must be identical.
System IP	- ACT IP Address: Enter the system IP address of the active system. - STB IP Address: Enter the system IP address of the standby system. - Netmask: Enter ‘255.255.255.0’. The subnet addresses of the active and standby systems must be identical.
Component IP	IP Address: Enter the IP address that the SCM will use. Netmask: Enter ‘255.255.255.0’.
Active System	Enter the host name of the active system.
Standby System	Default Gateway: Enter the gateway address. Host Name: Enter the host name of the standby system.

CHECK

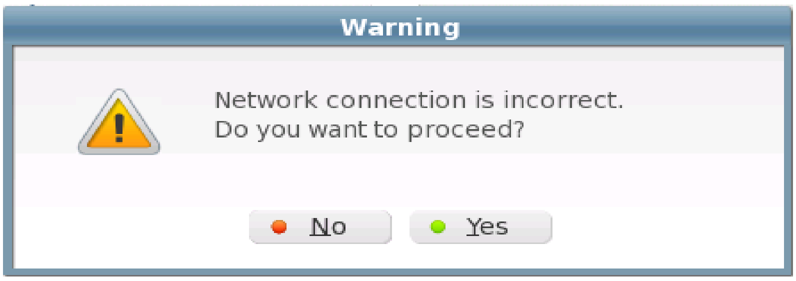
- If you install the SCM without checking the LAN ports, an error may occur when operating the system. Make sure to check the LAN ports and then proceed to the installation.



Warning

If all network links are not active,
the system does not operate properly.
Do you want to proceed?

- If you install the SCM when there is an error in the LAN port, the warning message appears as shown below. Correct the port error and then proceed to the next step.

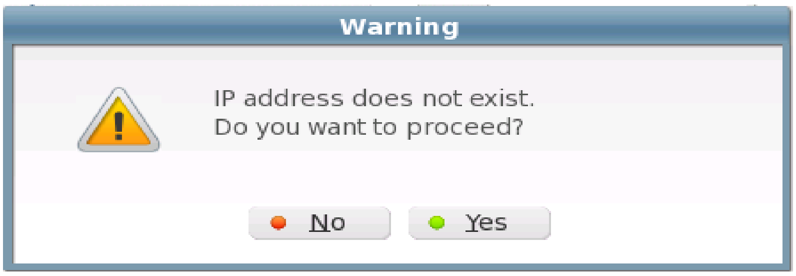


Warning

Network connection is incorrect.
Do you want to proceed?

NOTE

If the network information is not provided, the warning message appears as shown in the figure below. If the network information is configured incorrectly, the system may not operate properly.

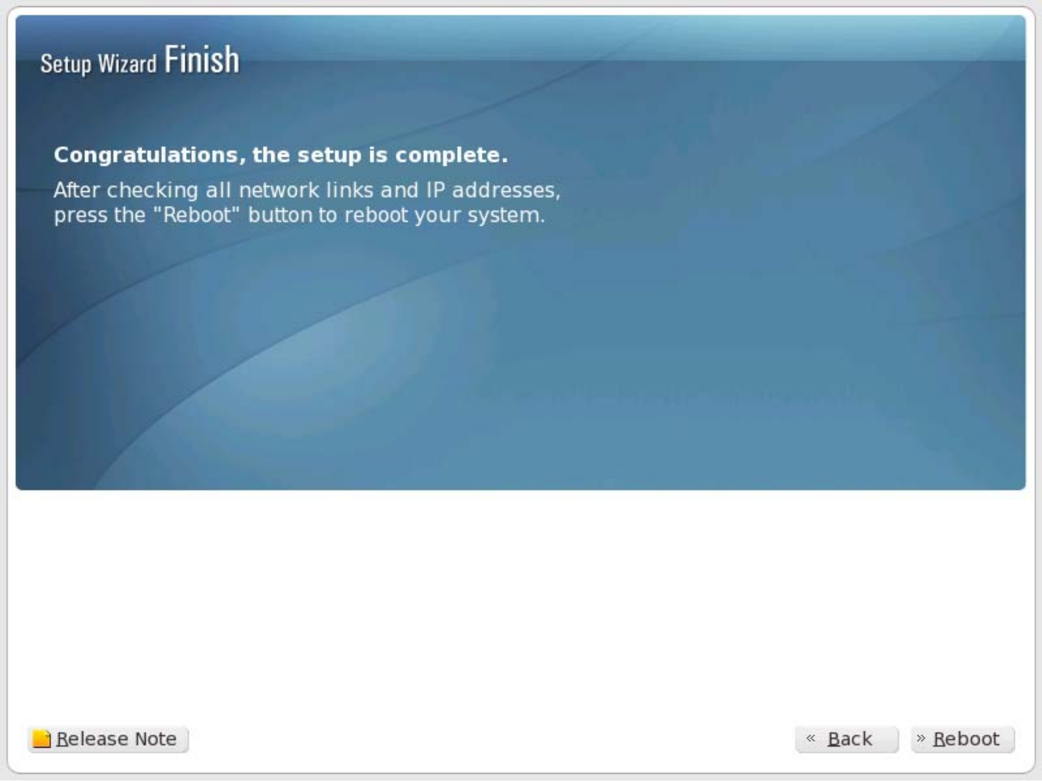


Warning

IP address does not exist.
Do you want to proceed?

4.4.4.4 Finishing the Configuration

When the configuration is completed, click the **Reboot** button to restart your computer. If a configuration value is incorrect, you can click the **Back** button to correct it.



Setup Wizard Finish

Congratulations, the setup is complete.

After checking all network links and IP addresses, press the "Reboot" button to reboot your system.

4.5 Updating SCM Server Software

This chapter describes the procedure for updating SCM software.

CAUTION

When updating the SCM software, all the services of the SCM stop. When the upgrade is complete, the SCM restarts automatically.

NOTE

To upgrade SCM software, you should upload upgrade files to SCM server by using USB memory stick. Next you can execute upgrade program on SCM server. The reason upgrade program should be executed on SCM server is that the Linux system do not allow you to execute programs on USB memory stick because of security.

4.5.1 Updating Stand Alone System

For standalone configuration, you can perform a updating as follows:

1) Store the package directory in your USB memory stick.

NOTE

The name of package directory is YYYYMMDD_SCME_X.X.X.X and its meanings are as follows

YYYY: year

MM: month

DD: day

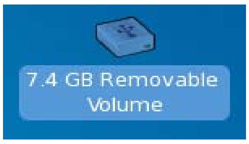
X.X.X.X: SCM version

- platform version
- major version
- minor version
- build version

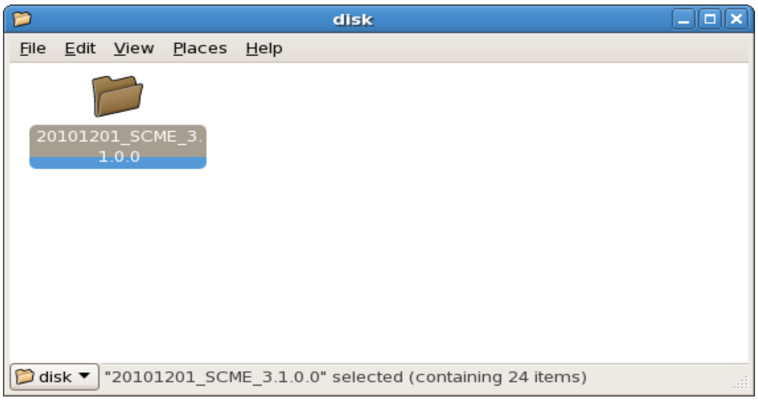
2) Login as root user by using the keyboard and mouse that is connected to the SCM server.

3) Insert the USB memory stick into the SCM server

4) Double-click a USB memory icon on the Linux desktop.



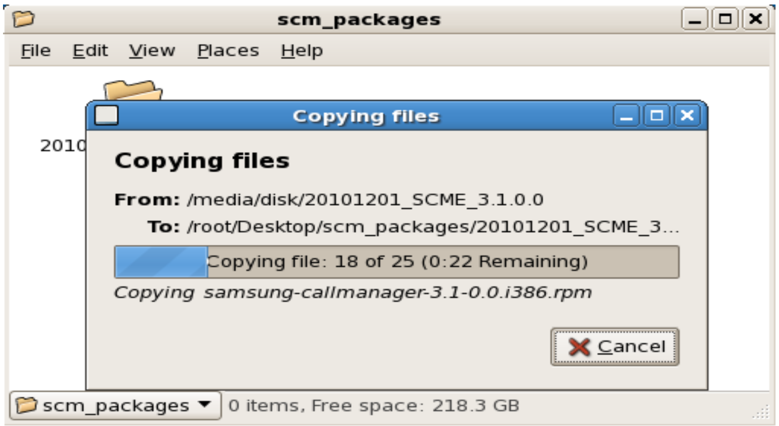
5) Click a directory stored in the USB memory and click right button of mouse. And select 'Copy' menu.



"20101201_SCME_3.1.0.0" selected (containing 24 items)

6) Double-click a 'scm_packages' directory icon on the Linux desktop.

7) Click right button of mouse in 'scm_packages' directory window. And select 'Paste' menu. So the package directory stored in the USB memory will be copied into the 'scm_packages' directory.



Copying files

From: /media/disk/20101201_SCME_3.1.0.0

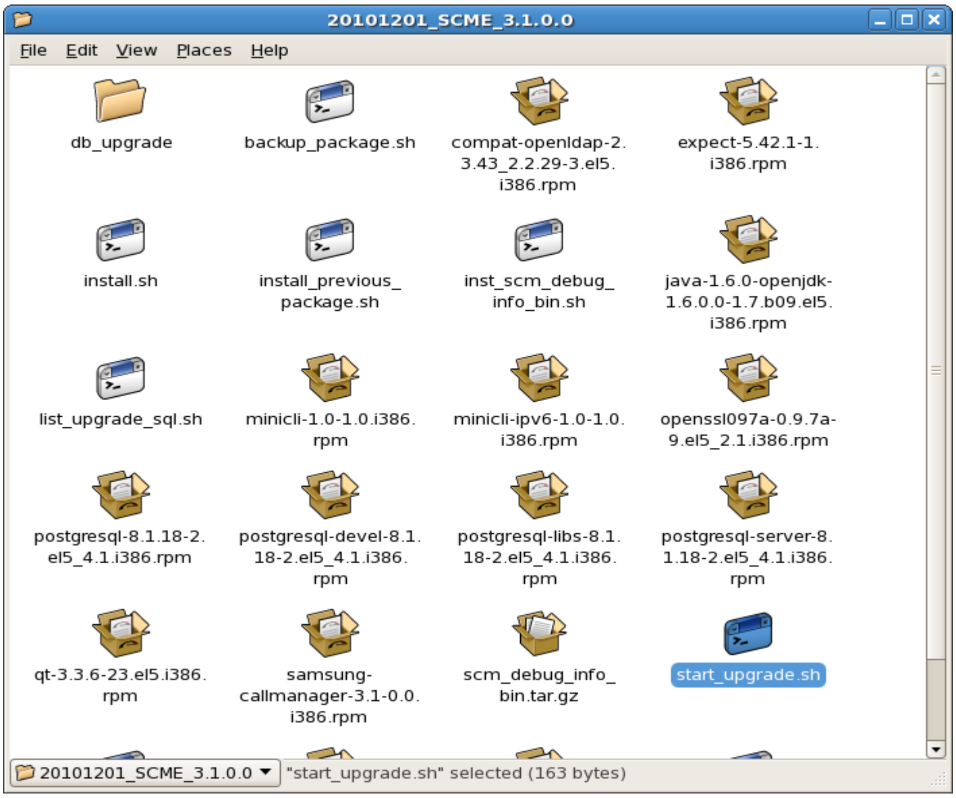
To: /root/Desktop/scm_packages/20101201_SCME_3...

Copying file: 18 of 25 (0:22 Remaining)

Copying samsung-callmanager-3.1-0.0.i386.rpm

0 items, Free space: 218.3 GB

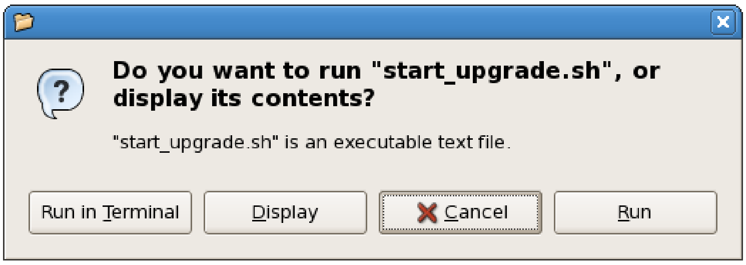
8) After copy, double-click the package directory. And double-click ‘start_upgrade.sh’ executable file.



20101201_SCME_3.1.0.0
File Edit View Places Help
db_upgrade
backup_package.sh
compat-openldap-2.3.43_2.2.29-3.el5.i386.rpm
expect-5.42.1-1.i386.rpm
install.sh
install_previous_package.sh
inst_scm_debug_info_bin.sh
java-1.6.0-openjdk-1.6.0.0-1.7.b09.el5.i386.rpm
list_upgrade_sql.sh
minicli-1.0-1.0.i386.rpm
minicli-ipv6-1.0-1.0.i386.rpm
openssl097a-0.9.7a-9.el5_2.1.i386.rpm
postgresql-8.1.18-2.el5_4.1.i386.rpm
postgresql-devel-8.1.18-2.el5_4.1.i386.rpm
postgresql-libs-8.1.18-2.el5_4.1.i386.rpm
postgresql-server-8.1.18-2.el5_4.1.i386.rpm
qt-3.3.6-23.el5.i386.rpm
samsung-callmanager-3.1-0.0.i386.rpm
scm_debug_info_bin.tar.gz
start_upgrade.sh
20101201_SCME_3.1.0.0

"start_upgrade.sh" selected (163 bytes)

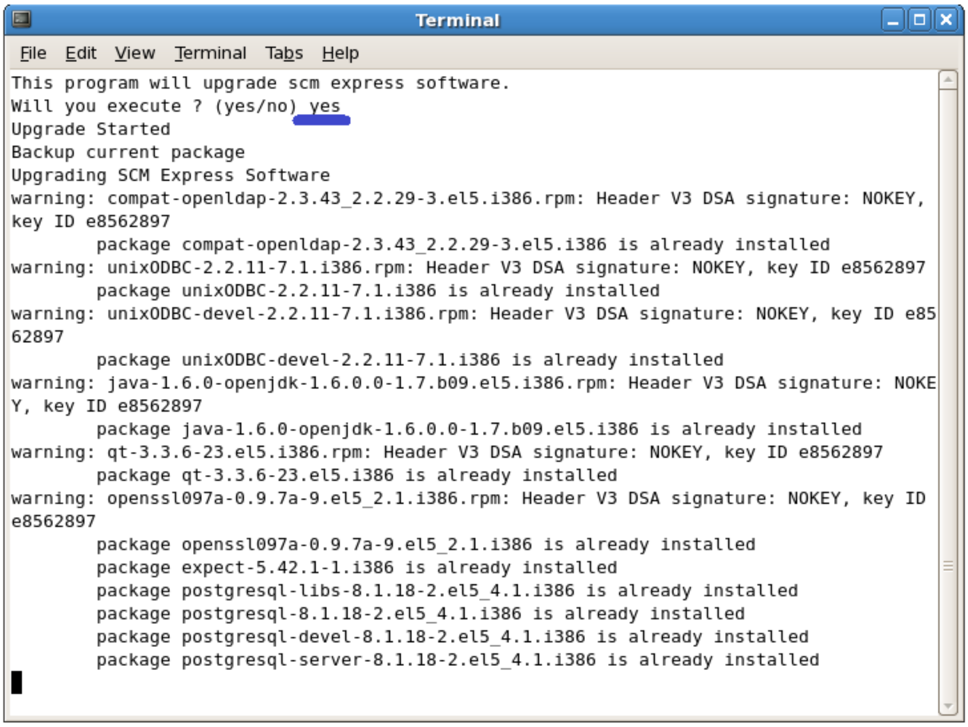
9) Click ‘Run in terminal’ button.



Do you want to run "start_upgrade.sh", or display its contents?

"start_upgrade.sh" is an executable text file.

10) Enter 'yes' if you want to update SCM software. Updating is progressed as follow. And system will reboot if all procedure is done.



```
This program will upgrade scm express software.
Will you execute ? (yes/no) yes
Upgrade Started
Backup current package
Upgrading SCM Express Software
warning: compat-openldap-2.3.43_2.2.29-3.el5.i386.rpm: Header V3 DSA signature: NOKEY,
key ID e8562897
        package compat-openldap-2.3.43_2.2.29-3.el5.i386 is already installed
warning: unixODBC-2.2.11-7.1.i386.rpm: Header V3 DSA signature: NOKEY, key ID e8562897
        package unixODBC-2.2.11-7.1.i386 is already installed
warning: unixODBC-devel-2.2.11-7.1.i386.rpm: Header V3 DSA signature: NOKEY, key ID e85
62897
        package unixODBC-devel-2.2.11-7.1.i386 is already installed
warning: java-1.6.0-openjdk-1.6.0.0-1.7.b09.el5.i386.rpm: Header V3 DSA signature: NOKE
Y, key ID e8562897
        package java-1.6.0-openjdk-1.6.0.0-1.7.b09.el5.i386 is already installed
warning: qt-3.3.6-23.el5.i386.rpm: Header V3 DSA signature: NOKEY, key ID e8562897
        package qt-3.3.6-23.el5.i386 is already installed
warning: openssl097a-0.9.7a-9.el5_2.1.i386.rpm: Header V3 DSA signature: NOKEY, key ID
e8562897
        package openssl097a-0.9.7a-9.el5_2.1.i386 is already installed
        package expect-5.42.1-1.i386 is already installed
        package postgresql-libs-8.1.18-2.el5_4.1.i386 is already installed
        package postgresql-8.1.18-2.el5_4.1.i386 is already installed
        package postgresql-devel-8.1.18-2.el5_4.1.i386 is already installed
        package postgresql-server-8.1.18-2.el5_4.1.i386 is already installed
```

4.5.2 Updating High Availability System

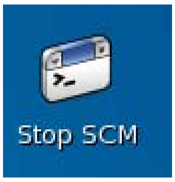
For high availability configuration, you can perform a updating as follows:

1) Store the package directory in your USB memory stick.

> NOTE
>
> The name of package directory is YYYYMMDD_SCME_X.X.X.X and its meanings are as follows
>
> YYYY: year
>
> MM: month
>
> DD: day
>
> X.X.X.X: SCM version
>
> - platform version
>
> - major version
>
> - minor version
>
> - build version

2) Login as root user by using the keyboard and mouse that is connected to the standby SCM server.

3) Double-click a 'Stop SCM' icon on the Linux desktop. And you have standby SCM stopped.

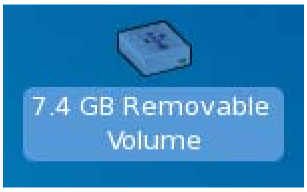


4) Login as root user by using the keyboard and mouse that is connected to the active SCM server.

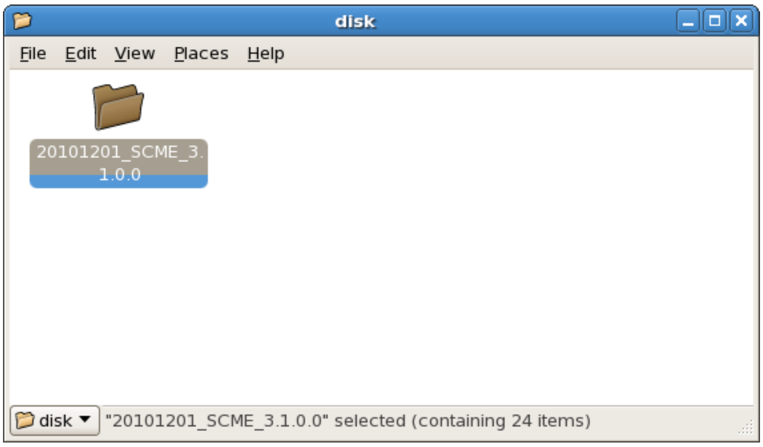
5) Double-click a 'Stop SCM' icon on the Linux desktop. And you have active SCM stopped.

6) Insert the USB memory stick into the active SCM server

7) Double-click a USB memory icon on the Linux desktop.

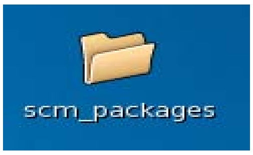


8) Click a directory stored in the USB memory and click right button of mouse. And select ‘Copy’ menu.

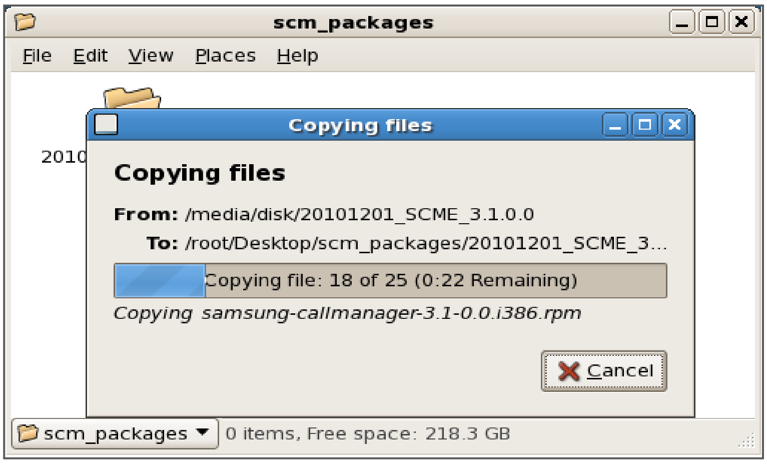


"20101201_SCME_3.1.0.0" selected (containing 24 items)

9) Double-click a ‘scm_packages’ directory icon on the Linux desktop.



10) Click right button of mouse in ‘scm_packages’ directory window. And select ‘Paste’ menu. So the package directory stored in the USB memory will be copied into the ‘scm_packages’ directory.



Copying files

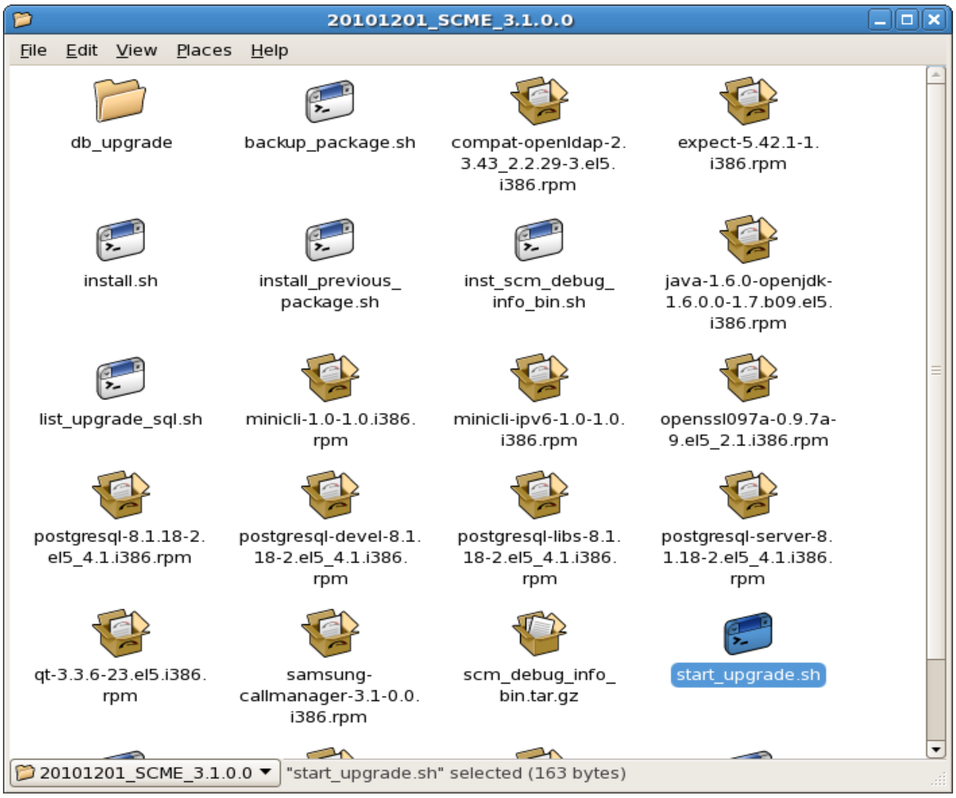
From: /media/disk/20101201_SCME_3.1.0.0
To: /root/Desktop/scm_packages/20101201_SCME_3...

Copying file: 18 of 25 (0:22 Remaining)

Copying samsung-callmanager-3.1-0.0.i386.rpm

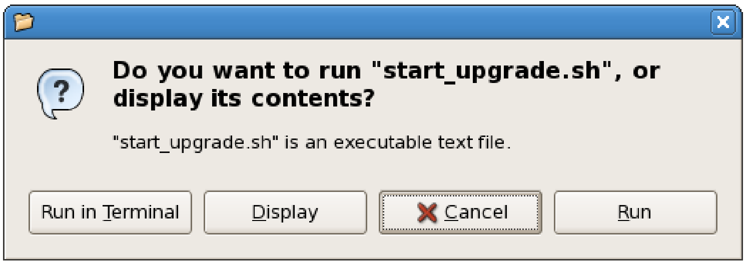
0 items, Free space: 218.3 GB

11) After copy, double-click the package directory. And double-click ‘start_upgrade.sh’ executable file.


20101201_SCME_3.1.0.0
File Edit View Places Help
db_upgrade
backup_package.sh
compat-openldap-2.3.43_2.2.29-3.el5.i386.rpm
expect-5.42.1-1.i386.rpm
install.sh
install_previous_package.sh
inst_scm_debug_info_bin.sh
java-1.6.0-openjdk-1.6.0.0-1.7.b09.el5.i386.rpm
list_upgrade_sql.sh
minicli-1.0-1.0.i386.rpm
minicli-ipv6-1.0-1.0.i386.rpm
openssl097a-0.9.7a-9.el5_2.1.i386.rpm
postgresql-8.1.18-2.el5_4.1.i386.rpm
postgresql-devel-8.1.18-2.el5_4.1.i386.rpm
postgresql-libs-8.1.18-2.el5_4.1.i386.rpm
postgresql-server-8.1.18-2.el5_4.1.i386.rpm
qt-3.3.6-23.el5.i386.rpm
samsung-callmanager-3.1-0.0.i386.rpm
scm_debug_info_bin.tar.gz
start_upgrade.sh
20101201_SCME_3.1.0.0

"start_upgrade.sh" selected (163 bytes)

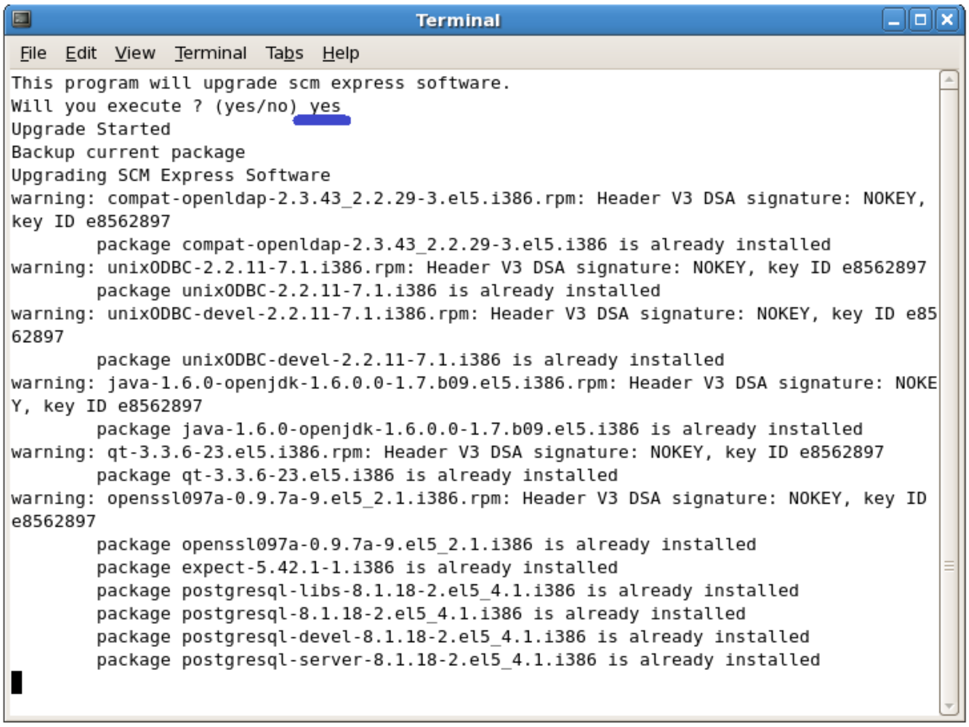
12) Click ‘Run in terminal’ button.



Do you want to run "start_upgrade.sh", or display its contents?

"start_upgrade.sh" is an executable text file.

13) Enter ‘yes’ if you want to update SCM software. Updating is progressed as follow. And system will reboot if all procedure is done.



```
This program will upgrade scm express software.
Will you execute ? (yes/no) yes
Upgrade Started
Backup current package
Upgrading SCM Express Software
warning: compat-openldap-2.3.43_2.2.29-3.el5.i386.rpm: Header V3 DSA signature: NOKEY,
key ID e8562897
        package compat-openldap-2.3.43_2.2.29-3.el5.i386 is already installed
warning: unixODBC-2.2.11-7.1.i386.rpm: Header V3 DSA signature: NOKEY, key ID e8562897
        package unixODBC-2.2.11-7.1.i386 is already installed
warning: unixODBC-devel-2.2.11-7.1.i386.rpm: Header V3 DSA signature: NOKEY, key ID e85
62897
        package unixODBC-devel-2.2.11-7.1.i386 is already installed
warning: java-1.6.0-openjdk-1.6.0.0-1.7.b09.el5.i386.rpm: Header V3 DSA signature: NOKE
Y, key ID e8562897
        package java-1.6.0-openjdk-1.6.0.0-1.7.b09.el5.i386 is already installed
warning: qt-3.3.6-23.el5.i386.rpm: Header V3 DSA signature: NOKEY, key ID e8562897
        package qt-3.3.6-23.el5.i386 is already installed
warning: openssl097a-0.9.7a-9.el5_2.1.i386.rpm: Header V3 DSA signature: NOKEY, key ID
e8562897
        package openssl097a-0.9.7a-9.el5_2.1.i386 is already installed
        package expect-5.42.1-1.i386 is already installed
        package postgresql-libs-8.1.18-2.el5_4.1.i386 is already installed
        package postgresql-8.1.18-2.el5_4.1.i386 is already installed
        package postgresql-devel-8.1.18-2.el5_4.1.i386 is already installed
        package postgresql-server-8.1.18-2.el5_4.1.i386 is already installed
```

Insert the USB memory stick into the standby SCM server. And proceed to update as you do active server

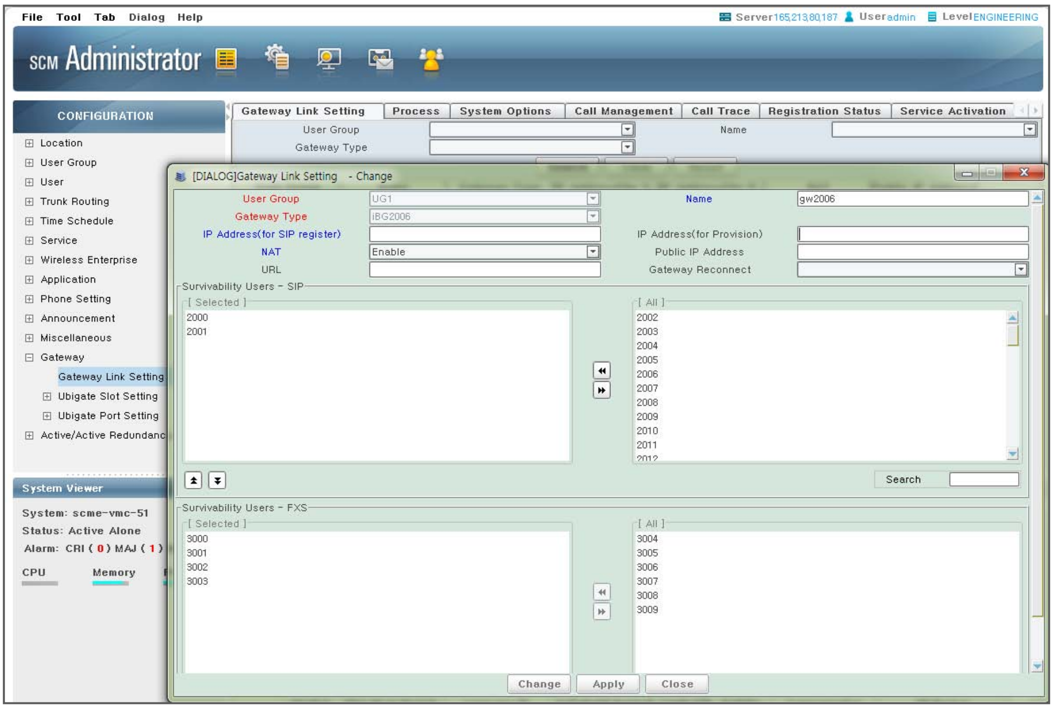
CHAPTER 5. Installing Ubigate iBG Series Gateways

5.1 Preparing SCM Server

To have Gateways interoperate with SCM, the following items must be configured for SCM server.

Creating Gateway Link

You must register the Gateway to interoperate with SCM using the **[CONFIGURATION > Gateway]** menu.



System: scme-vmc-51
Status: Active Alone
Alarm: CRI (0) MAJ (1)

User Group: UG1
Gateway Type: iBG2006
Name: gw2006
IP Address(for SIP register):
IP Address(for Provision):
NAT: Enable
Public IP Address:
URL:
Gateway Reconnect:

Survivability Users - SIP
[Selected]: 2000, 2001
[All]: 2002, 2003, 2004, 2005, 2006, 2007, 2008, 2009, 2010, 2011, 2012

Survivability Users - FXS
[Selected]: 3000, 3001, 3002, 3003
[All]: 3004, 3005, 3006, 3007, 3008, 3009

Item	Description
User Group	Specify a user group which will be assigned to Gateway.
Name	Enter a name for Gateway.
Gateway Type	Enter a model type for Gateway.
IP Address (for SIP register)	Enter the IP address of Gateway for SIP registration.
IP Address (for Provision)	Enter the IP address of Gateway for provision. Generally this should be same address for SIP register.
NAT	If the gateway is running under NAT, Enables this option.
Public IP Address	When the gateway is running under NAT, enter the public IP address of Gateway.
Survivability Users-SIP	This is the list of SIP phones for survivability to allocate to the voice gateway. When SCM creates the profile for a SIP phone, it includes the IP address and the port of the interoperating gateway in survival mode. When the SIP phone is disconnected from SCM, it sends a register message to the gateway included in the profile.
Survivability Users-FXS	This is the list of FXS phones of the voice gateway. If the gateway type is Ubigate iBG, this item is not selective list.

SCM provides the survivable telephony support service, whereby, when an IP phone is disconnected from SCM, the phone is connected to the gateway for minimum PBX features. The survival feature really works by the gateway and the IP phone and not by SCM. Generally, it is usually used not when there is a problem with SCM but when the IP network between the IP phone and SCM experiences a trouble, especially when the phone and SCM are in different locations.
Ubigate iBG Gateways support both the survival mode and the SCM interoperation mode.

Survivable Telephony Mode

When SCM's gateway is interoperating with SCM, if the gateway determines that the IP network with SCM is disconnected, it uses the service profiles downloaded from SCM for the FXS subscribers and SIP phone subscribers to continue to provide gateway's native call processing services.
In particular, Ubigate iBG Gateways use the SIP phone subscriber service profile downloaded from SCM to automatically configure dial-peer for processing incoming calls for SIP phones and authenticates SIP phones in order to make calls and provide supplementary services.
Ubigate iBG Gateway series periodically (30 seconds by default) send Register messages to SCM. If it receives a 200 OK response, it enters the SCM interoperation mode again.

Supplementary Service on Survival mode

Ubigate iBG Gateway series service provides only the following features in survival mode.

Service	Description
Call Forward	Call Forward All, Busy and No Answer
Hold/Resume	-
Transfer	Consultation and Blind Transfer
DND	Do Not Disturb
Conference	Conference On Answer Only
Call Waiting	-
Call Pickup	Direct and Group Call Pickup
MOH	Music On Hold

5.2 Ubigate iBG series Hardware

The Ubigate iBG series are available for the voice gateway of SCM, and can be used following models.

Table 5.1 Voice Port Capacity of iBG series

Model	FXS	FXO	T1/PRI	SIP Phone (Survivability)
iBG3026	60	28	4	256
iBG2016	40	24	4	128
iBG2006	16	16	2	64
iBG1003A4	4	2	NA	50
iBG1003A8	8	2	NA	50
iBG1003AG	16	2	NA	50
iBG1003D4	4	NA	2	50

iBG3026

Detailed installation for the iBG3026, please refer to the ‘iBG3026 Installation Manual’.

iBG2016

Detailed installation for the iBG2016, please refer to the ‘iBG2016 Installation Manual’.

iBG2006

Detailed installation for the iBG2006, please refer to the ‘iBG2006 Installation Manual’.

iBG1003

Detailed installation for the iBG1003, please refer to the ‘iBG1003 Installation Manual’.

5.3 Ubigate iBG series Software

5.3.1 Configuring Gateway System

Following example shows the commands used verify the gateway 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
```

How to Configure IP address

Configuration Steps

- configure terminal
- interface
- ip address
- exit

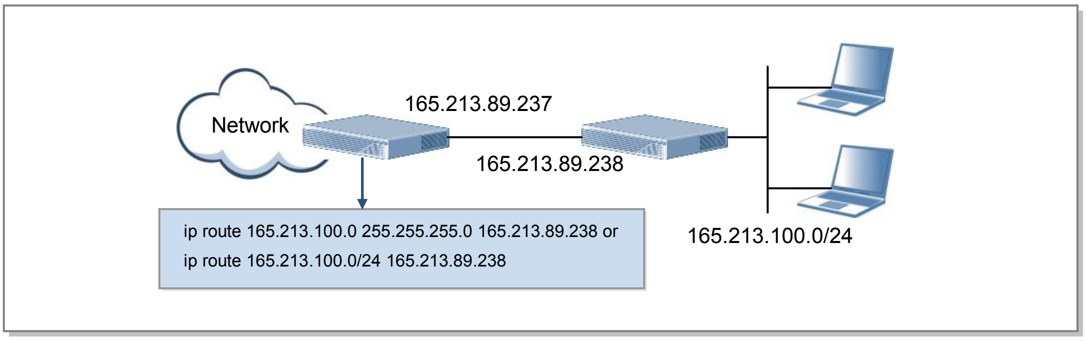
Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters global configuration mode.
2	Interface type number Example) /configure# interface Ethernet 0/0	Enters interface configuration mode to configure specific interface.
3	ip address ip_address subnet_mask Example) /configure/interface/ethernet(0/0)# 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

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.
Following steps show the way to add a route entry.

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. Following figure illustrates a simple network configuration.



ip route 165.213.100.0 255.255.255.0 165.213.89.238 or
ip route 165.213.100.0/24 165.213.89.238

```
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
```

5.3.2 Connecting to Network

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.
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.
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.

shutdown voip-gateway

VoIP gateway must be shutdown before set the IP address of VoIP gateway, follows next procedures.

Configuration Steps

- configure terminal
- voip-gateway
- shutdown
- exit

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 Example) /configure/voip-gateway# shutdown	Shuts down voip call services
4	exit Example) /configure/interface/ethernet(0/0)# exit	Exits the current mode

bind interface

To bind the interface for source address of VoIP signaling and media, follow next procedures.

Configuration Steps

- configure terminal
- voip-gateway
- bind control
- bind media
- exit

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 type num Example) /configure/voip-gateway# bind control interface ethernet 0/0	Sets source interface for SIP and H.323.
4	bind media interface type num Example) /configure/voip-gateway# bind control interface ethernet 0/0	Sets source interface for media - RTP/RTCP.
5	exit Example) /configure/voip-gateway# exit	Exits the current mode

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

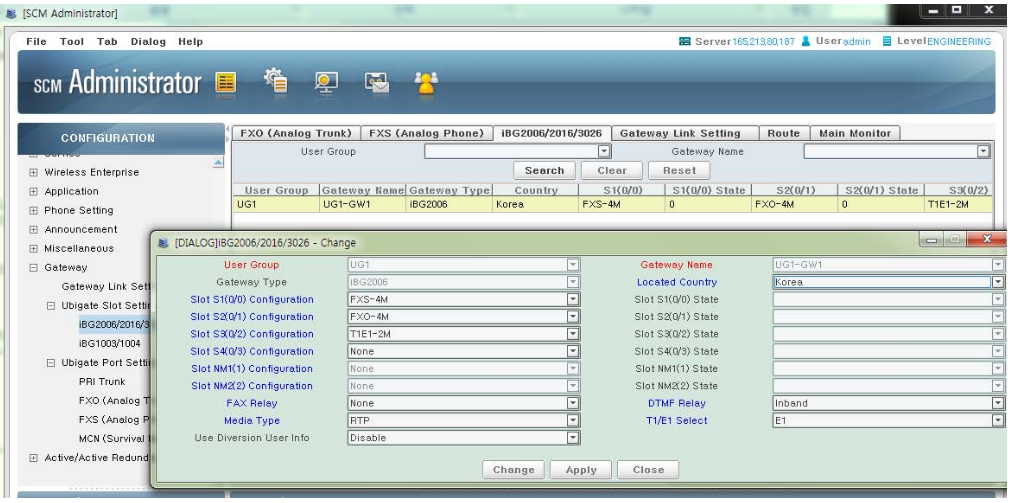
Step	Command	Purpose
1	configure terminal Example) # configure terminal	Enters global configuration mode.
2	voip-gateway Example) /configure# voip-gateway	Enters voip-gateway configuration mode.
3	host domain-name DOMAIN.COM Example) /configure/voip-gateway# host domain-name samsung.com	Sets domain name for Ubigate iBG
4	exit Example) /configure/voip-gateway# exit	Exits the current mode

5.3.3 Connecting to PSTN

To allow interoperation between Ubigate iBG series and SCM, the following information must be configured. You can use the SCM Administrator and modify the information for Ubigate iBG series.

5.3.3.1 Configuring Slot Setting

This section describes the configuration of Slot Setting.
Selects a Gateway which you want to configure in the following window, and press change button and select change.
Selects a Slot Configuration item and choose a card type properly.
Slot State indicates actual card equipment state. This state can be updated by receiving information from the gateway.
If necessary, change following configurations for the gateway.



User Group: | Gateway Name:

User Group	Gateway Name	Gateway Type	Country	S1(0/0)	S1(0/0) State	S2(0/1)	S2(0/1) State	S3(0/2)
UG1	UG1-GW1	iBG2006	Korea	FXS-4M	0	FXO-4M	0	T1E1-2M

User Group	UG1	Gateway Name	UG1-GW1
Gateway Type	iBG2006	Located Country	Korea
Slot S1(0/0) Configuration	FXS-4M	Slot S1(0/0) State	
Slot S2(0/1) Configuration	FXO-4M	Slot S2(0/1) State	
Slot S3(0/2) Configuration	T1E1-2M	Slot S3(0/2) State	
Slot S4(0/3) Configuration	None	Slot S4(0/3) State	
Slot NM1(1) Configuration	None	Slot NM1(1) State	
Slot NM2(2) Configuration	None	Slot NM2(2) State	
FAX Relay	None	DTMF Relay	Inband
Media Type	RTP	T1/E1 Select	E1
Use Diversion User Info	Disable		

FAX Relay

To selects type of FAX relay for the gateway, use the ‘FAX relay’ menu in Slot Setting configuration window.

- T38 redundancy 0: Using T38 fax relay with redundancy number 0.
- T38 redundancy 1: Using T38 fax relay with redundancy number 1.
- T38 redundancy 2: Using T38 fax relay with redundancy number 2.
- T38 redundancy 3: Using T38 fax relay with redundancy number 3.
- Path-through g.711 U-law: Using Path-through g.711 U-law fax relay.
- Path-through g.711 A-law: Using Path-through g.711 A-law fax relay.

DTMF Relay

To selects type of DTMF relay for the gateway, use the ‘DTMF relay’ menu in Slot Setting configuration window.

- Inband: inband.
- SIP Notify: SIP NOTIFY method.
- SIP Info: SIP INFO method using named events.
- SIP Info-digits: SIP INFO method using decimal number.
- RFC2833: Out-of-band 2833 (RTP-NTE)

Media Type

To selects type of RTP media type for the gateway, use the ‘Media Type’ menu in Slot Setting configuration window.

- RTP: RTP
- SRTP-AES: SRTP using AES Counter Mode.
- SRTP-ARIA: SRTP using ARIA counter Mode.
- SRTP-ARIA-AES: SRTP using ARIA and AES.

T1/E1 Select

To selects carrier-type of T1/E1 for the gateway, use the ‘T1/E1 Select’ menu in Slot Setting configuration window. If this value is different with the gateway configuration, the gateway will reboot to change carrier-type of T1/E1.

- E1
- T1

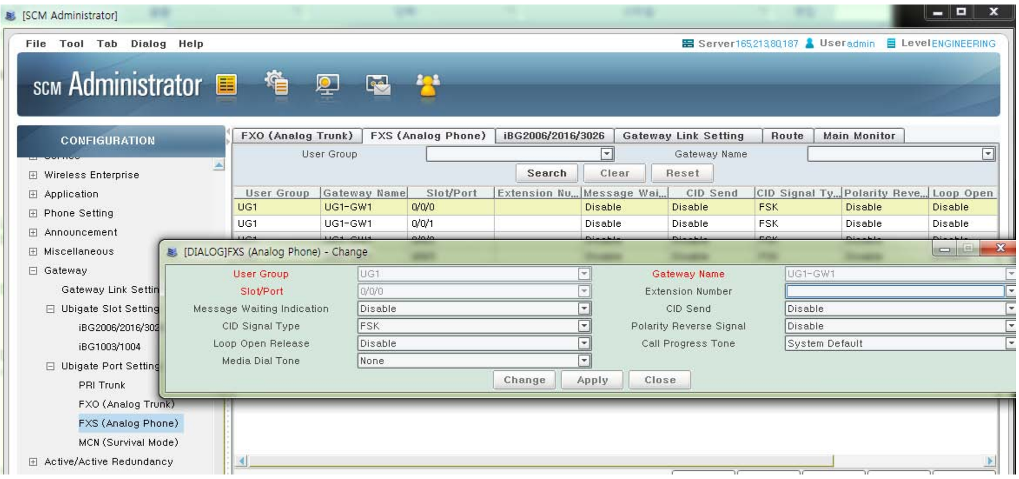
Diversion Userinfo Select

Select to whether to use the userinfo (sip:userinfo@domain) of Diversion header as Caller ID.

- disable
- enable

5.3.3.2 Configuring FXS ports

This section describes the configuration of analog FXS voice ports.
Selects an FXS port which you want to configure in the following window, and press change button and select change.
Change configurations of the FXS port, in the following window you can change items except User Group, Slot/Port and Gateway Name.



User Group	Gateway Name	Slot/Port	Extension Nu...	Message Wai...	CID Send	CID Signal Ty...	Polarity Reve...	Loop Open
UG1	UG1-GW1	0/0/0		Disable	Disable	FSK	Disable	Disable
UG1	UG1-GW1	0/0/1		Disable	Disable	FSK	Disable	Disable

User Group	UG1	Gateway Name	UG1-GW1
Slot/Port	0/0/0	Extension Number	
Message Waiting Indication	Disable	CID Send	Disable
CID Signal Type	FSK	Polarity Reverse Signal	Disable
Loop Open Release	Disable	Call Progress Tone	System Default
Media Dial Tone	None		

Message Waiting Indication (MWI)

To enables/disables MWI for a specified FXS voice port, use the ‘Message Waiting Indication’ menu in FXS port configuration window.

- Disable: Disables MWI
- Audible: Enables audible MWI
- Visible: Enables visible MWI

CID Signal Type

To selects type of caller ID for a specified FXS voice port, use the ‘CID Signal Type’ menu in FXS port configuration window.

- FSK: Using FSK type for sending and receiving the caller ID. This is the most common setting. (default)
- DTMF: Using DTMF type for sending and receiving the caller ID.

Loop Open Release

To enables/disables a supervisory disconnect signal on an FXS port, use the ‘Loop Open Release’ menu in FXS port configuration window.

Extension Number

To sets extension number of an FXS port, use the ‘Extension Number’ menu in FXS port configuration window.

CID Send

To enables/disables allowance of sending of caller ID information for a specified FXS port, use the ‘CID Send’ menu in the FXS port configuration window.

Polarity Reverse Signal

To enables/disables battery polarity reversal function, use the ‘Polarity Reverse Signal’ menu in the FXS port configuration window.

Call Progress Tone

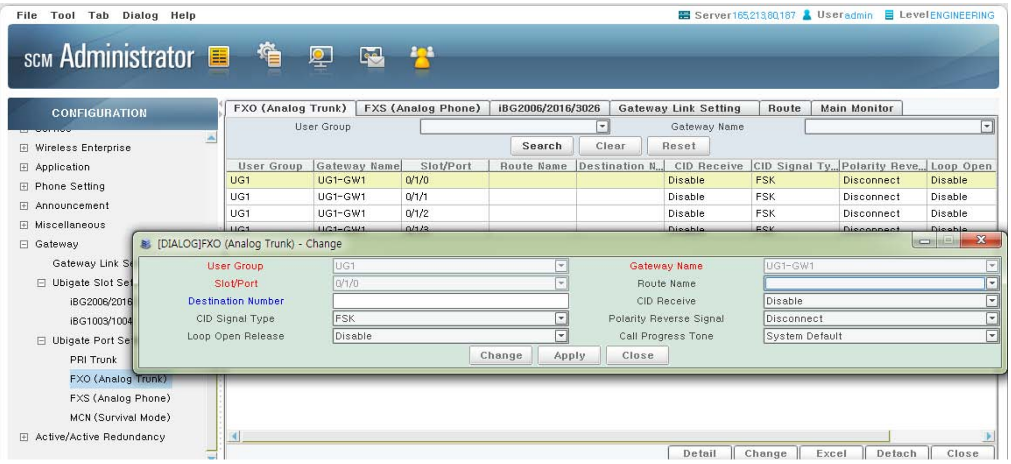
To specify a regional analog voice-interface-related call progress tone, use the ‘Call Progress Tone’ menu in the FXS port configuration window.

- Korea
- USA/Canada
- Britain
- Italy
- Germany
- Russia
- Australia

5.3.3.3 Configuring FXO ports

This section describes the configuration of analog FXO voice ports.
Selects an FXO port which you want to configure in the following window, and press change button and select change.

Change configurations of the FXO port, in this window you can change items except User Group, Slot/Port, Link State and Gateway Name.



User Group	Gateway Name	Slot/Port	Route Name	Destination N...	CID Receive	CID Signal Ty...	Polarity Reve...	Loop Open
UG1	UG1-GW1	0/1/0			Disable	FSK	Disconnect	Disable
UG1	UG1-GW1	0/1/1			Disable	FSK	Disconnect	Disable
UG1	UG1-GW1	0/1/2			Disable	FSK	Disconnect	Disable
UG1	UG1-GW1	0/1/3			Disable	FSK	Disconnect	Disable

[DIALOG]FXO (Analog Trunk) - Change

User Group	UG1	Gateway Name	UG1-GW1
Slot/Port	0/1/0	Route Name	
Destination Number		CID Receive	Disable
CID Signal Type	FSK	Polarity Reverse Signal	Disconnect
Loop Open Release	Disable	Call Progress Tone	System Default

Destination Number

To selects destination number of plar, use ‘Destination Number’ menu in FXO port configuration window. PLARs (switched) connections enable the user to make a call without dialing any digits.

CID Signal Type

To selects type of caller ID for a specified FXO voice port, use the ‘CID Signal Type’ menu in FXO port configuration window.

- FSK: Using FSK type for sending and receiving the caller ID. This is the most common setting. (default)
- DTMF: Using DTMF type for sending and receiving the caller ID.

Loop Open Release

To enables/disables a supervisory disconnect signal on an FXO port, use the ‘Loop Open Release’ menu in FXO port configuration window.

Route Name

To selects name of an FXO trunk, use ‘Route Name’ menu in the FXO port configuration window.

CID Receive

To enables/disables allowance of receiving of caller ID information for a specified FXO port, use the ‘CID Receive’ menu in the FXO port configuration window.

Polarity Reverse Signal

To enables/disables battery polarity reversal function, use the ‘Polarity Reverse Signal’ menu in the FXO port configuration window.

- Disconnect: Enables Polarity Reverse Signal to detect disconnect
- Disconnect-Answer: Enables Polarity Reverse Signal to detect disconnect and answer.
- Disable: Disables Polarity Reverse Signal detection.

Call Progress Tone

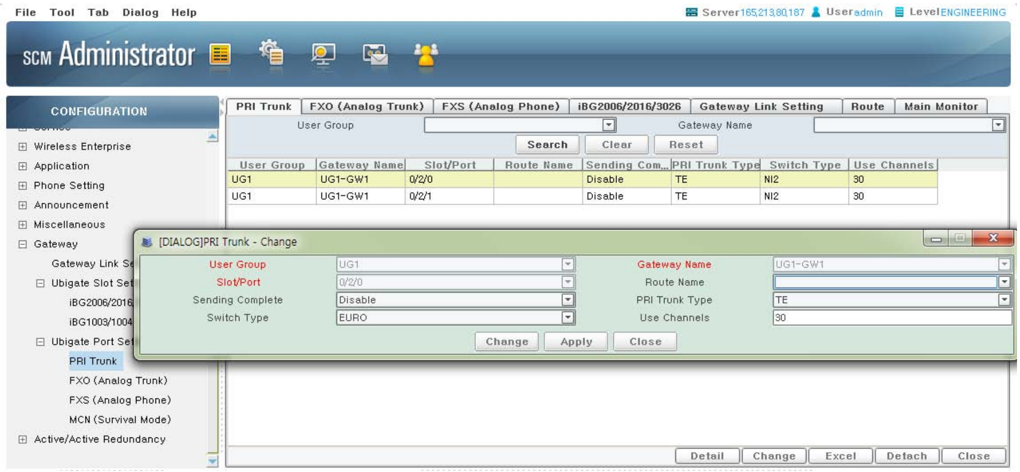
To specify a regional analog voice-interface-related call progress tone, use the ‘Call Progress Tone’ menu in the FXO port configuration window.

- Korea
- USA/Canada
- Britain
- Italy
- Germany
- Russia
- Australia

5.3.3.4 Configuring PRI trunk

This section describes the configuration of ISDN-PRI trunks.
Selects an ISDN-PRI trunk which you want to configure in the following window, and press change button and select change.

Change configurations of the ISDN-PRI trunk, in this window you can change items except User Group, Slot/Port and Gateway Name.



User Group	Gateway Name	Slot/Port	Route Name	Sending Com...	PRI Trunk Type	Switch Type	Use Channels
UG1	UG1-GW1	0/2/0		Disable	TE	NI2	30
UG1	UG1-GW1	0/2/1		Disable	TE	NI2	30

[DIALOG]PRI Trunk - Change

User Group	UG1	Gateway Name	UG1-GW1
Slot/Port	0/2/0	Route Name	
Sending Complete	Disable	PRI Trunk Type	TE
Switch Type	EURO	Use Channels	30

Sending Complete

To enables/disables sending complete options parameter, use ‘Sending Complete’ item in the PRI Trunk-Change window.

Switch Type

To selects switch type, use ‘Switch Type’ menu in the PRI Trunk-Change window.

- N12
- DMS100
- NTT
- QSIG
- DMS250
- EURO
- CCITT
- 4ESS
- 5ESS
- AUS

Route Name

To selects name of an ISDN-PRI trunk, use ‘Route Name’ menu in the PRI Trunk-Change window.

PRI Trunk Type

To selects type of PRI trunk, use ‘PRI Trunk Type’ menu in the PRI Trunk-Change window

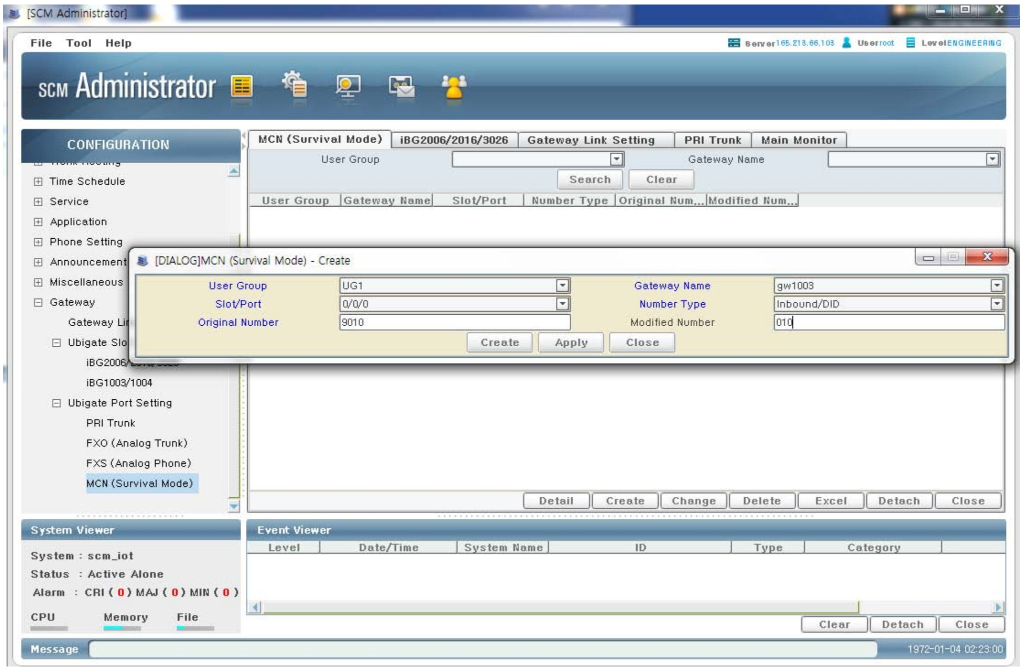
- TE
- NT

Use Channels

To sets number of channels, use ‘Use Channels’ menu in the PRI Trunk-Change window.

5.3.3.5 Configuring MCN

This section describes the configuration of MCN (Survival Mode).
Press Create button to make a MCN rule for survival mode of the gateway. MCN translates an original number into modified number when a call is incoming or outgoing on the specific port. This works only for survival mode of the gateway.



[DIALOG]MCN (Survival Mode) - Create

User Group: UG1
Gateway Name: gw1003
Slot/Port: 0/0/0
Number Type: Inbound/DID
Original Number: 9010
Modified Number: 010

Create Apply Close

System Viewer
System : scm_iot
Status : Active Alone
Alarm : CRI (0) MAJ (0) MIN (0)

5.3.4 Connecting to SCM Server

Before setting iBG, you must configure SCM in advance. Here is the essential information to start configuration:

- IP address, port number, and transport type of SCM
- Domain name
- gw-uri name
- FXS subscriber's number and password
- Trunk URI name if it needs to register the trunk

gw-uri is a representative name of Ubigate iBG and SCM maintains iBG as an Endpoint.
Domain name of iBG must be same with SCM's configuration.
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.
You should shutdown voip-gateway before configuring call-server, and the VoIP gateway source address must be set in advance.
You can set the call server in the following ways:

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	Shuts down voip call services
4	bind control interface *type num* Example) /configure/voip-gateway# bind control interface ethernet 0/0	Sets source interface for SIP
5	bind media interface *type num* Example) /configure/voip-gateway# bind media interface ethernet 0/0	Sets source interface for media

(Continued)

Step	Command	Purpose
6	host domain-name *DOMAIN.COM* Example) /configure/voip-gateway# host domain-name scme.com	Sets domain name
7	call-server ip-address *ip-addr* [udp | tcp | tls] [sip | sips] [expires *expires*] [retry *retry*] Example) /configure/voip-gatway# call-server ip-address ipv4:90.90.90.100	Sets a SCM IP Address. Expires and retry timer for FXS subscribers and trunks may be set. Use voice service SIP global configuration for transport type and uri.
8	call-server ip-address *ip-addr* [udp | tcp | tls] [sip | sips] [expires *expires*] [retry *retry*] secondary Example) /configure/voip-gatway# call-server ip-address ipv4:90.90.90.101 secondary	Sets secondary SCM server IP Address. Expires and retry timer for FXS subscribers and trunks may be set. Use voice service SIP global configuration for transport type and uri.
9	call-server gw-uri *uri* [expires *expires*] [retry *retry*] Example) /configure/voip-gateway# call-server gw-uri iBG2016	Set gw-uri and Ubigate iBG will register to SCM as an Endpoint. Expires and retry timer of GW-URI may be set.
10	no shutdown	Enables voip call services
11	exit Example) /configure/voip-gateway# exit	Exits the current mode.

5.3.5 Updating Gateway Software

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

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.

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

CHAPTER 6. Installing SIP Phones

6.1 Connecting SIP Phones

6.1.1 Safety Precautions

To reduce the risk of personal injury, follow these precautions before connecting telephone circuits:
Never install telephone wiring during a lightning storm.
Never install telephone jacks in a wet location unless the jack is specifically designed for wet locations.
Do not connect stations in a humid area.
Never touch non-insulated telephone wires or terminals unless the telephone line has been disconnected at the network interface.
Connect stations using #24 AWG or #26 AWG cables.

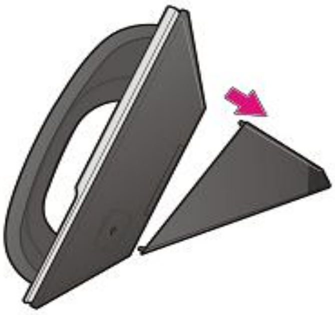
6.1.2 Wall-Mounting SMT-i5200 Keysets

Assemble the wall-mount bracket where you want to use the phone. The wall-mount bracket is an optional item.

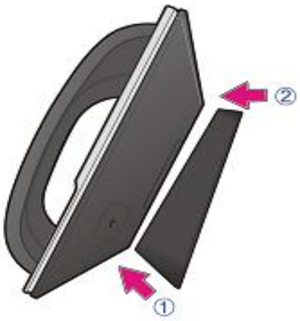
6.1.2.1 To install the wall-mounting bracket follow the steps below:

1) First, choose the location where you want to install the phone, and then determine the positions of the screws by placing the phone at the target location on the wall.

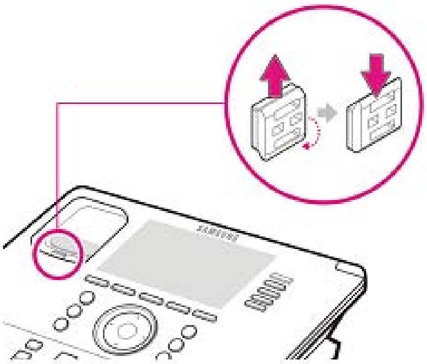
2) Remove the base wedge of the phone.
   a) Fix one latch of the base wedge to the top or bottom groove of the phone.
   b) Push the remaining latch into the remaining groove on the opposite side.



3) Insert the wall-mount bracket as shown in the figure.



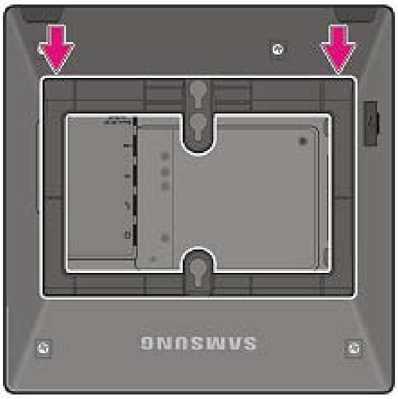
4) Pull out the handset retainer, and then insert it in the opposite direction, as shown in the figure.
Only the up-down direction changes.
The front-back remains unchanged.



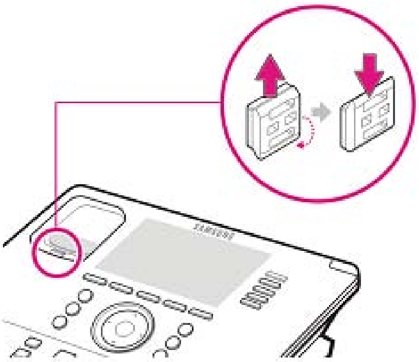
5) Install the phone on the wall.

6.1.2.2 To detach the wall-mounting bracket follow the steps below:

1) You can detach the phone from the bracket by pressing the **[Push]** section at the bottom of the bracket.
   Detach the phone more easily by pulling the entire bottom of the bracket instead of only the **[Push]** section.



2) Pull out the handset retainer, change the direction and then insert it again.



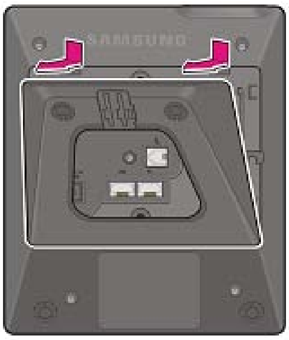
6.1.3 Wall-Mounting SMT-i3105 Keysets

The SMT-i3105 keysets do not require an optional wall-mounting bracket. Reverse the base wedge to serve as the wall mount bracket.

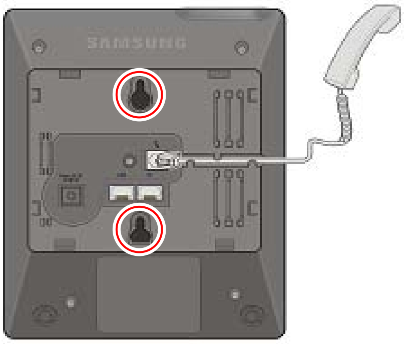
6.1.3.1 To wall-mount the SMT-i3105 follow the steps below:

1) First, choose the location where you want to install the phone, and then determine the positions of the screws by placing the phone at the target location on the wall.

2) Remove the base wedge of the phone by pressing the **[Push]** mark on the top of the wedge to push it out

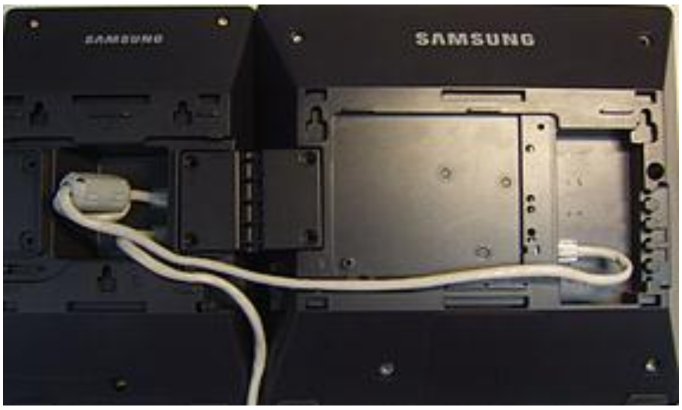


3) Use screw holes 1 and 2 to attach the base wedge to a standard electrical outlet box.



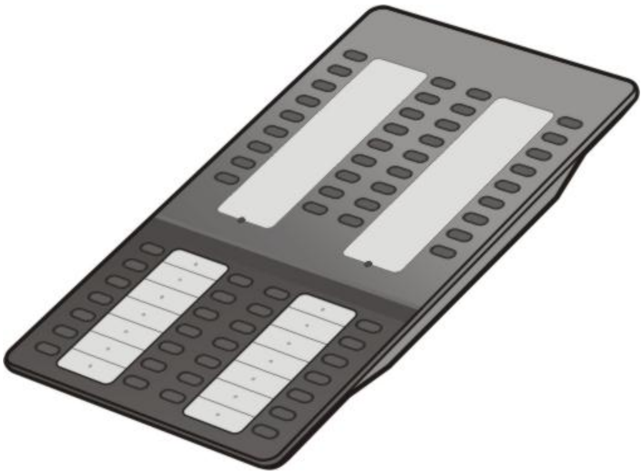
6.1.4 SMT-i5264 Add-On Module

The SMT-i5264 Add-On Module only attaches to SMT-i5200 series.
If PoE is used, PoE connection should be connected to the LAN port of the SMT-i5264 first then transfer over to the phone. As shown in following figure the SMT-i5264 can transfer the power from the LAN port to the phone port, but the phone can’t transfer power to the AOM.



6.1.4.1 Setting-Up SMT-i5264 AOM

SMT-i5264 AOM will register to an SIP phone device. The SMT-i5264 will receive an SIP phone extension. It can be paired to any SIP phone as the add-on module.



6.1.5 Connecting the SMT-A52GE Gigabit Adaptor

The Gigabit Adaptor processes the Gigabit data for a Gigabit LAN connection on the PC connected to the SMT-i5200 series IP phone.

6.1.5.1 COMPONENTS

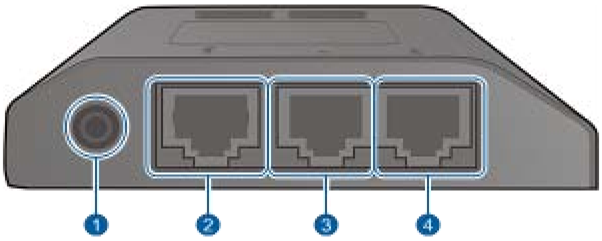
The SMT-A52GE comes with the following components:

Gigabit Adaptor

2 Fixing Screws

LAN Cable

6.1.5.2 CONFIGURATION AND FUNCTIONS



Port	Function
qQPower (DC 5 V)	DC power adaptor connection port
wQIP Phone PSE	- A port connected to the IP phone's LAN port via the LAN cable. This is shipped together with the Gigabit Adaptor (10/100BASE-TX) - If PoE (Power over Ethernet) is provided via the G-LAN PD port, it supplies PoE to the IP phone.
eQG-PC	LAN cable port connected to the PC (10/100/1000BASE-T)
rQG-LAN PD	- LAN cable port connected to the network (10/100/1000BASE-T) - If PoE is supplied via the LAN, a power supply is not required for the IP phone or adaptor.

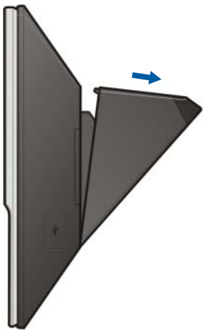
NOTE

DC power adaptor is not included.

6.2 Connecting to Network

6.2.1 How to connect to a phone

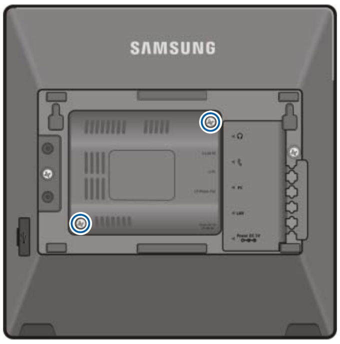
1) Separate the base wedge at the back of the phone.



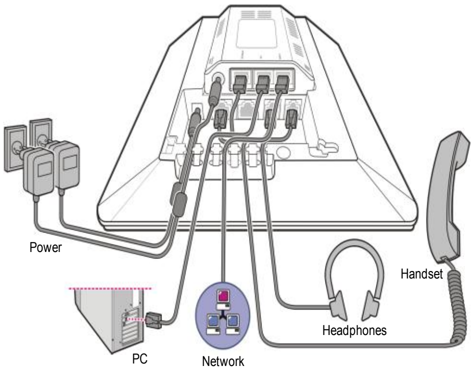
2) Mount the Gigabit Adaptor onto the back of the body.

NOTE

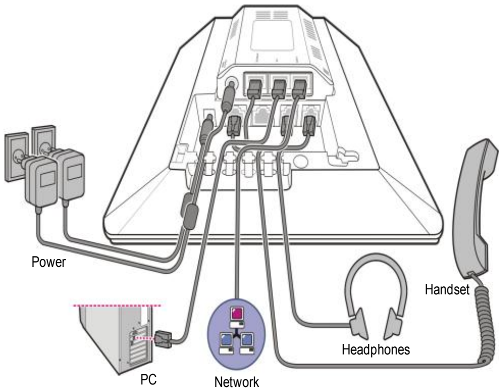
The back of the Gigabit Adaptor is sharp, so take care to avoid injury. When you connect the Gigabit Adaptor to the IP phone which is currently in use, disconnect the PC cable connected to the IP phone, and connect it to the G-PC port of the Gigabit Adaptor. This will leave the PC connection port, usually used for the IP phone, vacant.



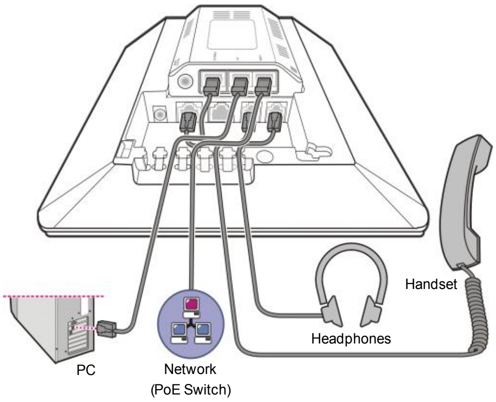
3) Connect the cable.
When PoE is supplied via the LAN:



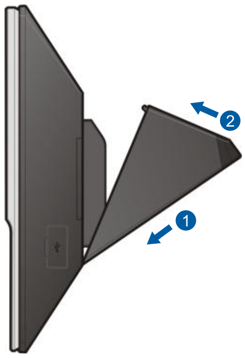
4) Connect the cable.
When PoE is supplied via the LAN:



When PoE is not supplied via the LAN:



5) Attach the base wedge to the back of the phone.



6.3 Connecting to SCM Server

The User can configure the register information and the network information easily, when the phone is not registered with the system.

> ⚠ **WARNING**
>
> If you enter the wrong information in the easy install menu, the phone may not be registered with a system or cannot connect to the network. You should enter the information correctly provided from the system administrator.

6.3.1 Configuration Type

The SMT-i5200 and SMT-i3100 series SIP phones support 3 types of configuration methods.

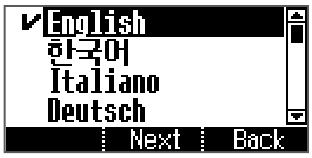
Config. Type	Description
Standard	User can configure all the information to register with system manually. This mode is including following steps. - SIP server setting - SIP authentication setting - NTP server setting
Server	All the information to register with system is downloaded from a Configuration server. - If the system using MAC Address authentication type, ID/Password is not mandatory. - Please contact the system administrator detail information about the phone authentication type.
PnP (Plug & Play)	This feature allows a phone to be registered with the system when powered on so that it becomes available for service. - To use the **[PnP]** mode, the PnP environment must be configured by the system administrator. - If you choose the **[PnP]** mode, the network mode of the phone is changed to DHCP and the network setting step is skipped. - Please contact the system administrator about detail information about the **[PnP]** mode.

6.3.2 Easy Installation of SMT-i3105/5210/5230

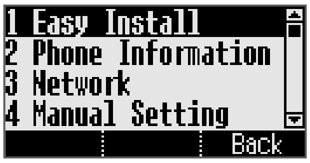
1) To get to the SETUP MODE unplug the power cord from the phone. Press and hold the * button while you plug power back into the phone. Release the * button when you see Samsung in the display.

When the phone reboot is complete, the Language Menu will display. Select the language to use and press the Next soft button to advance to the Configuration Menu.

- The system administrator can change the language of the phone after registered with the system.



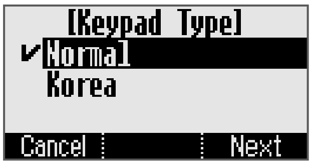
2) Select the **[1 Easy Install]** Menu.



3) Select the Keypad Type.

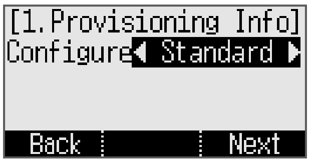
- In case of use Korean language, select Korea, in other case select Normal.

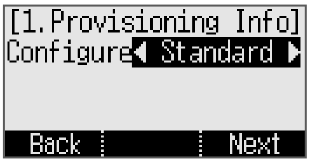
Press the **[Next]** Button.

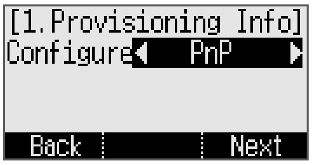


4) Select the configuration mode. The steps of the easy install menu might be changed depending on type of the configuration mode.

Press the **[Next]** Button.

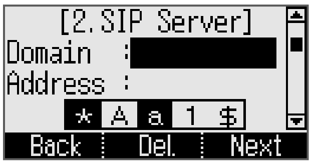

[1.Provisioning Info]
Configure◀ Standard ▶

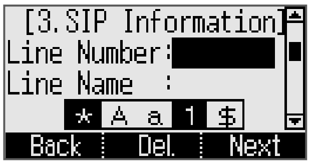

[1.Provisioning Info]
Configure◀ Standard ▶

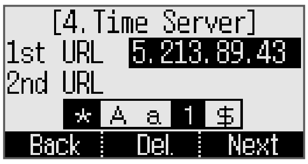

[1.Provisioning Info]
Configure◀ PnP ▶

5) If the **[Standard]** configuration mode is selected, The following steps are added.
- SIP Server: Enter the SIP server information.
- SIP Register Information: Enter the sip register information.
- Time Server: Enter the time server (NTP) URL and update interval.

Press the **[Next]** Button.

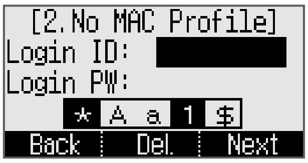

[2.SIP Server]
Domain :
Address :

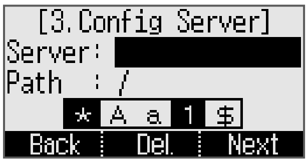

[3.SIP Information]
Line Number:
Line Name :


[4.Time Server]
1st URL 5.213.89.43
2nd URL

6) In case the **[Server]** configuration mode is selected, You can enter ID/Password.
- If the system using MAC Address authentication type, ID/Password is not mandatory.
- Please contact the system administrator detail information about the configuration server address and authentication type.

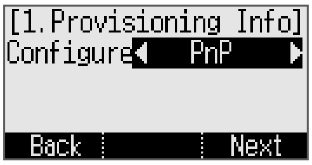
Press the **[Next]** Button.


[2.No MAC Profile]
Login ID:
Login PW:


[3.Config Server]
Server:
Path : /

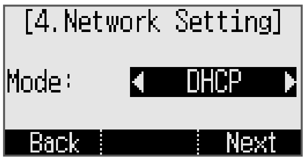
7) In case the **[PnP]** configuration mode is selected, There is nothing to do in this step.
- Please contact the system administrator about detail information about the PnP mode.

Press the **[Next]** Button.


[1.Provisioning Info]
Configure ◀ PnP ▶

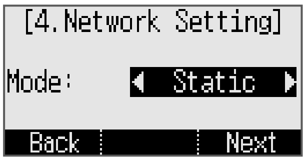
8) Select the network mode and enter detail network information.

- If you choose the PnP configuration mode, the Network mode of the phone is changed to DHCP and the Network Setting step is skipped in the easy Install feature.
- If you enter the wrong information, the phone may not be registered with a system or cannot connect to the network.



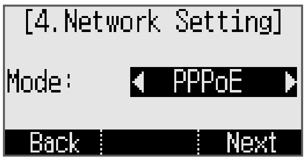
[4.Network Setting]

Mode: ◀ DHCP ▶



[4.Network Setting]

Mode: ◀ Static ▶

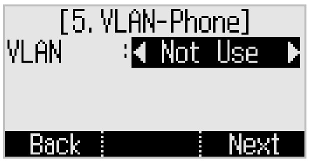


[4.Network Setting]

Mode: ◀ PPPoE ▶

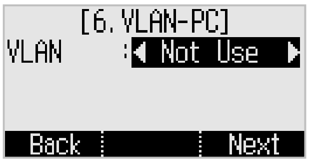
9) Enter VLAN information.

- If you enter the wrong information, the phone may not be registered with a system or cannot connect to the network.



[5.VLAN-Phone]

VLAN :◀ Not Use ▶

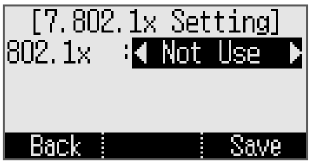


[6.VLAN-PC]

VLAN :◀ Not Use ▶

10) Enter 802.1x information

- If you enter the wrong information, the phone may not be registered with a system or cannot connect to the network.

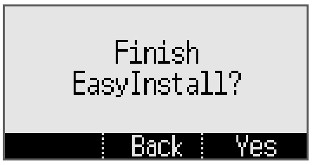


[7.802.1x Setting]

802.1x :◀ Not Use ▶

11) All steps of the easy install is ended, press the **[Yes]** button to finish the easy install. Then the phone will be restart.

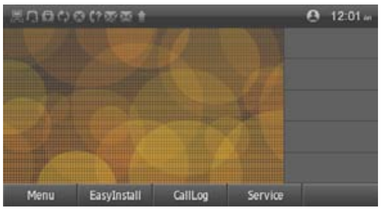
- You can change the information already entered. Press the **[Back]** button till the step you want, and edit the information

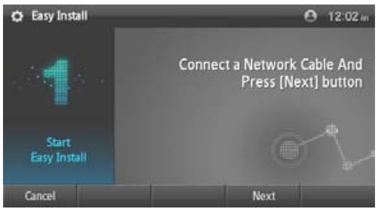


Finish
EasyInstall?

6.3.3 Easy Installation of SMT-5243

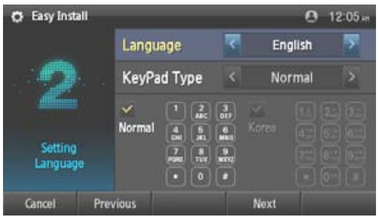
1) In case the phone is not registered with the system, **[Easy Install]** button will be displayed. Press **[Easy Install]** button, then the easy install menu will be shown. Check a network cable and press **[Next]** button.





Connect a Network Cable And Press [Next] button

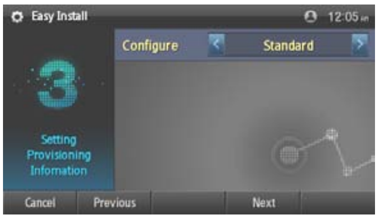
2) Select the language to use.
   - The system administrator can change the language of the phone after registered with the system.



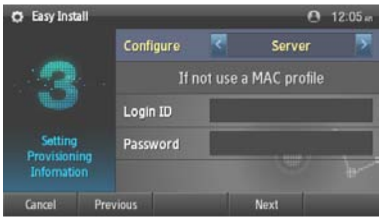
Language English

KeyPad Type Normal

3) Select the configuration mode. The steps of the easy install menu might be changed depending on type of the configuration mode.
   Press the **[Next]** Button.



Configure Standard

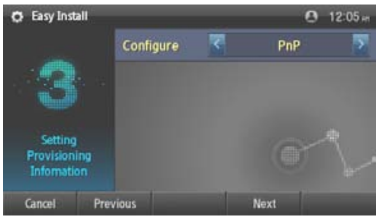


Configure Server

If not use a MAC profile

Login ID

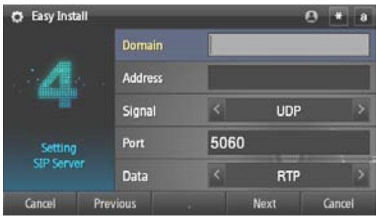
Password

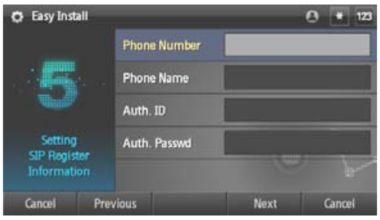


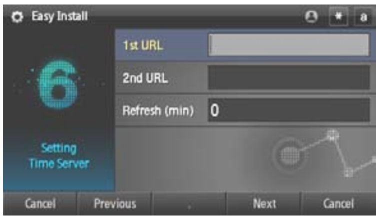
Configure PnP

4) If the **[Standard]** configuration mode is selected, the following steps are added.
   - SIP Server: Enter the SIP server information.
   - SIP Register Information: Enter the sip registration information.
   - Time Server: Enter the time server (NTP) URL and update interval.

   Press the **[Next]** Button.

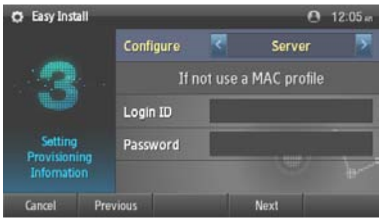


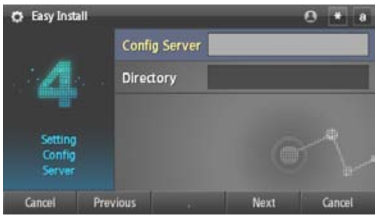




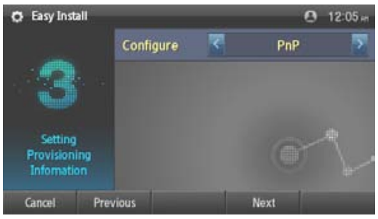
5) In case the **[Server]** configuration mode is selected, You can enter ID/Password.
   - If the system using MAC Address authentication type, ID/Password is not mandatory.
   - Please contact the system administrator detail information about the configuration server address and authentication type.

   Press the **[Next]** Button.



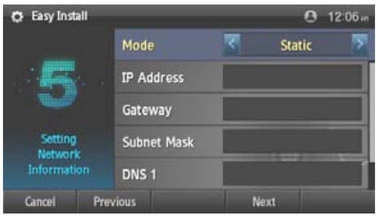


6) In case the **[PnP]** configuration mode is selected, There is nothing to do in this step. Press the **[Next]** Button.
   - Please contact the system administrator about detail information about the PnP mode.



7) Select the network mode and enter detail network information.

- If you choose the PnP configuration mode, the Network mode of the phone is changed to DHCP and the Network Setting step is skipped in the easy Install feature.
- If you enter the wrong information, the phone may not be registered with a system or cannot connect to the network.



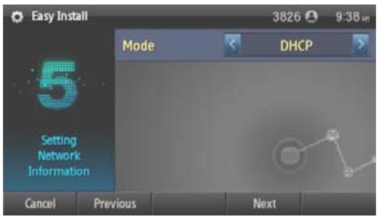
Mode Static

IP Address

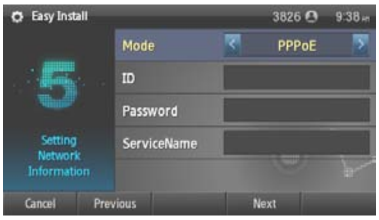
Gateway

Subnet Mask

DNS 1



Mode DHCP



Mode PPPoE

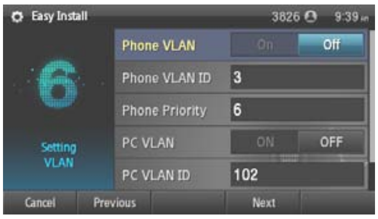
ID

Password

ServiceName

8) Enter VLAN information.

- If you enter the wrong information, the phone may not be registered with a system or cannot connect to the network.



Phone VLAN On Off

Phone VLAN ID 3

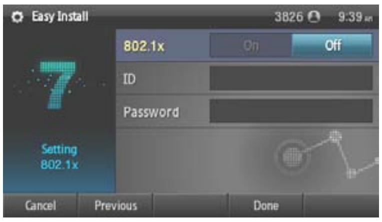
Phone Priority 6

PC VLAN ON OFF

PC VLAN ID 102

9) Enter 802.1x information

- If you enter the wrong information, the phone may not be registered with a system or cannot connect to the network.



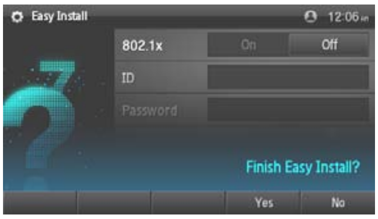
802.1x On Off

ID

Password

10) All steps of the easy install is ended, press the **[Finish]** button to finish the easy install. Then the phone will be restart.

- You can change the information already entered. Press the **[Previous]** button till the step you want, and edit the information.



Easy Install

802.1x: Off

ID

Password

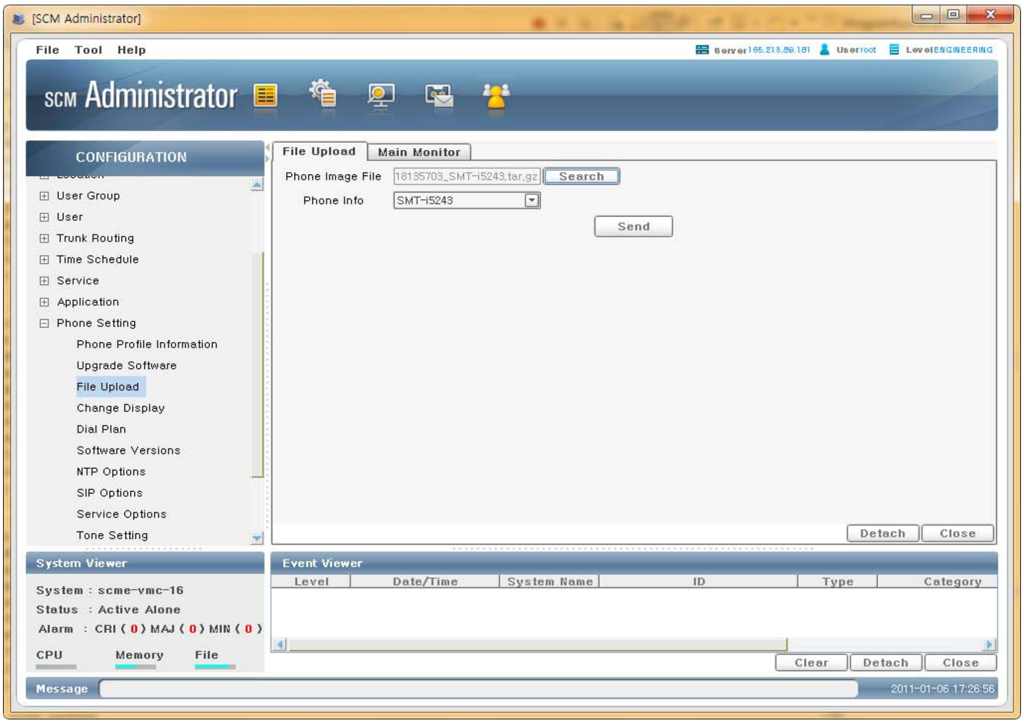
Finish Easy Install?

6.4 Upgrading SIP Phone Software

When you need upgrading SIP phone software, follow by these steps.

1) **Preparing Software**
   First of all, you should copy phone software image file to your local PC.

2) **Uploading Package**
   You can upload the phone software image file using **[CONFIGURATION > Phone Setting > File Upload]** menu.



Server 165.213.89.181 User root Level ENGINEERING

Phone Image File: 18135703_SMT-i5243.tar.gz

Phone Info: SMT-i5243

System : scme-vmc-16
Status : Active Alone
Alarm : CRI (0) MAJ (0) MIN (0)

2011-01-06 17:26:56

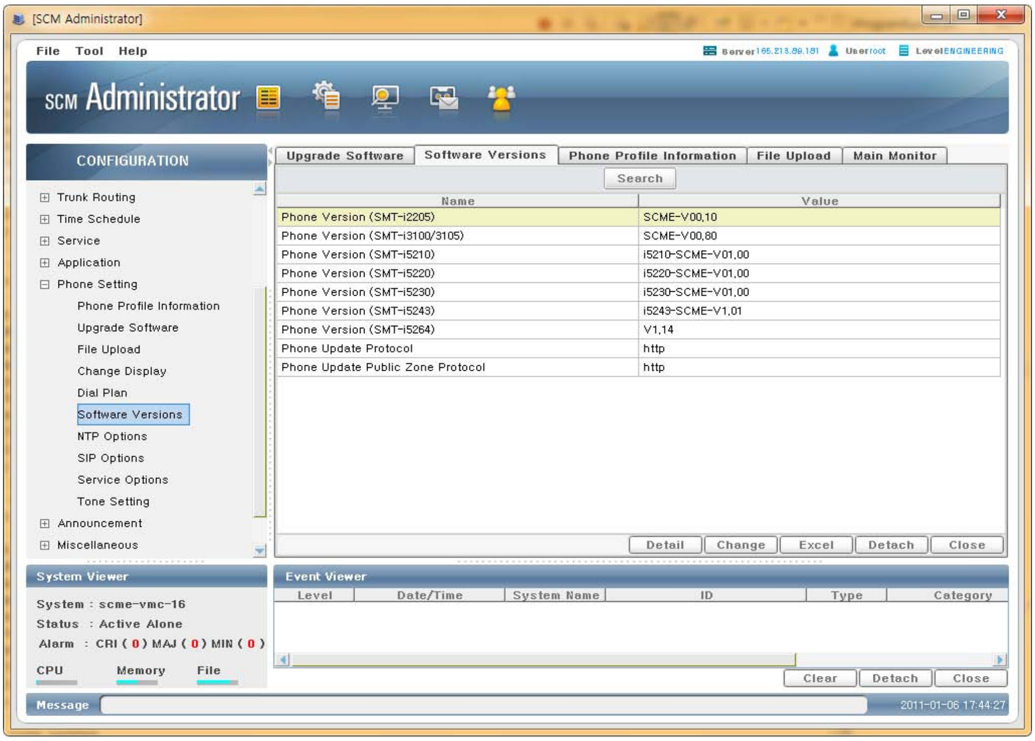
You can upload the phone software image file to SCM following steps:

① Click Search button.
② Select Upgrade phone software image
③ Check Phone name in Phone Info category.
④ Click Send button.

The Phone software image sends to SCM and copy to pre-defined directory in system automatically.

3) Check Software Version

You can check the phone software information using **[CONFIGURATION > Phone Setting > Software Versions]** menu.



Name	Value
Phone Version (SMT-i2205)	SCME-V00,10
Phone Version (SMT-i3100/3105)	SCME-V00,80
Phone Version (SMT-i5210)	i5210-SCME-V01,00
Phone Version (SMT-i5220)	i5220-SCME-V01,00
Phone Version (SMT-i5230)	i5230-SCME-V01,00
Phone Version (SMT-i5243)	i5243-SCME-V1,01
Phone Version (SMT-i5264)	V1,14
Phone Update Protocol	http
Phone Update Public Zone Protocol	http

System Viewer
System : scme-vmc-16
Status : Active Alone
Alarm : CRI (0) MAJ (0) MIN (0)
CPU Memory File

2011-01-06 17:44:27

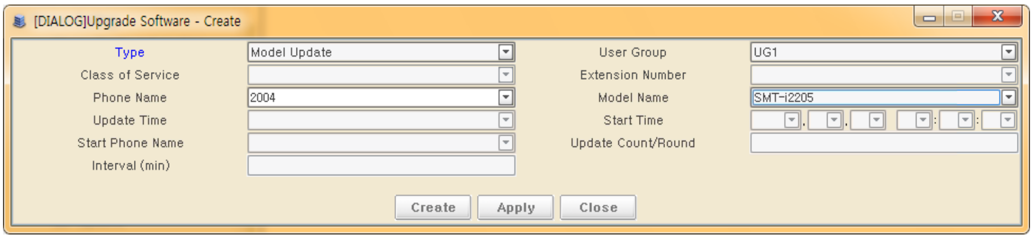
4) Upgrading Software

You can upgrade the phone software using **[CONFIGURATION > Phone Setting > Upgrade Software]** menu.

First of all, press Create button then pop-up following window.

In Dialog box, select Type to Model Update, User Group, Phone Name, Model Name and Extension Number.

After click Apply button, phone will reboot automatically and start upgrade process.



Type	Model Update	User Group	UG1
Class of Service		Extension Number	
Phone Name	2004	Model Name	SMT-i2205
Update Time		Start Time	
Start Phone Name		Update Count/Round	
Interval (min)			

You can use scheduled upgrade for multiple phones in this menu.

ABBREVIATION

C

CLI	Command Line Interface
CPU	Central Processing Unit

D

DDR	Double Data Rate
DVD	Digital Video Disc

F

FTP	File Transfer Protocol

H

HA	High Availability
HDD	Hard Disk Drive

I

IP	Internet Protocol

L

LAN	Local Area Network

O

ODD	Optical Disc Drive

R

RAM	Random Access Memory
ROM	Read Only Memory

S

SCM	Samsung Communication Manager

SCM

System Description

Copyright 2013

Samsung Telecommunications America

All rights reserved. No part of this manual may be reproduced in any form or by any means-graphic, electronic or mechanical, including recording, taping, photocopying or information retrieval systems – without express written permission of the publisher of this material.