

T A B L E O F C O N T E N T S

USER INSTRUCTIONS

PART	DESCRIPTION
------	-------------

- | | |
|--------------------------|--|
| <u>1</u> | <u>Dual-Band AP Quick Set-Up Guide</u> |
| <u>2</u> | <u>Quick Software Upgrade Guide for Dual-Band AP & WIP-5000M</u> |
| <u>3</u> | <u>WIP-5000M Quick Reference Guide</u> |
| <u>4</u> | <u>WIP-5000M User Guide</u> |
| <u>5</u> | <u>SMT-R2000 User Manual</u> |

Dual Band AP (SMT-R2000)

Quick Set-Up Guide

Set-Up Process:

- Site survey to determine the location of APs and the required APs.
- Program each AP for the country code, SSID, RF channel, IP addresses, security, etc.
- Program system for dual band AP type, enable registration, and handset IP addresses, etc.
- Connect one AP and register all handsets.
- Installed other APs to the desirable locations.
 - a. Note: The distance for the IP connection is about 300 ft. Data switches will be required for the distance over the limit.

1: System Components

1. Load OfficeServ 500 or OfficeServ 100 or OS 7200 system with MCP2 software version 2.6x or up. OS 7400 with MP40 software version 3.25 and up.
2. Connect both MCP and MGI to the same data network and have the IP addresses programmed.
3. Connect the **WAN** port of dual band APs (SMT-R2000) to the same data (subnet) network.
4. Power on the system.
5. Power on AP either through the power adaptor or PoE switch.

2: Pre-determinate the following data

1. System IP address
2. System Gateway IP address
3. WLAN SSID
4. AP IP addresses (can be different that the system subnet but must be unique for each AP)
5. AP RF channels (frequency planning)
6. AP external antenna on or off
7. Handset IP addresses
8. Static WIP IP registration enable or disable
9. WEP key enable or disable

For example:

Sample Configuration Table (3 APs + 4 Handsets)

1. System IP: 165.213.97.185
2. MGI IP: 165.213.97.190
3. System gateway: 165.213.97.1

- 4. System ID: 123456 (must be numeric, max 6 digits)
- 5. AP TX Power: 100% (max)
- 6. AP1 IP: 192.168.111.11
- 7. AP1 RF CH: 1
- 8. AP2 IP: 192.168.111.12
- 9. AP2 RF CH: 6
- 10. AP3 IP: 192.168.111.13
- 11. AP3 RF CH: 11
- 12. Handset 1 IP: 165.213.97.101
- 13. Handset 2 IP: 165.213.97.102
- 14. Handset 3 IP: 165.213.97.103
- 15. Handset 4 IP: 165.213.97.104
- 16. WEP key: Disable
- 17. Static WIP Reg: Enabled
- 18. CODEC: G729

3: Programming System Data Base

Note: Skip any MMC field that is not mentioned.

1. Enter the technician mode (MMC 800, pw: 4321).
2. MMC 830
 - a. Verify the desirable system IP and gateway address are in place.
e.g.
System IP: 165.213.97.185 Gateway: 165.213.97.1
3. MMC 831
 - a. Make sure at least one MGI card is in the system and the ITP phones and MGI IP addresses are not conflict with handset IP addresses.
4. MMC 849
 - a. Use password "0000" to enter.
[ENTER PASSWORD]
[0000]
 - b. Select "Dual AP" type.
[SELECT AP TYPE]
[DUAL AP]

Note: System will restart and erase all existing wireless data. Data from MMC 845 to MMC 849 will be reset to the factory default. After system comes back, go back to the MMC 849 and continue the following:
 - c. Enable VoWLAN registration.
[REGISTER VoWLAN]
[ENABLE]
 - d. Enable Static IP handset registration.
[STATIC WIP IP]
[ENABLE]
5. MMC 848
 - a. Set handset IP address for each handset.
[IP: 001 USED:]
[165. 213. 97. 101]

4: Programming SMT-R2000

Note: It takes about 1 minute to reboot the SMT-R2000.

1. Set IP address of the PC to the same subnet address range of SMT-R2000.

- a. Ex. Set PC to the following:
 - i. IP: 192.168.111.5
 - ii. SM: 255.255.255.0
2. Connect PC to the SMT-R2000 via LAN or WLAN
 - a. For LAN:
 - i. Connect a data cable to the **LAN port** of the SMT-R2000
 - b. For WLAN:
 - i. Factory default SSID is **SMT-R2000-WLAN1** (802.11b/g)
3. Make sure the SMT-R2000 is in idle state. It takes about 1 minute from power on to idle state. The following LED shows idle state.
 - a. WAN: ON
 - b. LAN: OFF
 - c. 2.4GHz: flashing
 - d. 5GHz: flashing
 - e. PWR: ON
4. Access the Web management page of the SMT-R2000 by using "Internet Explorer"
 - a. The default setting of SMT-R2000:
 - i. IP: **192.168.111.10**
 - ii. ID: admin
 - iii. PW: samsung
 - b. Using "ping 192.168.111.10" to confirm the connectivity.
5. Select country code and click [Update]
6. Under [Basic Setting]
 - a. Optional
 - i. Time Compensation: -6(CH)
 - ii. Location: AP1 (or AP2, etc.)
 - b. Must change
 - i. IEEE 802.11b/g (SSID): 123456
 1. Current software version of WIP-5000M requires numeric SSID.
 - c. Click [Update]
7. Under [Manage],
 - a. [Ethernet Setting]
 - i. WAN Interface Settings
 1. Static IP Address: 192.168.111.11 (Must use different address for each AP)
 - b. [Wireless Setting]
 - i. Radio Interface 2, Mode: IEEE 802.11g
 1. Channel: 1 (set the desirable channel)
 - c. Click [Update]
8. Repeat above steps for all APs.

5: Programming Handsets (WIP-5000M)

1. Handset Registration

- b. Need to un-register first, if handsets have previous registration data.
 - i. Press <menu>, <6>, <3>, <password> (default 1234), <1> to un-register.

- b. Enter the following info to register the handset:

- i. Press <Menu>.
- ii. Select <6> for System.
- iii. Select <1> for Registration.
- iv. Select <1> for System 1.
- v. Select <2> for Static IP mode.
- vi. Select <1> for Basic Type AP
- vii. Enter handset IP address and press <OK>
 - i. e.g. 165.213.97.101 (use "*" for ".")

Note: DO NOT ENTER LEADING 0 FOR IP ADDRESS. EX. Enter 165.213.97.101 not 165.213.097.101.

viii. Enter System IP address, e.g. 165.213.97.185, and press <OK>.

ix. Enter System Gateway, e.g. 165.213.97.1, and press <OK>.

x. Enter System Netmask, e.g. 255.255.255.0, and press <OK>.

xi. Enter System SSID, e.g. 123456, and press <OK>.

xii. Enter user ID, e.g. **1212**, and press <OK>; all handsets have the same default ID & PW.

xiii. Enter password, e.g. **0000**, and press <OK>.

xiv. Skip encryption by pressing <OK>. (It takes about 30 seconds to complete one handset registration.)

xv. Default wireless IP handset extension number starts with 3301. Use MMC 724 to change numbering plan.

- c. Repeat the above process for each handset.

Remarks

Quick Troubleshooting if handset fails to register:

1. Ping IP address of MCP from PC (via wireless WLAN connection)
 - a. If fails, make sure that
 - i. MCP, MGI and SMT-R2000 have the LAN cables connected to the same data switch.
 - ii. The LAN cable is connected to the WAN port of SMT-R2000.
2. Check MMC settings to make sure that
 - a. "Dual AP" is selected in MMC 849.
 - b. "Register VoWLAN" is enabled in MMC 849.
 - c. WIP registration mode is matched between system and the handset.
 - i. If "Static WIP IP" is enabled in the system, handset needs to use the static IP mode.
 - d. Handset IP addresses are programmed in the MMC 848.
 - e. There is no IP addresses conflict in the network.
 - f. The MCP/MGI and the handset are in the same subnet range.
3. Handset registration process
 - a. Make sure not leading 0 in the IP address field. EX. Enter 165.213.97.101 not 165.213.097.101.

SMT-R2000 Security:

This quick set up guide provides only an example for set-up. The data is automatically broadcast through WLAN when SMT-R2000 is connected to the network. That means any PC with WLAN card is able to associate to the AP and access to the data network.

Dealers are expected to work with the IT department to determine the proper measure for the data network security. The data network security and WLAN security are the big topic in the industry.

1. SMT-R2000 dual band AP has the factory default as "SSID broadcast". It can be unchecked.
 - i. [Security], [11b/g Security Setting], Broadcast (uncheck the box)
2. If WEP key is used, the following settings are required for WIP-5000M to work:
Under [Security], [11b/g Security Setting]
 - i. Wlan1 Key Length: 128 bits
 - ii. Key Type: ASCII
 - iii. WEP keys: 1234567890123 (13 ASCII characters)
 - iv. Authentication: Open System
3. MAC filtering feature can be used to allow only some devices (ex. handsets) to the AP. If this feature is used, all APs should have the list.
 - i. [Manage], [MAC Filtering],
 1. Filter: Allow only stations in list
 2. At the bottom of screen, type in MAC address in the box, and click [Add]

4. If radio 1 (802.11a) is not used, it should be turned off to prevent back door to the AP.
 - i. [Manage], [Radio], Status: (check) Off

SMT-R2000 Repeater Mode (Wireless Distribution System):

WDS function is used to extend the coverage wirelessly. One repeater jump is allowed for each AP.

1. The host AP MAC address and RF channel info are required to set up the repeater mode. Under the repeater AP,
 - a. [Manage], [WDS], Radio:1
 - i. Remote Address: (enter host AP MAC address)
 - b. [Manage], [Wireless Settings], Radio Interface 1
 - i. Channel: (set to the same channel as the host AP)

WIP-5000M:

1. Handset has hidden mode for the following info:
 - a. Software version
 - b. IP address
 - c. MAC address
 - d. Phone State
 - e. Display RSSI, voice quality is guarantee when CQ>=45

To access the hidden mode:

- **In Idle state:** <menu>, <hold>, <*>, <#>
 - **In conversation state (only RSSI):** <music key>, <#>
3. When handset is out of range,
 - a. It will maintain the call for 30 seconds to allow user to come back to the coverage area;
 - b. It will keep searching AP (in pre-defined time interval).
 - c. Once in range, handset will automatically re-registered and in service.

System:

1. Handset can be **cleared** (de-registered) from system by using MMC 849.
 - a. After selecting the extension number, move the right softkey to the field "FORCED"

[WI P REGI STER CLEAR]

[3301 : FORCED]
 - b. Press right softkey again

[WI P REGI STER CLEAR]

[ARE YOU SURE?NO]

c. Press <1> to start the process

2. Useful MMCs

- MMC 847: Display status of WLI and WAP
- MMC 815: Customer database copy
- MMC 724: Dial numbering plan
 - Wireless IP handset is under "IP STN NUM PLAN"
 - For OfficeServ 500M version, VoWLAN starts with IDX061
 - For OfficeServ 500L version, VoWLAN starts with IDX121
 - For OfficeServ 7200, VoWLAN starts with IDX061
 - For OfficeServ 100, VoWLAN starts with IDX033
- MMC 805: Adjust voice path gain
- MMC 217: Station pair assignment
- MMC 210: To change call forward setting
- MMC 846: To change handset registration user id and password
- MMC 844: IP Station Type (handset is "Mobile Phone" type)
- MMC 101: Reset handset password

Quick Software Upgrading Guide for Dual-Band AP (SMT-R2000) & WIP-5000M

Wireless Access Point – SMT-R2000 (Dual-Band)

Requirements:

1. A PC with an Ethernet network card or a 802.11a or b or g Wi-Fi client card

Set Up:

1. Set TCP/IP address of the PC to the same subnet range.
e.g. Windows XP
 - a. Right click "My Network Places" from desktop
 - b. Right click "Local Area Connection" and select "Properties"
 - c. Double click "Internet Protocol (TCP/IP)"
 - d. Select "Enter the following IP address" and enter the PC IP address, e.g.
 - i. IP address: 192.168.111.5
 - ii. Subnet mask: 255.255.255.0
 - iii. Default gateway: 192.168.111.1
 - e. Select <OK>, and <OK>
2. Connect PC to the access point through either
 - a. Wired network, or
 - i. Connect laptop PC Ethernet port to the WAN port of the SMT-R2000
 - b. Wireless LAN
 - i. Move laptop PC within the AP coverage range, say less than 10 ft
 - ii. Associate the PC to the AP
 1. Default SSID is "SMT-R2000-WLAN1" for 802.11b/g, and
 2. Default SSID is "SMT-R2000-WLAN0" for 802.11a
 - iii. If you move PC from one access point coverage to another, the PC may still connect to the previous AP. You may need to disable and enable the WLAN card in the PC to force to connect to the desired AP.
3. Connect PC to the Web page of the access point by using Internet Explorer web browsing application software.
 - a. Enter the IP address of the AP at the address bar and press GO
e.g. 192.168.111.10
 - b. Login to the AP Web management page
 - i. User name: **admin**
 - ii. Password: **samsung**

Steps:

1. From the AP web page, go to Maintenance > Upgrade
2. Use <Browse...> button to select the file.
 - a. Default file name is **smtr2k022110000_upgrade.tar**
3. Click <Upgrade> button to start the process
4. It takes about 8 minutes to complete the process.

Handset

The user registration data will be preserved during the software upgrade process. After software upgrade, turn-on the handset will automatically re-register to the system.

Requirements:

1. A SMT-R2000 access point.
2. A PC with a network card or WLAN card.
3. PC TFTP server software.
 - a. E.g. "SolarWinds" or "WinTFTP Server"

Set Up:

Same instruction from the previous page.

Steps:

1. From AP web page, change SSID of AP to numeric digits for handset
 - a. Basic Settings: IEEE 802.11b/g (SSID): 11
 - b. Update
2. **From PC, run TFTP server software**
e.g. WinTFTP Server 1.0
 - a. Set up upload filename path and make sure file is in the directory
e.g. C:\temp
3. From handset,
 - a. Enter the downloading mode
 - i. Press <5> and <END> at the same time while in power off mode.
The downloader version should be v3.02 or above.
 - ii. Press <2> "Download App." to enter the downloading mode
 - iii. Press <1> to "Edit IP"
 1. Assign an IP address for handset. e.g. 192.168.111.21
 2. Press <OK>
 3. Enter SSID of the system. e.g. 11
 4. Press <OK>
 5. Press <OK> to skip WEP key entry
 6. Press <2> to disable WEP key. The display will flash between "SAMSUNG" and "*** Downloader ***". The handset is ready to download the software.
 - b. Ping handset IP address from the DOS Windows of the PC. E.g. >ping 192.168.111.21 -t
 - c. After receiving the response from the ping, use CTRL-C to cancel the operation.
 - d. Open Internet Explorer, enter the handset IP address at the address field, and click GO. E.g. 192.168.111.21
 - e. After handset web page pops up, enter password of the handset (default 1234), and select "Download".

- f. Enter TFTP server address (PC IP address). e.g. 192.168.111.5
- g. Enter file name. e.g **ofsr_v03.06.00_0320_type1.r0** and click <Start Download> button. The handset LCD will show running numbers and "Burning".
- h. After completion, the handset LCD will show "Download OK"
- i. Remove the handset battery and re-insert the battery.
- j. Turn on the handset power and press <menu>, <hold>, <*>, <#> and <1> to check the software version number.

Note: It is better to assign different IP address (e.g. 192.168.111.22) for each handset.

SMT-R2000

User 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 2006**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 if their respective companies.

PRINTED IN USA

INTRODUCTION

Purpose

This manual introduces Access Point(AP)/Repeater SMT-R2000, and describes how to use the SMT-R2000 and troubleshoot when any failure occurs. In addition, this document describes its hardware configuration and circuits and provides the parts list for SMT-2000.

Document Content and Organization

This manual consists of five Chapters and two Appendices.

CHAPTER 1. Introduction of SMT-R2000

Introduces SMT-R2000 and describes the configuration and specifications of SMT-R2000.

CHAPTER 2 - 7. Using the SMT-R2000

Describes how to use the menus of the SMT-R2000.

CHAPTER 8. Troubleshooting

Describes how to troubleshoot when any failure occurs while operating the SMT-R2000.

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

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



CAUTION

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



CHECKPOINT

Provides the operator with checkpoints for stable system operation.



NOTE

Indicates additional information as a reference.

Revision History

EDITION	DATE OF ISSUE
00	May 2006

SAFETY CONCERNS

For product safety and correct operation, the following information must be given to the operator/user and shall be read before the installation and operation.

Symbols



Caution

Indication of a general caution



Restriction

Indication for prohibiting an action for a product



Instruction

Indication for commanding a specifically required action



CAUTION

**When Removes Shield Can**

When removes Shield Can, be careful of the damage of RF terminal parts caused by heat.

TABLE OF CONTENTS

Purpose	I
Document Content and Organization	I
Conventions	II
Revision History	II
Symbols.....	III
Caution	IV
CHAPTER 1. Introduction of SMT-R2000	1-1
1.1 SMT-R2000 Overview	1-1
1.2 SMT-R2000 Configuration	1-2
1.3 Hardware Specification	1-4
CHAPTER 2. Basic Settings	2-1
2.1 Basic Setup	2-1
2.2 Change of Web Page Language and Setup	2-3
CHAPTER 3. Security	3-1
3.1 Blocking Network via Station Isolation	3-1
3.2 SSID View, Station Isolation, Security Mode.....	3-1
3.3 None (Plain-text)	3-2
3.4 Guest Network.....	3-3
3.5 Static WEP	3-3
3.6 IEEE 802.1x.....	3-5
3.7 WPA Personal.....	3-6
3.8 WPA Enterprise	3-7
CHAPTER 4. Status	4-1
4.1 Interfaces	4-1

4.2	Event	4-2
4.3	Transmit/Receive Statistics.....	4-4
4.4	Client Associations.....	4-5
4.5	Sessions	4-6
4.6	Neighboring Access Points.....	4-6

CHAPTER 5. Manage 5-1

5.1	Ethernet (Wired) Setting	5-1
5.2	Wireless Settings	5-6
5.3	Configuring Radio Settings.....	5-9
5.4	Virtual Wireless Network (VWN)	5-12
5.5	Wireless Distribution System (WDS) Settings.....	5-15
5.6	Controlling Access by MAC Address Filtering	5-18
5.7	Load Balancing	5-19
5.8	Port Control.....	5-20
5.9	Port Forward.....	5-21

Chapter 6. Services 6-1

6.1	Quality of Service (QoS) Setup	6-1
6.2	Simple Network Management Protocol (SNMP)	6-6
6.3	NTP Server Setting.....	6-9

CHAPTER 7. Maintenance 7-1

7.1	Configuration Management.....	7-1
7.2	Firmware Upgrade	7-2

CHAPTER 8. Troubleshooting 8-1

8.1	LED Failure	8-2
8.2	Power Failure	8-3
8.3	Wireless Failure -5 GHz	8-4
8.4	Wireless Failure -2.4 GHz	8-5
8.5	Network Connection Failure	8-6

0-9	9-1
A	9-4
B	9-5
C	9-6
D	9-7
E	9-8
F	9-9
G	9-9
H	9-10
I	9-10
J	9-12
L	9-12
M	9-13
N	9-14
O	9-15
P	9-16
Q	9-17
R	9-17
S	9-19
T	9-20
U	9-21
V	9-22
W	9-22
X	9-24

CHAPTER 1. Introduction of SMT-R2000

This chapter introduces SMT-R2000 and describes the configuration and specifications of SMT-R2000.

1.1 SMT-R2000 Overview

SMT-R2000 is a wireless LAN Access Point (AP) that is available in the construction of a wireless network and can be used as a wireless LAN repeater.

As a wireless LAN repeater, SMT-R2000 is installed within the cell area of AP or the repeater, and re-transmits the data of wireless terminals, such as wireless notebook and wireless PDA, in the outside of the cell area of neighboring AP to AP.

- **AP:** The AP for wireless LAN is an access device for wireless network connection and performs the relay function among wireless terminals and wired LAN. In general, the AP has a specified use area and a specific frequency.
- **Repeater:** If AP signal for wireless LAN is transferred over a specified distance, the output signal will be attenuated. Therefore, a device that creates new wave or raises output voltage is required to enlarge the transfer distance. To do so, the wireless LAN repeater is used as a device to restore and relay the transfer signals.

1.2 SMT-R2000 Configuration

This section describes the configuration of SMT-R2000.

1.2.1 Front Panel of SMT-R2000

The front panel of SMT-R2000 is as shown in the figure below:

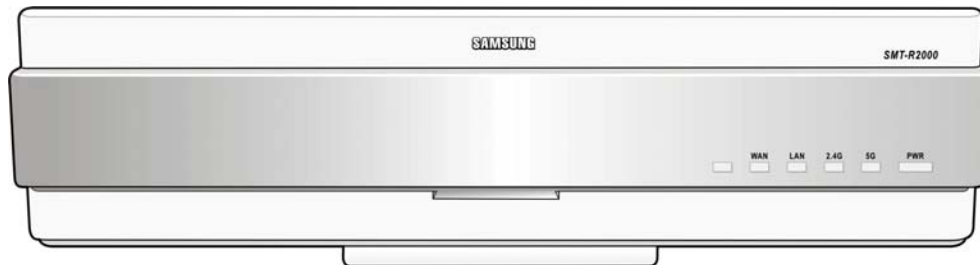


Figure 1.1 Front Panel of SMT-R2000

The following table describes each LED of the front panel:

Table 1.1 LEDs of SMT-R2000

LED	Function	Blue LED turns on	Blue LED turns off	Blue LED blinks
WAN	WAN operation status	WAN is in normal operation	WAN fails to operate	Data is being transmitted/received through WAN
LAN	LAN operation status	LAN is in normal operation	LAN fails to operate	Data is being transmitted/received through LAN
2.4 GHz	2.4 GHz operation status	2.4 GHz Wireless LAN is in operation	2.4 GHz Wireless LAN fail to operate	Data is being transmitted/received through 2.4 GHz Wireless LAN
5 GHz	5 GHz operation status	5 GHz Wireless LAN is in operation	5 GHz Wireless LAN fail to operate	Data is being transmitted/received through 5 GHz Wireless LAN
PWR	Power supply status	Power supply is normal	Power supply fails	-

1.2.2 Rear Panel of SMT-R2000

The rear panel of SMT-R2000 is as shown in the figure below:

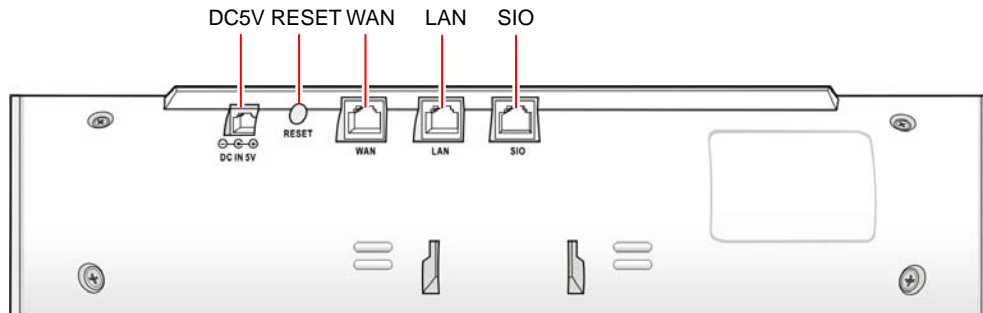


Figure 1.2 Rear Panel of SMT-R2000

The following table describes each port of the rear panel:

Table 1.2 Ports of SMT-R2000

Port	Function
DC IN 5 V	Port for connecting to local power supply adaptor(5 V, 2 A)
RESET	External RESET input port of the system
WAN	LAN port for connecting to WAN(RJ-45)
LAN	LAN port for connecting to LAN(RJ-45)
SIO	Used for connecting to PC to check the operational status of SMT-R2000

1.3 Hardware Specification

The SMT-R2000 hardware specification is as follows:

Table 1.3 SMT-R2000 Hardware Specification

Category	Sub-Category	Item	Specification
WLAN	IEEE 802.11a	Wireless Access	CSMA/CA
		Frequency	5.15~5.825 Ghz
		Transmission Method	OFDM
		Transmission Output	14 dBm(25 mW) or more in 54 Mbps mode
			15 dBm(30 mW) or more in 48 Mbps mode
			16 dBm(50 mW) or more in 36 Mbps mode
			17 dBm or more in other modes
		Bandwidth	20 Mhz or less
		Spectrum Mask	-20 dBr or less at Fc+/- 11 Mhz
			-28 dBr or less at Fc+/- 20 Mhz
			-40 dBr or less at Fc+/- 30 Mhz
		Receive Sensitivity	-65 dBm or less in 54 Mbps mode
			-82 dBm or less in 6 Mbps mode
		Adjacent Channel Rejection	-1 dB or more in 54 Mbps mode
			16 dB or more in 6 Mbps mode
	IEEE 802.11g	Wireless Access	CSMA/CA
		Frequency	2.4~2.4835 Ghz
		Transmission Method	OFDM
		Transmission Output	14 dBm(25 mW) or more in 54 Mbps mode
			15 dBm(30 mW) or more in 48 Mbps mode
			16 dBm(50 mW) or more in 36 Mbps mode

Category	Sub-Category	Item	Specification
			17 dBm or more in other modes
		Bandwidth	20 Mhz or less
		Spectrum Mask	-20 dBr or less at Fc+/- 11 Mhz
			-28 dBr or less at Fc+/- 20 Mhz
			-40 dBr or less at Fc+/- 30 Mhz
		Receive Sensitivity	-65 dBm or less in 54 Mbps mode
			-82 dBm or less in 6 Mbps mode
		Adjacent Channel Rejection	-1 dB or more in 54 Mbps mode
			16 dB or more in 6 Mbps mode
WLAN	IEEE 802.11b	Wireless Access	CSMA/CA
		Frequency	2.4~2.4835 Ghz
		Transmission Method	DSSS
		Transmission Method	17 dBm or more
		Bandwidth	26 Mhz or less
		Spectrum Mask	Primary Sidelobe: -30 bBr or less
		Receive Sensitivity	-76 dBm or less(11 Mbps)
ANTENNA	-	Built-in ANT	2 dBi Dipole ANT
		Diversity	Support- default
ETHERNET	-	Link Speed	Ethernet 10/100 base -T
Power Supply	-	Adaptor	Input: 100~240 VAC, 50~60 Hz Output: 5 V, 2 A
		POE	Support- IEEE802.3af compliant
Bottom Case	-	Dimension	115h x 60w x 35d(mm)
		Weight	148 g or less
Environment	Temperature	Operational Temperature	0~45°C
		Storage Temperature	-20~70°C
Authentication	Korea	Authentication for specification	MIC

Category	Sub-Category	Item	Specification
	Europe	Authentication for specification	CE
	U.S.A.	Authentication for specification	FCC
	Wi-Fi	WLAN Compatibility test	802.11a/b/g Radio interoperability & WPA1.0


CHAPTER 2. Basic Settings

2.1 Basic Setup

Summary of Basic AP Setup Status

Items	Description
IP Address	Show the IP address of an AP. Since the IP address is allocated from DHCP or as a fixed value from 'Ethernet Setup' as described in Guest Interface Ethernet (Wired) Setup , this item cannot be modified.
MAC Address	<p>Shows the MAC address of an AP.</p> <p>MAC address is a permanent and unique Hardware address of a device indicating Network interface. The MAC address is assigned by a manufacturer and users cannot change the MAC addresses. In this item, the address is supported for the purpose to provide the information as a unique identifier of interface and indicates the MAC address of a bridge.</p> <p>This address is an address to be known to other Networks.</p> <p>To check Guest or Internal interface of AP, refer to Status > Interface.</p>
Firmware Version	<p>Show the version information of a firmware currently installed in AP.</p> <p>Whenever the new version of SMT-R2000 firmware is released, the firmware is upgraded to enable to use AP with the strengthened function.</p> <p>For the method to upgrade of a firmware, refer to Firmware Upgrade.</p>
Country Code	<p>Chooses AP-using country. When you change the country code, be aware of channel setup.</p> <p>Note: When you change the country code, you must reboot after completing the update.</p>
Compensation of Base Period	Compensates Coordinated Universal Time (UTC) received via NTP. For example, since Seoul has the time difference of 9 hours from the UTC, 9 (SL) is selected.
Location	Describes the location of AP.

Network Setup

Item	Description
Current Password	<p>Enter the current administrator' password. Before you change the password, you must enter the current password exactly.</p> <p>If the password is correct, the check mark is displayed and the following items can be changed.</p>
New Password	<p>Enter a new administrator password. The letters you entered are displayed as “*” not to show to others.</p> <p>The administrator's password should be alphabetical string with 8-letter at maximum length.</p> <p> As the first step for Radio LAN security, it is recommended to change the administrator password.</p>
Confirmation of New Password	<p>Re-enter the administrator password to confirm the new administrator password.</p>
802.11a, 802.11b/g	<p>Enter the name of radio Network as a string. This name will be applied to all APs over (SSID) the network. Whenever APs are added, the APs will share this SSID.</p> <p><i>Service Set Identifier (SSID)</i> is an alphabetical and numerical string with 32 letters at maximum length.</p> <p>Note: If you re-set SSID while you access and set AP via a radio client, the access to AP may be disconnected. In this case, you should re-access with new SSID after storing the changes.</p>

Note: SMT-R2000 does not allow the change of multiple setups at the same time. If you establish a network with multiple APs or several administrators access Administrator's Web page and change the setups, all APs in the group will enter to the standby mode until the synchronization is completed. However, this action does not ensure the complete application of the setups changed by various users.

Update of Basic Setup

If new setup is completed, click the Update button to apply the changes.

Summary of Basic Setup Status

When the basic setup is updated, the summary of changes can be displayed along with the information of the next step.

The security for AP is not set in the initial operation. The security setup is, also, the important step. Refer to Security.

Re-click of the basic setup changes the summary of the Setup page into the standard basic setup page.

2.2 Change of Web Page Language and Setup



The design panel on the top of all AP setup screen enables you to customize the exteriors of all Web pages. You can change font sizes and select one of various languages.

Locale



You can choose one of the following two languages:

- English/US
- Korean/Korea

The choice of the language you want converts texts on all pages in English or Korean.

Font Size

Click one of font size buttons on the design panel to change text sizes on the screen.

Configuration	Description
	Normal
	Large

Color Scheme

To customize the colors on the screen, select one of the following three options:

Configuration	Description
Scheme 1	Change the colors into Grey and Blue.
Scheme 2	Change the colors into Grey and White.

CHAPTER 3. Security

Security Setup is performed independently according to the radio modes.

At the tabs of "11a Security Setup" and "11b/g Security Setup", the securities in 11a mode and 11b/g mode should be set, respectively. The security mode, SSID view, and Station Isolation set at this time operate independently by set radios.

3.1 Blocking Network via Station Isolation

If the Station Isolation option is activated, AP can block out the communication between the radio clients of the relevant radio band. However, the communication between the radio client and the wired equipments is continuously permitted.

This traffic blocking, also, is applied to the client connected to the network via WDS link. If the Station Isolation item is activated, the client, also, cannot communicate with other clients. For the information on WDS, refer to [WDS Setup](#).

The following setup information describes how to set the security mode at AP. If the data is to be exchanged into AP, the client should set the security mode and the encryption key the same as thoses of AP.

Notes: Other Security modes besides the Plain-text mode are applied only to "Internal" network. To "Guest" network, only the Plain-text. (For the information on Guest network, refer to [Guest Access Setup](#).)

3.2 SSID View, Station Isolation, Security Mode

In order to set the security of AP, select the security mode, and set the items described below. (As explained below, the SSID view and the Station Isolation items can be activated/non-activated for the preparatory measure.)

Item	Description
Broadcast SSID	In order to activate the item of Broadcast SSID , select the checkbox.

Item	Description
	<p>IN the default setup, AP contains the <i>Service Set Identifier</i> (SSID) into Beacon frame to transmit it.</p> <p>You can prevent the automatic retrieval of your AP by not transmitting SSID. In this case, the network name of AP (SSID) is not displayed on the network list that can be connected by the client. The client should designate the correct network name in order to access AP.</p>
Station Isolation	<p>Select the checkbox if activating the Station Isolation item.</p> <p>If the Station Isolation item is unchecked, the radio client can communicate with other clients via AP.</p> <p>If the Station Isolation item is checked AP can block out the communication between the radio clients. However, the communication between the radio client and the wired equipment continues to be continued. This traffic block out is applied also to the client connected to the network via WDS link. If the Station Isolation item is activated, this client also cannot communicate with other wireless clients. For the information on WDS, refer to WDS Setup.</p> <p>Select one of the following security modes.</p> <ul style="list-style-type: none"> • None (Plain-text) • Static WEP • IEEE 802.1x • WPA Enterprise • WPA Personal <p>To Guest network, only the "None (Plain-text)" security mode can be set. (For this information, refer to Guest Access Setup.)</p> <p>Other security modes besides the Plain-text mode are applied only to the "Internal" network.</p>

3.3 None (Plain-text)

None (Or Plain-text) mode means that the client does not encrypt the data when it communicate with SMTR2000.

If the "None (Plain-text)" is selected, other security items are not necessary to be set any more.

3.4 Guest Network

To Guest network, only the "None (Plain-text)" security mode can be set.

This feature make the guest client access without the security setup.

The minimum method for protecting the Guest network is to block out the transmission of SSID (Network name).

For the information on Guest network, refer to [Guest Access Setup](#).

3.5 Static WEP

Wired Equivalent Privacy is a protocol of data encryption for 802.11 wireless network. All clients and APs should have the shared key of 64-bit (40 bit secret key + 24 bit initialization vector (IV)) for the data encryption.

64-bit WEP key and 128-bit WEP key cannot be shared to be used.

If selecting "Static WEP" as the security mode, the following items should be set.

Item	Description
Key Index to be used	Select the key index on the drop down menus (1 ~ 4). The default key index is 1. The key index that is to be used indicates what key to be used for the encryption in the data transmission.
Key Length	Designate the length of the WEP key by selecting one of the followings: <ul style="list-style-type: none">• 64 bit• 128 bit
Key Types	Designate the type of WEP key by selecting one of the followings: <ul style="list-style-type: none">• ASCII• Hex
WEP Key	Up to four WEP keys can be designated. Enter in each test box the character ring that is used as WEP key. In case of "ASCII" selected, the input can be made by combining the ASCII characters. In case of "HEX" selected, hexadecimal (Combination of 0-9 and a-f or A-F) can be entered. Enter the characters as many as the figure designated at "Characters required" item. The character ring entered into this item is RC4WEP key shared by the client and AP.

Item	Description
	<p>The client should set the same WEP key in the same index as designated in AP. (Refer to Static WEP Key Setup Rules.)</p> <p>Characters required: Means the number of the characters necessary for WEP key. The necessary items are automatically updated according to the key lengths and the key types.</p>
Authentication	<p>The authentication algorithm is the procedure checking if the relevant client, in case of using Static WEP security mode, is permitted for the access to AP.</p> <p>Designate the authentication algorithm to be used by selecting one of followings:</p> <ul style="list-style-type: none"> • Open System • Shared Key <p>Note: You can select either of Open System checkbox or the public key checkbox.</p> <p>The authentication of Open System method permits the accesses by all clients. In this case, whether the client uses the correct WEP is not important. This authentication algorithm is used in the None (Plain-text), IEEE 802.1x, WPA security mode. If the authentication algorithm is set as "Open System", all clients can access AP.</p> <p>Note that just because a client station is allowed to <i>associate</i> does not ensure it can exchange traffic with an access point. A station must have the correct WEP key to be able to successfully access and decrypt data from an access point, and to transmit readable data to the access point.</p> <p>Shared Key authentication requires the client station to have the correct WEP key in order to associate with the access point. When the authentication algorithm is set to "Shared Key", a station with an incorrect WEP key will not be able to associate with the access point.</p> <p>Open System and Shared key. The cases of selecting both of two algorithms are as follows:</p> <ul style="list-style-type: none"> • If the client is set to use both of WEP security mode and the Shared Key authentication mode, the client should have the correct WEP key for the access to AP. • If the client is set to use the WEP security mode and the Open System authentication mode, the client should have the correct WEP key for the access to AP.
Static WEP Key Setup Rules	<ul style="list-style-type: none"> • All clients should set the Wireless LAN (WLAN) security mode as WEP. In addition, the client should have one of the WEP keys set at

Item	Description
	<p>AP in order to disscramble the data transmitted from AP into the client.</p> <ul style="list-style-type: none"> • In order to decrypt the data from the client into AP, AP should have all keys that the clients use. • Both of AP and the client should allocate the same key to the same index. For example, if AP allocates the WEP key, abc123 into No.3 index, the client should also allocate the same key into No.3 index. • In some of the wireless client software such as Funk Odyssey, you can encrypt the data transmitted into other key by designating many WEP keys. By doing so, the neighboring AP cannot disscramble this data transmission. • If WEP is set by interworking with the Samsung WIP-5000M terminal, the Open system should be checked for its authentication, and for the WEP key should be surely selected with 128 bit, ASCII type, and only the figure should be entered in the key value.

3.6 IEEE 802.1x

IEEE 802.1x is a standard that defines the port-based authentication and the key management method. Extensible Authentication Protocol (EAP) message can be transmitted into IEEE 802.11 network using the EAP Encapsulation Over LANs (EAPOL) protocol. IEEE 802.1x generates periodically the keys. The frame body of 802.11 frame and the Cyclic redundancy Checking (CRC) can be encrypted using RC4 Stream Cipher.

This mode needs RADIUS server in order to authenticate the users. The user account can be managed at the external RADIUS server.

AP needs the RADIUS server that supports the EAP like the Microsoft Internet Authentication Server. If the Windows client can operate, the authentication server should support the Protected EAP (PEAP) and MSCHAP V2).

If using the external RADIUS server, you should have the options for the various authentication modes, such as the certificate, Kerberos, and public authentication, which IEEE 802.1x mode supports. The most important thing is that the client should use the same authentication mode the same as the one that AP uses.

If "IEEE 802.1x" security mode is selected, the following items should be selected:

Item	Description
Radius IP	Enter the Radius IP in the text box. <i>Radius IP</i> is the IP Address of RADIUS.
Radius Key	Enter the Radius key in the text box. Radius Key is the shared key that is to be used at RADIUS server. The text that you enter is expressed into “*” characters so that other cannot see it. This value is not transmitted into the network.

3.7 WPA Personal

Wi-Fi Protected Access Personal is Wi-Fi Alliance IEEE 802.11i standard that includes a *Counter mode/CBCMAC Protocol-Advanced Encryption Algorithm - (CCMP-AES)* method and *Temporal Key Integrity Protocol (TKIP)* method. WPA Personal uses the Pre-shared Key (PSK) instead of IEEE 802.1x and EAP. PSK takes the role of certificate.

This security mode is compatible with the wireless client supporting the early WPA mode.

In case of using "WPA Personal" **security mode**, the following items should be set.

Item	Description
WPA Version	Select the security mode of the client that AP will support. <ul style="list-style-type: none"> WPA WPA2 Both <p>WPA: Select WPA if all clients in the network support the early WPA and if there is no client supporting a new WPA2.</p> <p>WPA2: Select WPA2 that supports the security in the level of IEEE 802.11i standard if all clients in the network support WPA2.</p> <p>Both: Select “Both” if the client supporting WPA2 and the one supporting only WPA are mixed. If this option is selected, the WPA client and the WPA2 client can all access the network and be authenticated.</p>
Cipher Suites	Select the cipher suite you want use: <ul style="list-style-type: none"> TKIP CCMP (AES) Both <p>Temporal Key Integrity Protocol (TKIP) is a default value.</p> <p>TKIP is an encryption method safer than the WEP key encryption. TKIP</p>

Item	Description
	<p>can minimize the reuse of the same key in the encryption, which is the weakness of WEP, by changing the encryption key more frequently. TKIP uses 128-bit "Temporal Key" shared by AP and the client. Temporal Key can be made by combining the MAC Address of the client and the 16-octet Initialization Vector. TKIP performs the encryption using the RC4 algorithm the same as the case of WEP, but it can enhance the network security by changing the Temporal Key at every 10,000 packet.</p> <p>Counter mode/CBC-MAC Protocol (CCMP) is an encryption method for IEEE802.11i that uses the Advanced Encryption Standard (AES). CCMP uses the Cipher Block Chaining Counter (CBCCTR) mode and Cipher Block Chaining Message Authentication Code (CBC-MAC) for the encryption and the integrity checkup.</p> <p>If either of TKIP or CCMP (AES) is selected, Pairwise cipher is AES, and Groupwise cipher is TKIP. Pairwise cipher is used for unicast, and Groupwise cipher for multicast/broadcast. The client supporting TKIP and the one supporting AES can access AP. The WPA client should have one of the following items:</p> <ul style="list-style-type: none"> • A valid TKIP key • A valid CCMP (AES) key <p>The client not set as WPA Personal cannot access AP.</p>
Key	<p>The key value corresponding to <i>Pre-shared Key</i>, which is a public key for the WPA Personal mode. Minimum 8 characters up to 63 characters can be entered.</p>

3.8 WPA Enterprise

Wi-Fi Protected Access Enterprise that uses Remote Authentication Dial-In User Service (RADIUS) is the one that has established the Wi-Fi Alliance IEEE 802.11i standard including Advanced Encryption Standard (AES), Counter mode/CBC-MAC Protocol (CCMP), and Temporal Key Integrity Protocol (TKIP) method. The Enterprise mode needs the RADIUS server for the user authentication.

This security mode is compatible with the client that supports the early WPA.

If "WPA Enterprise" **security mode** is selected, the following items should be selected:

Item	Description
WPA Version	<p>Select the security mode of the client that AP will support.</p> <ul style="list-style-type: none"> • WPA • WPA2 • Both <p>WPA: Select WPA if all clients in the network support the early WPA and if there is no client supporting a new WPA2.</p> <p>WPA2: Select WPA2 that supports the security in the level of IEEE 802.11i standard if all clients in the network support WPA2.</p> <p>Both: Select "Both" if the client supporting WPA2 and the one supporting only WPA are mixed. If this option is selected, the WPA client and the WPA2 client can all access the network and be authenticated.</p>
Cipher Suites	<p>Select the cipher suite you want use:</p> <ul style="list-style-type: none"> • TKIP • CCMP (AES) • Both <p>Temporal Key Integrity Protocol (TKIP) is a default value.</p> <p>TKIP is the encryption method safer than the WEP key encryption. TKIP minimizes the reuse of the same key, which is a weakness of WEP, by changing the encryption key more frequently. TKIP uses the 128-bit "Temporal Key" shared by AP and the client. Temporal Key can be made by combining the MAC Address of the client and the 16-octet initialization Vector. TKIP performs the encryption using the RC4 algorithm the same as the case of WEP, but it can enhance the security of the network by changing the Temporal Key at every 10,000 packets.</p> <p>Counter mode/CBC-MAC Protocol (CCMP) is an encryption method for IEEE802.11i that uses the Advanced Encryption Standard (AES). CCMP uses the Cipher Block Chaining Counter (CBCCTR) mode and Cipher Block Chaining Message Authentication Code (CBC-MAC) for the encryption and the checkup of the message integrity.</p> <p>If all of TKP and CCMP (AES) are selected, the client supporting TKIP and the one supporting AES can access AP. The client that has been set as the WPA Enterprise mode should have one of the followings:</p> <ul style="list-style-type: none"> • A valid TKIP RADIUS IP address and valid shared key • A valid CCMP (AES) IP address and valid shared key <p>The client that is not set in WPA Enterprise mode cannot access AP.</p> <p>The default setup is to use both of TKIP and CCMP. If all of TKIP and CCMP are selected, the client that is set as the WPA Enterprise mode</p>

Item	Description
	<p>should have one of the followings:</p> <ul style="list-style-type: none"> • A valid TKIP RADIUS ID address and RADIUS key • A valid CCMP (AES) IP address and RADIUS key
Radius IP	<p>Enter the Radius IP in the text box.</p> <p><i>Radius IP</i> is the IP Address of RADIUS.</p>
Radius Key	<p>Enter the Radius key in the text box.</p> <p><i>Radius Key</i> is the public key that is shared at the RADIUS server. The text that you enter is expressed into “*” characters so that other cannot see.</p> <p>This value is not absolutely transmitted into the network.</p>

Update Setting

The security setup can be updated as follows:

- Move to the **security** menu.
- Set the desired security item.
- Click the **Update** button to apply the changes.

CHAPTER 4. Status

4.1 Interfaces

Move to Status>Interface before monitoring wired LAN/wireless LAN (WLAN) settings.

Note: Two-radio AP can resolve current wireless settings for Radio One and Radio Two. The One-radio AP can resolve settings for Radio One.

This page shows current SMT-R2000 settings. It shows both Ethernet (Wired) settings and Wireless settings.

Ethernet (Wired) Settings

The Internal Interface item shows the Ethernet MAC address, VLAN ID, IP address, and subnet mask.

The Guest Interface item shows the MAC address and VLAN ID.

Click the **Edit** link to modify the settings.

Wireless Settings

The Radio Interface item shows the radio mode and channel, in addition to the MAC address, and the network name of the internal interface and Guest interface. (For more information, see [Wireless Settings](#) and [Radio Settings](#)).

Click the **Edit** link to modify the settings.

4.2 Event

A user can verify current events generated in SMT-R2000 on this page.

This page provides an option to activate "Remote Log Relay Host" to capture errors showing on the kernel log and all system events. (For this settings, the remote log relay host settings are required. See Kernel Message for Remote Log Relay Host)

Note: SMT-R2000 obtains information on date and time using Network Time Protocol (NTP). Time information is stored in UTC format known as Greenwich Mean Time. Therefore, the stored time information should be modified to user's local time.

For information on NTP settings, see [NTP Server Setting](#).

For Log Relay

- For Remote Login
- Log Relay Host Setting
- ["Activation/Deactivation of Log Relay Function > Event Page](#)

For Remote Login

The kernel log is a wide ranging list including kernel messages such as error conditions, and system events (see System Log).

Kernel log messages are directly verified through the administrator web interface of the related AP. First, it should be set up as the syslog is operated as "Log Relay Host" in a remote server. Then it is available to set up as SMT-R2000 transfers the syslog message to the remote server.

When collecting syslog messages of an AP using a remote server, a user can take some advantages as follows:

- Collects syslog messages from various APs.
- Stores messages older than those stored to one AP.
- Performs management and errors in the form of script.

Log Relay Host Setting

To use the Kernel Log Relay function, the remote server should be set up as being received syslog messages. The method of setting up the remote server varies according to the remote log host used by a user. The following is an example of setting up a remote Linux server using syslog daemon.

Example of Using Linux Syslog Function

It is available to activate the syslog daemon of the Linux server according to the following procedure. For this, the authority for root account is required.

1. Log in in root account to the server to be used as the syslog relay host.

The following works needs the authority for root account. If not logged in in root account, enter su to the command line to acquire the authority for root (“super user”).

2. Add “-r” next to the SYSLOGD variable on the top of the /etc/init.d/syslogd file.

SYSLOGD=”-r”

Information on syslogd command option can be obtained using the man page. (Enter man syslog into the command line.)

3. To all messages to the file, modify the /etc/syslog.conf file.

As an example, if storing a log file naming “AP_syslog”, add the following command:

```
*.* -/tmp/AP_syslog
```

If using the man page, information on the option of syslog.conf is obtained. (Enter man syslog.conf to the command line.)

4. Enter the following command to the command line to restart the syslog server.

```
/etc/init.d/syslogd restart
```

Note: The analog process uses port 514 basically. It is recommended to use the basic port. However, if desired to modify this log port, check if the port allocated to the syslog is not used for other processes.

Activation/Deactivation of Log Relay Function > Event Page

To activate and set up the log relay function on the **Status > Event** page, set up the log relay option and click the Update button as described below:

Item	Description
Event Log Relay	Select if activating or deactivating the log relay host.

Item	Description
	If selecting the check box of the relay log, the log relay host is activated and it is available to modify the IP address and port items of the relay server.
Relay Host	Set up the IP address or DNS of the relay host.
Relay Port	Set up the port that the syslog process of the relay server is to use. The basic port is 514.

Storing Settings

Click Update to apply the modification.

If activating the event log relay function, the remote logging is activated when clicking Update. The related AP will transfer kernel messages to the remote log server in real time.

If the event log relay function is not used, the remote login is deactivated when clicking Update.

Event

Event shows system events on the AP, which are the same to those where stations are connected and authenticated. The real-time event is verified on **Status > Event** of the AP administrator web page.

4.3 Transmit/Receive Statistics

To view transmit/receive statistics for a particular access point, navigate to Status > **Transmit/Receive** on the Administration Web pages for the access point you want to monitor.

This page provides some basic information about the current access point and a real-time display of the transmit and receive statistics for this access point as described in the following table. All transmit and receive statistics shown are totals since the access point was last started. If the AP is rebooted, these figures indicate transmit/receive totals since the re-boot.

Item	Description
IP Address	IP Address for the access point.
MAC Address	Media Access Control (MAC) address for the specified interface.

Item	Description
	<p>A MAC address is a permanent, unique hardware address for any device that represents an interface to the network. The MAC address is assigned by the manufacturer.</p> <p>SMT-R2000 has a unique MAC address for each interface. A two-radio access point has a different MAC address for each interface on each of its two radios.</p>
VLAN ID	<p>Virtual LAN (VLAN) ID</p> <p>A VLAN is a software-based, logical grouping of devices on a network that allow them to act as if they are connected to a single physical network, even though they may not be.</p> <p>VLANs can be used to establish internal and guest networks on the same access point.</p>
Name (SSID)	<p>Wireless network name. Also known as the SSID, this alphanumeric key uniquely identifies a wireless local area network.</p> <p>The SSID is set on the Basic Settings tab. (See Provide Administrator Password and Wireless Network Name.)</p>

Transmit and Receive Information

Item	Description
Total Packets	Indicates total packets sent (in Transmit table) or received (in Received table) by this access point.
Total Bytes	Indicates total bytes sent (in Transmit table) or received (in Received table) by this access point.
Errors	Indicates total errors related to sending and receiving data on this access point.

4.4 Client Associations

You can check the accessed stations along with the information on the packet traffic sent to/received from each station.

Link Integrity Monitoring

SMT-R2000 provides the link integrity monitoring function to constantly check the connection with each client accessed (even the situation that data has been exchanged). To do so, AP transfers data packets to clients at the interval of several second in no-traffic. Through the data packet transfer, AP detects that a client is out of range of AP (even

when abnormal traffic occurs). If the relevant client is disappeared for 300 seconds, the client access is removed from the client access list (even when the client access is removed from the client access list (even when the client access is sustained)).

4.5 Sessions

A “session” is the period of time in which a user on a client device with an unique MAC address maintain a connection with the network. This page provides real-time session monitoring information including which clients are associated with an access point. It displays idle time, data rate, signal, utilization, transmit/receive statistics and error rates.

What is different between Associated and Session?

Association indicates that a client accesses a specific AP, while Session indicates that a client accesses Network. In the same session, the client-Network access can move from a cluster AP to another cluster AP. Clients can roam between APs and manage sessions.

To view transmit/receive statistics for a particular access point, navigate to Status >

4.6 Neighboring Access Points

“Neighboring Access Points” are whose access points within range of wireless detection.

This page shows configuration information and statistics on neighboring access points. By default, the neighboring access point detection is disabled.

CHAPTER 5. Manage

5.1 Ethernet (Wired) Setting

In this chapter you can set Ethernet Local Area Network (LAN).

Note: In this chapter, two wired Ethernet, virtual network (VLAN), NAT, and DHCP server can be set. When configuring virtual network, data terminal that configures the network should also support VLAN.

DNS Name Setting

Item	Description
DNS Name	<p>Enter the DNS name for the access point in the text box.</p> <p>This is the host name. It may be provided by your ISP or network administrator, or you can provide your own.</p> <p>The rules for system names are:</p> <ul style="list-style-type: none">• This name can be up to 20 characters long.• Only letters, numbers and dashes are allowed.• The name must start with a letter and end with either a letter or a number.

Use Guest Access

Guest network and internal LAN can be set in one SMT-R2000.

Internal LAN and Guest Network Setting

Local Area Network (LAN) is a communication network used in a limited area like a floor in a building. LAN connects various network devices such as computers, storage medias, and printers.

Ethernet is the most general technology among technologies that implement LAN. Wi-Fi (IEEE) is another type of LAN technology.

The SMT-R200 allows you to configure two different LANs on the same access point: one for a secure internal LAN and another for a public guest network with no security and little or no access to internal resources. To configure these networks, you need to provide both Wireless and Ethernet (Wired) settings.

Information on how to configure the Ethernet (Wired) settings is provided in the sections below.

(For information on how to configure the Wireless settings, see [Setting the Wireless Interface](#). For an overview of how to set up the Guest interface, see [Setting up Guest Access](#).)

Whether to Use Guest Access

The SMT-R2000 ships with the Guest Access feature disabled by default. If you want to provide guest access on your AP, enable Guest access on the Ethernet (Wired) Settings tab.

Item	Description
Guest Access	By default, the SMT-R2000 ships with Guest Access disabled. <ul style="list-style-type: none">To allow Guest Access, click Enabled.To disable Guest Access, click Disabled.

Specifying a Physical or Virtual Guest Network

If guest access is set to "Enabled", select the method of displaying "internal network" and "Guest network" in AP. First method is a physical method (1) that two networks directly connects to two different LAN ports of AP through cable. Second method is a virtual method (2) that connects AP WAN port to switch VLAN port and defines two different virtual LANs of the switch. (For more information, refer to [Guest Access Setting](#).)

Choose either physically separate or virtually separate internal and guest LANs as described below.

Item	Description
Guest Access	Select Enabled to enable Guest Access. (If you choose this option, you must select whether to use physically separate networks or VLANs on the next setting "For Guest access, use", and then provide details on VLAN or Wired setting for the Guest Network on the rest of the page.) <ul style="list-style-type: none">Select Disabled to disable Guest Access.If connected this access point to two separate networks for a "physically secure" solution, then choose Ethernet Port 2 from the

Item	Description
	<p>drop-down menu to set up your Guest network on the second Ethernet port.</p> <ul style="list-style-type: none"> If the access point is using only one physical connection to your internal LAN (extra port is not in use), then choose VLAN or Ethernet Port 1 from the drop-down menu. This will enable the “VLAN” settings where you must provide a VLAN ID. See also Configuring Guest Interface Ethernet (Wired) Settings. <p>Note: If guest interface and internal interface are reset through VLAN, the connection with AP may fail. First, the switch and DHCP server supports VLAN of IEEE 802.1Q. After setting VLAN in the Ethernet setting page, connect the Ethernet wired of the switch to the VLAN port. Access the administrator Web page through a new IP address.</p>

Enabling or Disabling Virtual Wireless Networks on the AP

If you want to configure the Internal network as a VLAN (whether or not you have a Guest network configured), you can enable “Virtual Wireless Networks” on the access point.

You must enable this feature if you want to configure additional virtual networks on VLANs on the **Manage > VWN** tab as described in Configuring Virtual Wireless Networks.

Item	Description
Virtual Wireless Networks	<p>Select Enabled to enable VLANs for the Internal network and for additional networks. (If you choose this option, you can run the Internal network on a VLAN whether or not you have Guest Access configured and you can set up additional networks on VLANs using the Manage > VWN tab as described in Configuring Virtual Wireless Networks.)</p> <ul style="list-style-type: none"> Select Disabled to disable the VLAN for the internal network, and for any additional virtual networks on this access point.

Configuring LAN or Internal Interface Ethernet Settings

To configure Ethernet (Wired) settings for the internal LAN, fill in the fields as described below.

Item	Description
MAC Address	<p>MAC address of internal interface for AP Ethernet port. Only reading is available and this item cannot change.</p> <p>If you choose to configure internal and Guest networks by “VLANs”, this field will be enabled.</p> <p>Provide a number between 1 and 4094 for the internal VLAN.</p> <p>AP will send DHCP request including VLAN tag. Switch and DHCP server should support VLAN IEEE 802.1Q frame. AP should be able to be connected to DHCP server.</p>
Connection Type	<p>You can select “DHCP” or “Static IP”.</p> <p><i>Dynamic Host Configuration Protocol (DHCP)</i> is a protocol that describes how to provide network setting information to network device by central server. DHCP server leases an IP address to client system, and provides the DNS server information, the IP address information of gateway, and subnet mask information.</p> <p>Static IP indicates that all network settings are provided manually. You must provide the IP address for the Samsung AP, its subnet mask, the IP address of the default gateway, and the IP address of at least one DNS nameserver.</p> <p>If you select "DHCP", the Samsung AP will acquire its IP Address, subnet mask, and DNS and gateway information from the DHCP Servers.</p> <p>Otherwise, if you select "Static IP", fill in the items described in "Static IP Settings."</p> <p>Note : If DHCP server does not exist in internal network, the connection type of AP should change from DHCP to static IP. Then, a new static IP address can be assigned to AP or default IP address can be used. If there is a plan to add a new Samsung AP, it is recommended to assign a new address. Later, when adding a new AP, IP address collision between two APs can be prevented.</p> <p>If you need to recover the default Static IP address, you can do so by resetting the AP to the factory defaults as described in Resetting Factory Default Configuration. Default IP address is 192.168.111.10.</p>
Static IP Address	<p>If you chose “Static IP” as the Connection Type, these fields will be enabled.</p> <p>Enter the target static IP address into the text box.</p>
Subnet Mask	<p>Enter the Subnet Mask in the text boxes. You must obtain this information from your ISP or network administrator.</p>

Item	Description
Default Gateway	Enter the Default Gateway in the text boxes.
DNS Name Server	<p><i>Domain Name Service</i> (DNS) converts <i>Domainname</i>www.Samsung Electronics.com) of network resource into IP address (e.g. 66.93.138.219). DNS server is called <i>Nameserver</i>.</p> <p>There are usually two Nameservers; a Primary Nameserver and a Secondary Nameserver.</p> <p>You can choose Dynamic or Manual mode.</p> <ul style="list-style-type: none"> If you choose Dynamic, the IP addresses for the DNS servers will be assigned automatically via DHCP. (This option is only available if you specified DHCP for the Connection Type. If you choose Manual, you should assign static IP addresses manually.

Configuring Guest Interface Ethernet (Wired) Settings

To configure Ethernet (Wired) Settings for the "Guest" interface, fill in the fields as described below.

Item	Description
MAC Address	MAC address of guest interface for AP Ethernet port. Only reading is available and this item cannot change.
VLAN ID	<p>If you choose to configure internal and Guest networks by "VLANs", this field will be enabled.</p> <p>Provide a number between 1 and 4094 for the Guest VLAN.</p>

Update Settings

To update Ethernet settings:

- Move to **Manage > Ethernet Settings**.
- Configure the ethernet settings as required.
- Click the **Update** button to apply the changes.

5.2 Wireless Settings

Wireless settings describe aspects of the local area network (LAN) related specifically to the radio device in the access point (802.11 Mode and Channel) and to the network interface to the access point (MAC address for access point and Wireless Network name, also known as SSID).

802.11h Regulatory Domain Control

Item	Description
802.11h Regulatory Domain Control	<p>The Administration UI will show whether IEEE 802.11h regulatory domain control is in effect on the AP. IEEE 802.11h cannot be disabled by an end user Administrator. The following details are provided for informational purposes only.</p> <p>IEEE 802.11h is a standard that provides two services required to satisfy certain regulatory domains for the 5GHz band. These two services are Transmit Power Control (TPC) and Dynamic Frequency Selection (DFS).</p> <ul style="list-style-type: none">• TPC requires that Radio Local Area Networks (RLANs) operating in the 5 GHz band use transmitter power control. This involves adhering to a regulatory maximum transmit output power and a mitigation requirement for each permitted channel. The result of which is the reduced interference with satellite services.• DFS requires that RLANs operating in the 5 GHz band implement a mechanism to avoid co-channel operation with radar systems and ensure uniform utilization of any available channels. <p>Notes:</p> <ol style="list-style-type: none">1. 802.11h is automatically enabled in the nation where AP is used and 802.11h is required. This standard is needed for the countries categorized as European Telecommunications Standard Institute (ETSI). 802.11h is enabled when some nations such as Korea (DFS) and England are selected from nation code. In this case, the 'Supports IEEE802.11h.' message is displayed.2. SMT-R2000 is a wireless device that sets channels dynamically under the 5GHz Dynamic Frequency Selection (DFS) technology standard condition. SMT-R2000 can detect radar signals. Thus, when radar signals are detected in the communication among SMTR2000, slave device that cannot detect radar signals, and Access Point (AP), the communication is not established by AP and operation is performed according to the channel movement command.

Setting the Wireless

The radio interface allows you to set the radio Channel and 802.11 mode as described below.

Note: On a two-radio AP, you must configure these radio interface settings for both **Radio Interface One** and **Radio Interface Two**.

Item	Description
Mac Address	<p>Indicates the Media Access Control () addresses for the interface.</p> <p>A MAC address is a permanent, unique hardware address for any device that represents an interface to the network. The MAC address is assigned by the manufacturer. You cannot change the MAC address. It is provided here for informational purposes as a unique identifier for an interface.</p>
Mode	<p>The <i>Mode</i> defines the <i>Physical Layer</i> (PHY) standard being used by the radio --></p> <p>SMT-R2000 is available as a single or dual band access point with one or two radios. The configuration options for Mode differ depending on which product you have.</p> <p>Single-Band AP: For the Single-Band AP, select one of these modes:</p> <ul style="list-style-type: none">• IEEE 802.11b• IEEE 802.11g <p>Dual-Band AP: For the dual band AP, select one of these modes: a mode for each Radio Interface.</p> <ul style="list-style-type: none">• IEEE 802.11b• IEEE 802.11g• IEEE 802.11a
Channel	<p>Select the Channel. The range of channels and the default is determined by the Mode of the radio interface.</p> <p>The Channel defines the portion of the radio spectrum the radio uses for transmitting and receiving. Each mode offers a number of channels, dependent on how the spectrum is licensed by national and transnational authorities such as the Federal Communications Commission (FCC) or the International Telecommunication Union (ITU-R).</p> <p>When setting to "Auto", AP automatically selects the idle channel. When DFS is supported in IEEE802.11a (when the 'supports IEEE802.11h' message is displayed), the channel is always set to AUTO.</p>

“Internal” Wireless LAN Setting

The Internal Settings describe the MAC Address (read-only) and Network Name (also known as the SSID) for the internal *Wireless LAN* (WLAN) as described below.

Item	Description
Mac Address	<p>MAC Shows the MAC address(es) for Internal interface for this access point. This is a read-only field that you cannot change.</p> <p>Although this access is point is physically a single device, it can be represented on the network as two or more nodes each with a unique MAC Address. This is accomplished by using multiple <i>Basic Service Set Identifiers</i> (BSSIDs) for a single access point.</p> <p>The MAC address(es) shown for the "Internal" access point is the BSSID(s) for the "Internal" interface.</p>
SSID	<p>Enter the SSID for the internal WLAN.</p> <p>The <i>Service Set Identifier</i> (SSID) is an alphanumeric string of up to 32 characters that uniquely identifies a wireless local area network. It is also referred to as the <i>Network Name</i>. There are no restrictions on the characters that may be used in an SSID.</p>

“Guest” Wireless LAN Setting

The Guest Settings describe the MAC Address (read-only) and wireless network name (SSID) for the *Guest Network* as described below. Configuring an access point with two different network names (SSIDs) allows you to leverage the Guest Interface feature on the Samsung AP. For more information, see [Setting up Guest Access](#).

Item	Description
Mac Address	<p>MAC Shows the MAC address for the Guest interface for this access point. This is a read-only field that you cannot change.</p> <p>Although this access is point is physically a single device, it can be represented on the network as two or more nodes each with a unique MAC Address. This is accomplished by using multiple <i>Basic Service Set Identifiers</i> (BSSIDs) for a single access point.</p> <p>The MAC address(es) shown for the "Guest" access point is the BSSID(s) for the "Guest" interface.</p>
SSID	<p>Enter the SSID for the <i>guest network</i>.</p> <p>The <i>Service Set Identifier</i> (SSID) is an alphanumeric string of up to 32 characters that uniquely identifies a wireless local area network. It is also</p>

Item	Description
	referred to as the <i>Network Name</i> . There are no restrictions on the characters that may be used in an SSID.--> For the guest network, provide an SSID that is different from the internal SSID and easily identifiable as the "guest" network.

Update Setting

To update Ethernet settings:

- Move to **Manage > Wireless Settings**.
- Configure the wireless settings as required.
- Click the **Update** button to apply the changes.

5.3 Configuring Radio Settings

The configuring Wireless Setting page allows a user to control the operation of the radio system.

A user can set up radio on/off, RF channel, beacon cycle, transmission power, IEEE 802.11 mode, etc.

SMT-R2000 can be set up as a dual-band AP.


Performance such as service range and transfer rate is different according to each wireless mode. Even though for the same wireless mode, the performance of SMT-R2000 may be different according to its environment.

AP operates in the following modes:

- IEEE 802.11b mode
- IEEE 802.11g mode
- IEEE 802.11a mode

Item	Description
Radio	SMT-R2000 is a Dual Band AP . A user can designate Radio 1 or Radio 2. Set up both Radio 1 and 2 to use SMT-R2000 as a Dual Band AP.
Status (On/Off)	Click the On or Off button to determine the on/off status of the wireless settings (Radio 1/Radio 2).

Item	Description
Mode	<p>A <i>mode</i> defines a standard of <i>Physical Layer</i> (PHY) used for wireless settings. SMT-R2000 can be operated as a single-band AP or dual-band AP.</p> <p>Single-Band AP: For Single-Band AP, select one from the following three modes. For other wireless modes, turn them off using the Mode menu.</p> <ul style="list-style-type: none"> • IEEE 802.11a • IEEE 802.11b • IEEE 802.11g <p>Notes: For SMT-R2000, the IEEE802.11a mode can be set up only in Radio 1, and the IEEE802.11b or IEEE802.11g mode can be set up only in Radio 2.</p> <p>Dual-Band AP: For Dual-Band AP, use the following combination:</p> <ul style="list-style-type: none"> • IEEE 802.11a / IEEE 802.11b • IEEE 802.11a / IEEE 802.11g • IEEE 802.11a / IEEE 802.11b / IEEE 802.11g <p>Notes: For two-radio AP, each radio can be set up as a different mode by selecting a radio from the Radio item.</p>
External Antenna	<p>If a user is located out of the wireless range of SMT-R2000, it is available to expand the wireless LAN range using an external antenna. Using a separately purchased antenna line and antenna, install the antenna nearby the user and turn this function on.</p>
Channel	<p>A channel means a part of a radio spectrum used by a radio for transmission and reception. The range of a channel and basic channel are determined by the radio interface mode.</p> <p>In most modes, the default settings are "Auto". If the channel settings are Auto, the AP selects a channel where the usage rate is lowest based on information on signal strength and traffic load. Except "Auto", it is available to select one from Channel 1 to 11.</p>
Beacon Interval	<p>An AP transfers beacon frames in regular intervals to notify the existence of wireless network. An AP basically transfers a beacon frame every 100m/sec (or 10 times per second).</p> <p>The unit of <i>beacon interval</i> is 'ms', and a value can be entered between 20 and 2000.</p>
DTIM Period	<p><i>Delivery Traffic Information Map</i> (DTIM) is a message used for beacon frames. DTIM contains a signal to make a client containing data to transfer to AP stop the sleep mode.</p>

Item	Description
	<p>The DTIM period indicates how often to transfer DTIM messages after loading to beacon messages.</p> <p>Designate a value between 1 and 255.</p> <p>If the DTIM period is set up as “1”, the DTIM message is included to all beacon frames. If the DTIM period is set up as “10”, the DTIM message is included to every tenth beacon frame.</p>
Maximum Stations Transmit Power	<p>Designate the maximum number of clients to allow accessing to AP. (0 ~ 2007)</p> <p>Enter the transfer power of AP in the unit of %.</p> <p>The default value is 100%.</p> <p> Recommendations:</p> <ul style="list-style-type: none"> • If possible, set up as the default value (100%) to maximize the service range of the AP and reduce the number of AP for a network. <p>To increase the capacity of the network, set up the transfer power of an AP low and arrange APs close. It reduces superposition and interference among APs. In addition, it makes a network safer when the transfer power of an AP is low, as a weak wireless signal is not transferred far.</p>
Rate Sets	<p>Set up the basic rate that the supported rate set of an AP and an AP broadcast to a network AP.</p> <ul style="list-style-type: none"> • The unit of Rates is Mbps. • The Supported Rate Sets indicates the transfer rate supported by an AP. It is available to set up multiple transfer rates. An AP selects the optimum transfer rate considering error rate and distance with a client. • The Basic Rate Sets is transferred to a network to communicate with other APs and clients in the network.
Enable Broadcast/Multicast Rate Limiting	<p>It is available to improve the performance of all networks by limiting the number of packets transferred through a network.</p> <p>Some protocols multicasts or broadcasts packets that most network nodes do not consider for such as ARP request, and DHCP or BOOTP messages. For these protocols, if setting rate limit control, it is available to limit the number of redundant packs.</p> <ul style="list-style-type: none"> • Click the Enabled button to activate the Multicast and Broadcast Rate and Limiting option. • Click the Disabled button to activate the Multicast and Broadcast Rate Limiting option.

Item	Description
	The default settings of Multicast/Broadcast Rate Limiting are 'disable'. Until the Multicast/Broadcast Rate Limiting option is activated, the following items are in deactivation status.
Broadcast/Multicast Rate Limit	Enter the value of rate limit for broadcast/multicast traffic. The value of rate limit should be between 1 and 50 (the number of packets per second). The default values of rate limit and the value of the maximum rate limit are "50".
Broadcast/Multicast Rate Limit Burst	The value of Rate Limit Burst is a value of the number that network traffic allows traffic bursts before exceeding the rate limit. The default values of rate limit and the value of the maximum rate limit are "75".

Update Setting

Update the wireless settings as follows:

- Move to **Manage > Radio**.
- Set up the wireless settings item required.
- Click the **Update** button to apply the modification.

Note: SMT-R2000 can set up both Radio 1 and Radio 2 on one page. According to the radio selected from the Radio item, the setting items displayed on the screen are applied to Radio 1 or Radio 2. If a radio is completely set up, click the Update button to store the modification, and then the user can set up another radio by selecting.

5.4 Virtual Wireless Network (VWN)

VLAN Setting

Notes:

- Set Virtual Wireless Networks to 'Activated' in the Ethernet setting page to set additional network in VLAN. See "Virtual Wireless Network Setting" of Ethernet setting menu.
- To configure additional networks on VLANs, you must first enable Virtual Wireless Networks on the Ethernet Settings page. See ["Enabling or Disabling Virtual Wireless Networks on the AP"](#).
- If VLAN option is set, the connection to AP may fail. First, check if the switch and DHCP server supports VLAN with IEEE 802.1Q. After setting VLAN option,

connect the Ethernet cable of the switch VLAN port (WAN port). Re-access the administrator Web page as a new IP address. (If necessary, contact the administrator for the setting of VLAN and DHCP.)

Item	Description
Virtual Wireless Network	You can configure up to 14 VWNs.
Activate	<p>You can enable or disable a configured network.</p> <p>To enable the specified network, check the Enabled checkbox beside the appropriate VWN.</p> <p>To disable the specified network, uncheck the Enabled checkbox beside the appropriate VWN.</p> <p>If you disable the specified network, you will lose the VLAN ID you entered.</p>
VLAN ID	<p>Provide a number between 1 and 4094 for the Internal VLAN.</p> <p>This will cause the access point to send DHCP requests with the VLAN tag. The switch and the DHCP server must support VLAN IEEE 802.1Q frames. The access point must be able to reach the DHCP server.</p> <p>Check with the Administrator regarding the VLAN and DHCP configurations.</p>
SSID	<p>Enter a name for the wireless network as a character string. This name will apply to all access points on this network. As you add more access points, they will share this SSID.</p> <p>The <i>Service Set Identifier</i> (SSID) is an alphanumeric string of up to 32 characters.</p> <p>Note: If you are connected as a wireless client to the same AP that you are administering, resetting the SSID will cause you to lose connectivity to the AP. You will need to reconnect to the new SSID after you save this new setting.</p>
Broadcast SSID	<p>Select the Broadcast SSID setting by selecting the Broadcast SSID checkbox.</p> <p>By default, the access point broadcasts (allows) the <i>Service Set Identifier</i> (SSID) in its beacon frames.</p> <p>You can suppress (prohibit) this broadcast to discourage stations from automatically discovering your access point. When the AP's broadcast SSID is suppressed, the network name will not be displayed in the List of Available Networks on a client station. Instead, the client must have the</p>

Item	Description
	<p>exact network name configured in the supplicant before it will be able to connect.</p> <p>Note: The Broadcast SSID you set here is specifically for this Virtual Network (One or Two). Other networks continue to use the security modes already configured:</p> <ul style="list-style-type: none"> • Your original Internal network (configured on Ethernet [Wired] tab) uses the Broadcast SSID set on Security. • If a Guest network is configured, the Broadcast SSID is always allowed.
Security Mode	<p>Select the Security Mode for this VLAN. Select one of the following:</p> <ul style="list-style-type: none"> • None (Plain-text) • Static WEP • IEEE 802.1x • WPA Enterprise • WPA Personal <p>Note: The Security mode you set here is specifically for this Virtual Network. Other networks continue to use the security modes already configured:</p> <ul style="list-style-type: none"> • Your original internal network (configured on Ethernet Settings page) uses the Security mode set on Security. • If a Guest network is configured, always set the security mode to "None".

Update Setting

To upgrade VLAN settings:

- Move to **Manage > VWN**.
- Configure the VLAN settings as required.
- Click the **Update** button to apply the changes.

5.5 Wireless Distribution System (WDS) Settings

SMT-R2000 lets you connect multiple access points using a Wireless Distribution System (WDS). WDS allows access points to communicate with one another wirelessly in a standardized way. This capability is critical in providing a seamless experience for roaming clients and for managing multiple wireless networks. It can also simplify the network infrastructure by reducing the amount of cabling required.

The WDS requires both APs using the same RF channels and the same SSID.

WDS (Repeater)

The following notes summarize some critical guidelines regarding WDS configuration. Please read all the notes before proceeding with WDS configuration.

Notes:

- When using WDS, be sure to configure WDS settings on both access points participating in the WDS link.
- You can have only one WDS link between any pair of access points. That is, a remote MAC address may appear only once on the WDS page for a particular access point.
- Both access points participating in a WDS link must be on the same Radio channel and using the same IEEE 802.11 mode. (See [Configuring Radio Settings](#) for information on configuring the Radio mode and channel.)
- When 802.11h is operational, setting up two WDS links can be difficult, as the operating channel of the two APs may keep changing, depending on the channel usage and radar interference.

To configure WDS on this access point, describe each AP intended to receive hand-offs and send information to this AP. Each destination AP needs the following description

Item	Description
Radio	<p>The Samsung AP is available as a one-radio or two-radio access point.</p> <p>One-Radio AP: On the one-radio version of SMT-R2000, this field is not included on the WDS tab.</p> <p>Two-Radio AP: For each WDS link on a two-radio AP, select Radio One or Radio Two. The rest of the settings for the link apply to the radio selected in this field. The read-only "Local Address" will change depending on which Radio you select here.</p>
Local Address	<p>Indicates the Media Access Control (MAC) addresses for this access point.</p> <p>A MAC address is a permanent, unique hardware address for any device</p>

Item	Description
	<p>that represents an interface to the network. The MAC address is assigned by the manufacturer. You cannot change the MAC address. It is provided here for informational purposes as a unique identifier for the access point or interface.</p> <p>One-Radio AP: On a one-radio access point, a single MAC address is shown at the top of the WDS settings page. The address shown for the one-radio AP is the MAC address for that radio AP. This is the address by which the AP is known externally to other networks.</p> <p>Two-Radio AP: For each WDS link on a two-radio AP, the Local Address reflects the MAC address for the Internal interface on the selected radio (Radio One on WLAN0 or Radio Two WLAN1).</p>
Remote Address	<p>Specify the MAC address of the destination access point; that is, the access point to which data will be sent or "handed-off" and from which data will be received, in other words the AP to which you are creating the WDS bridge.</p> <p>Click the drop-down arrow to the right of the Remote Address field to see a list of all the available MAC Addresses, their associated SSIDs and Signal Levels on the network. Select the appropriate MAC address from the list.</p> <p>Note: The SSID displayed in the drop-down list is simply to help you identify the correct MAC Address for the destination access point. This SSID is a separate SSID to that which you set for the WDS link. They two do not (and should not) be the same value or name.</p>
Bridge with	<p>Network to be connected to WDS link. By default, internal network is used.</p>

If you do not care about the WDS link security, encryption type is not required to be decided. If not, Static WEP can be selected as the encryption type.

Encryption Type	Description
None	<p>If you set encryption to None, the data sent between the APs across the WDS bridge will not be encrypted, but rather will be sent as plain text.</p>
WEP	<p>Specify whether you want <i>Wired Equivalent Privacy</i> (WEP) encryption enabled for the WDS link.</p> <p><i>Wired Equivalent Privacy</i> (WEP) is a data encryption protocol for 802.11 wireless networks. Both access points on the WDS link must be configured with the same security settings. For static WEP, a static 64-bit (40-bit secret key + 24-bit initialization vector (IV)) or 128-bit (104-bit</p>

Encryption Type	Description
	secret key + 24-bit IV) Shared Key for data encryption. For more information on WEP security, see Static WEP

Setting WDS Link Security Mode to None

If you select None as your preferred WDS encryption option, you will not be asked to fill in any more fields on the WDS tabbed page. All data transferred between the two APs on the WDS link will be unencrypted.

Setting WDS Link Security Mode to WEP

If you select WEP as your preferred type of encryption on the WDS link, a number of additional fields will appear on the WDS tabbed page.

Item	Description
Encryption	WEP
WEP	Select this option if you want to set WEP encryption on the WDS link.
Key Length	If WEP is enabled, specify the length of the WEP key: <ul style="list-style-type: none"> 64 bits 128 bits
Key Type	If WEP is enabled, specify the length of the WEP key: <ul style="list-style-type: none"> ASCII Hex
Characters Required	Indicates the number of characters required in the WEP key. The number of characters required updates automatically based on how you set key length and key type.
WEP key	Enter a string of characters. If you selected "ASCII", enter any combination of 0-9, a-z, and A-Z. If you selected "HEX", enter hexadecimal digits (any combination of 0-9 and a-f or AF). These are the RC4 encryption keys shared with the stations using the access point.

Update Settings

To update WDS settings:

- Move to **Manage > WDS**.
- Configure the WDS settings as required.
- Click the **Update** button to apply the changes.

5.6 Controlling Access by MAC Address Filtering

A Media Access Control (*Media Access Control*) address is a hardware address that is a solitary identifier of each network node. All IEEE 802 network equipment has a MAC address of 48-bit, and such address is generally composed of twelve 16-digits, and colons such as FE:DC:BA:09:87:65.

A wireless Network Interface Card (NIC), which is used by a client, has a solitary MAC address.

A user can adjust clients attempting to access to a wireless network, by setting up MAC addresses of clients to be allowed/blocked on "MAC Filtering". If the MAC filtering function is activated, only clients that MAC addresses are allowed can access to a network.

Using MAC Filtering

Using the MAC filtering function, a user can limit AP accesses based on Media Access Control (MAC) addresses. A user can also allow or block client accesses on the MAC address list through filter settings.

If the guest interface is activated, the MAC filtering setting is applied to both two BSSs.

In an AP using 802.11a and 802.11b/g, the MAC filtering settings are applied to both 802.11a and 802.11b/g.

Item	Description
Filter	<p>Click a button from the following buttons to set up the MAC address filter.</p> <ul style="list-style-type: none">• Accesses only permitted for terminals on the list.• All terminals on the list blocked.• Mac filtering not used.
Stations List	<p>Enter a 48-bit MAC address and click the Add button to add the MAC address to the terminal list.</p> <p>Then the MAC address will be added to the terminal list.</p> <p>Select the 48-bit MAC address and click the Delete button to remove the MAC address from the terminal list.</p> <p>A user can also allow or block a client in the list to access to an AP through filter settings.</p>

Settings Update

Update the MAC filtering settings as follows:

- Move to **MAC filtering** page..
- Set up the MAC filtering item as desired.
- Click the **Update** button to apply the modification.

5.7 Load Balancing

SMT-R2000 allows a user to distribute wireless client connections when configuring multiple AP environments to the SMT-R2000. The Load Balancing function prevents a specific AP performance from being lowered by unbalanced wireless traffic.


Load Balancing Settings

Activate "Load Balancing" before setting the load balancing. Then, set up the restrictions and processing method according to AP utilization rate.

Note:

- Click status > session on the administrator webpage to view the AP utilization rate ([See Session Monitoring page.](#))
- Even though a client terminates the access to an AP, if the client can access to the network thorough another AP service, the network will provide the service to the client continuously. The client attempts to access to another AP on the same subnet with the previous AP automatically. As the result, the client can move another AP on the same subnet without any loss.
- The load balancing settings are applied to the overall loads of an AP. If guest access is allowed, the load balancing is applied to all internal networks and guest networks.
- In two-radio AP, the load balancing settings are applied to the two radios together. However, each radio load is independently estimated, if guest access is allowed, the internal networks and guest networks are all included.

Item	Description
Load Balancing	Click Use to Enable AP load balancing settings. Click Disable to Disable the UAP load balancing settings.
Utilization for No New Associations	The utilization rate limit is related to wireless bandwidth utilization. Set up the limits of bandwidth utilization rate (%) that indicates when rejecting access of new clients. When the utilization rate exceeds the limit of AP utilization rate, the AP rejects the access of a new client.

Item	Description
	If this item is set up as '0', the AP allows all accesses regardless of the utilization rate.
Utilization for Disassociation	<p>The utilization rate limit is related to wireless bandwidth utilization.</p> <p>Set up the bandwidth utilization rate limit (%) that indicates when disconnect the client access.</p> <p>If the utilization rate of an AP exceeds the limit, the AP disconnects the client access.</p> <p>If setting up this item as 0, all client accesses are not disconnected regardless of the utilization rate.</p>
Stations Threshold for Disassociation	<p>Set up the desired number of clients to "Stations Threshold". If the number of clients accessing to AP at a specific time is the same to the setup value or less, all client accesses are not disconnected regardless of the value of "Utilization for Disassociation".</p> <p>Theoretically, the maximum number of simultaneously accessible clients is 2007.</p> <p> It is recommended to set up as a value between 30 and 50 at the maximum. In this range, an AP will be reasonably operated.</p>

Update Settings

Update the load balancing settings as follows:

- Move to the **Load Balancing** page.
- Set up the load balancing items as desired.
- Click the **Update** button to apply the modification.

5.8 Port Control

The Port Control function allows or blocks service access for a specific port served for a WAN IP. If a specific port that is used for Local IP is entered, this function allows or blocks service access.

Using Port Control

The Port Control function allows or blocks service access for a specific port served for a WAN IP. For a WAN IP, items where service access is allowed or blocked are as follows:

Telnet, HTTP, FTP, ICMP, ping

A user can allow or block that a WAN IP or Local terminal accesses to a specific service port through port-control settings.

Item	Description
Protocol Port Filtering	<p>The Protocol Port Filtering shows the list served by the current WAN IP settings.</p> <p>For the list, there are Telnet, HTTP, FTP, ICMP, and ping.</p> <ul style="list-style-type: none">• A user can allow or block WAN IP access by selecting Unblock or Block.
UDP/TCP Port Filtering List	<p>The Port filtering list shows the current list settings.</p> <p>Select the desired item and click the Delete button to delete from the list.</p> <p>Select the desired item and click the Add button to add to the list.</p> <ul style="list-style-type: none">• Port filtering UDP list• Port filtering TCP list
Port Number	Enter a specific UDP/TCP port to block from an internal terminal.
Delete/Add	A user can delete/add an item from/to the list using the Delete/Add button.

Update Settings

Update the Port Control settings as follows:

- Move to the **Manage > Port Control** page.
- Set up the Port Control item as desired.
- Click the **Update** button to apply the modification.

5.9 Port Forward

The NAT function converts an internal IP address into an IP address authorized in an external network to solve shortage of the IP addresses in the internal network or not to disclose an internal address to external networks.

The Port Forward function allows an external network to access to a terminal having an internal IP address through a specific WAN IP port.

Using Port Forward

This page allows an external network to access to a terminal having an internal IP address through a specific WAN IP port.

A user can access to the TCP/IP port of an internal client IP through a specific TCP/IP port of a WAN IP using TCP/IP Port settings.

Item	Description
Port Forwarding UDP/TCP List	<p>The Port Forward list shows the list currently set up.</p> <p>Select an item to delete and click the Delete button to delete from the list.</p> <p>Select an item to add and click the Add button to add to the list.</p> <ul style="list-style-type: none">• Port Forwarding UDP list• Port Forwarding TCP list
Local IP Address	Enter an internet IP address to forward.
Local Port	Enter an internal port number to forward.
General Port	Set up an external port number to convert for an existing local port.
Delete/Add	A user can delete/add from/to the list by using the Delete/Add button.

Update Settings

Update the Port Forward settings as follows:

- Move to the **Manage > Port Forwarding**.
- Set up the Port Forwarding item as desired.
- Click the **Update** button to apply the modification.

Chapter 6. Services

6.1 Quality of Service (QoS) Setup

In the pages of Quality of Service (QoS), parameters can be set in many queues in order to guarantee the high performance of the discriminated radio traffic such as Voice-over-IP (VoIP), audio, video, and streaming media.

QoS Setup

The Quality of Service (QoS) setup at SMT-R2000 means the parameters setup to the various categories of radio traffic and the efficient setup of maximum/minimum transmission wait time via Contention Windows. The setup items described here affect the AP data transmission.

Notes:

- In case of Guest Interface, QoS Queue setup affects the whole AP load (Both of BSS).
- Dual Band AP in case of Dual Band AP, these setups are applied to all
- 2.4GHz and 5 GHz radio. However, each radio traffic uses queues independently. (Guest traffic is an exception.)
- The traffics of Internal network and Guest network always use the same queue. This is the same as the case in Dual Band.

QoS of AP uses the Type of Service (ToS) information of IP packet header. AP inspects the ToS area of IP header for all packets that pass through AP. The priorities of the packets are determined by the allocation of the packets into one of many queues according to the values of ToS area. The parameters that you will set determines how each queue processes the data packet.

The following menus are contained in the page of Quality of Service setup.

- [AP EDCA Parameter Setup](#)
- [Wi-Fi Multimedia](#)
- [Station EDCA Parameter Setup](#)
- [Retry Number Setup](#)
- [Priority Setup](#)
- [Setup Update](#)

AP EDCA Parameter Setup

AP Enhanced Distributed Channel Access (EDCA) parameter affects the traffic that is transmitted from AP into the client.

Item	Description
Queue	<p>Queue is defined according to the data types that are to be transmitted from AP into the clients.</p> <p>Data 0 (Voice): This data needs the high priority and little delay time. The data affected by time, such as VoIP and streaming, is transmitted into this queue.</p> <p>Data 1 (Video): This data is a video data that needs the high priority and little delay time. The video data affected by time is transmitted into this queue.</p> <p>Data 2 (best effort): This data needs the middle-level priority, performance, and delay time. Most IP data are transmitted into this queue.</p> <p>Data 3 (Background): This data needs the lowest priority and the high performance. The bulk data that needs the maximized performance and that are little affected by time (Such as FTP data) are transmitted into this queue.</p> <p>For more information, refer to QoS Queues and Parameters to Coordinate Traffic Flow of IEEE 802.11e.</p>
AIFS (Inter-Frame Space)	<p><i>Arbitration Inter-Frame Spacing (AIFS)</i> means the wait time (ms) for the <i>data frame</i>.</p> <p>AIFS is the value between 1 and 255.</p> <p>For more information, refer to DCF Control of Data Frames and Interframe Spaces of IEEE802.11.</p>
cwMin (Minimum Contention Window)	<p>This parameter is the input value of the algorithm that determines the early random backoff wait time ("window") value.</p> <p>The value designated at the Minimum Contention Window item is the maximum value of the initial random backoff wait time that is to be determined by the algorithm.</p> <p>The random figure that is firstly generated will be the one between 0 and the value defined at this item.</p> <p>When the random backoff wait time firstly generated before the transmission of the data frame expires, the retry counter increases, and the random backoff (window) value doubles. This process will be repeated until the size of the random backoff value reaches the value defined at the</p>

Item	Description
	<p>Maximum Contention Window item.</p> <p>The valid "cwmin" values are 1, 3, 7, 15, 31, 63, 127, 255, 511, or 1024. The value of "cwmin" should be less than that of "cwmin".</p> <p>For more information, refer to IEEE802.11 Random Backoff and Minimum / Maximum Contention Windows.</p>
cwMax (Maximum Contention Window)	<p>The value appointed by the Maximum Contention Window item is the maximum value that the random backoff value is multiplied. The random backoff value increases by double until the data frame is transmitted or the value reaches the Maximum value of Contention Window.</p> <p>Once the random backoff value reaches the Maximum Contention Window value, the retry will be repeated until it reaches the maximum retry number.</p> <p>The valid "cwmax" value is 1, 3, 7, 15, 31, 63, 127, 255, 511, or 1024. The value of "cwmax" should be larger than that of "cwmin".</p> <p>For more information, refer to Random Backoff and Minimum / Maximum Contention Windows of IEEE 802.11.</p>
Max. Burst Length	<p>AP EDCA Parameter Only (Max. Burst Length option is applied only to the traffic that is transmitted from AP into the client.)</p> <p>This value means the Maximum Burst Length (ms) that will be permitted for the burst packet to the radio network. Packet Burst is the set of the frames that are transmitted without the header information. By using the burst packet, the overhead can decrease, and the higher performance can be obtained as its result.</p> <p>The valid Max. Burst Length values are the ones between 0.0 and 999.9.</p>

Wi-Fi Multimedia

In default setup, AP is set by using Wi-Fi MultiMedia (WMM). If WMM option is activated, the controlling function of the QoS priority and the access to the radio media are activated. By using WMM, QoS setup of SMT-R2000 controls the downstream traffic (AP ED A parameter) that is transmitted from AP into the client and the upstream traffic (station EDCA parameter) that is transmitted from the client into AP.

If WMM is set as 'not-used', the station EDCA parameter option will be released.

Even though WMM is set as 'not-used', you can still set some of the AP EDCA parameter options.

- If releasing the WMM setup, click "Disable".
- If setting WMM, click "Enable".

Station EDCA Parameter Setup

Station Enhanced Distributed Channel Access (EDCA) parameter affects the traffic transmitted from the client into AP.

Item	Description
Queue	<p>Queue is defined according to the data types that are to be transmitted from AP into the clients.</p> <p>Data 0 (Voice): This data needs the high priority and little delay time. The data affected by time, such as VoIP and streaming, is transmitted into this queue.</p> <p>Data 1 (Video): This data is a video data that needs the high priority and little delay time. The video data affected by time is transmitted into this queue.</p> <p>Data 2 (best effort): This data needs the middle-level priority, performance, and delay time. Most IP data are transmitted into this queue.</p> <p>Data 3 (Background): This data needs the lowest priority and the high performance. The bulk data that needs the maximized performance and that are little affected by time (Such as FTP data) are transmitted into this queue.</p> <p>For more information, refer to QoS Queues and Parameters to Coordinate Traffic Flow of IEEE 802.11e.</p>
AIFS (Inter- Frame Space)	<p><i>Arbitration Inter-Frame Spacing (AIFS)</i> means the wait time (ms) for the <i>data frame</i>.</p> <p>For more information, refer to DCF Control of Data Frames and Interframe spaces of IEEE802.11.</p>
cwMin (Minimum Contention Window)	<p>This parameter is the input value of the algorithm that determines the early random backoff wait time ("window") value.</p> <p>The value designated at the <i>Minimum Contention Window</i> item is the maximum one of the early random backoff wait time that is to be determined by the algorithm.</p> <p>The random figure firstly generated will be the ones between 0 and the value defined at this item.</p> <p>If the random backoff wait time firstly generated before the transmission of the data frame expires, the retry counter increases, and the value of the</p>

Item	Description
	<p>random backoff (window) doubles. This process will be repeated until the value reaches the value defined at the Maximum Contention Window item.</p> <p>For more information, refer to Random Backoff and Maximum Contention Windows of IEEE 802.11.</p>
cwMax (Maximum Contention Window)	<p>The value appointed by the Maximum Contention Window item is the maximum value that the random backoff value is multiplied. The random backoff value increases by doubles until the random backoff value reaches the maximum value of the Contention Window.</p> <p>Once the random backoff value reaches the one of Maximum Contention Window, the retries will continue until a maximum number of retries allowed is reached.</p> <p>Once the Maximum Contention Window size is reached, retries will continue until a maximum number of retries allowed is reached.</p> <p>For more information, refer to Random Backoff and Minimum / Maximum Contention Windows of IEEE 802.11.</p>
TXOP Limit	<p>Station EDCA Parameter Only (TXOP Limit option is applied only to the traffic transmitted from the client into AP.)</p> <p><i>Transmission Opportunity</i> (TXOP) means the time interval that the WME client becomes to have the right to transmit the data.</p>

Retry Number Setup

AP has been set, as its default setup, to permit the retransmission number for the IP Data Packets into the determined value (Default: Six times). The retransmission packet is limited so that it can be provided only at IP

The default retransmission value means the application to the IP packets not mentioned in the retry number list by ports.

Retry Number List by Ports is the one where the protocol type (TCP/UDP) of the IP packet and the destination port no. are selected and the retry number for the relevant transmission packets are allocated. Retransmission List of IP Packet by Destination Ports can register up to 16 lists.

Priority Setup

Priority Level List by Ports is the one where the protocol types of IP packet and the destination port number are selected and the priority values (Within 0~7) for the relevant

transmission packet are allocated. Priority List of IP Packets by Destination Ports can register up to 16 lists.

Update Settings

The QoS setup can be updated as follows:

- Move to **Service > QoS**.
- Set up the necessary QoS items.
- Click “**Update**” to apply the changes.

6.2 Simple Network Management Protocol (SNMP)

SNMP Setting

Start/stop control of SNMP agents, community password configuration, access to MIBs, and configuration of SNMP Trap destinations is provided through the Samsung AP as described below.

Item	Description
SNMP Use/Not SNMP Use	<p>You can select whether to use SNMP in a network. Default is SNMP is not used.</p> <ul style="list-style-type: none">• To enable SNMP, click Enabled.• To disable SNMP, click Disabled. <p>You must click Update to save your settings.</p> <p>Note: If you do not enable SNMP, all remaining fields on the SNMP page will be disabled.</p>
Read-only community name for permitted GETs	<p>Enter a read-only community name.</p> <p>The community name, as defined in SNMPv2c, acts as a simple authentication mechanism to restrict the machines on the network that can request data to the SNMP agent. The name functions as a password and the request is assumed to be authentic if the sender knows the password.</p> <p>The community name can be in any alphanumeric format.</p>

Item	Description
Port number the SNMP agent will listen to	<p>By default an SNMP agent only listens to requests from port 161. However, you can configure this so the agent listens to requests on another port.</p> <p>Enter the port number on which you want the SNMP agents to listen to requests.</p>
Restrict the sources of SNMP requests to only the designated hosts or subnets	<p>You can restrict the source of permitted SNMP requests.</p> <ul style="list-style-type: none"> • To restrict the source of permitted SNMP requests, click Enabled. • To permit any source submitting an SNMP request, click Disabled.
Hostname or subnet of Network Management System	<p>Set DNS host name or subnet of a device that can perform GET/SET request.</p> <p>As with community names, this provides a level of security on SNMP settings. The SNMP agent will only accept requests from the hostname or subnet specified here.</p> <p>To specify a subnet, enter one or more subnetwork address ranges in the form <i>AddressRange/MaskLength</i> where <i>AddressRange</i> is an IP address and <i>MaskLength</i> is the number of mask bits. Both formats <i>NetAddress/NetMask</i> and <i>NetAddress/MaskLength</i> are supported. Individual hosts can be provided for this, i.e. I.P Address or Hostname. For example, if you enter a range of 192.168.1.0/24 this specifies a subnetwork with address 192.168.1.0 and a subnet mask of 255.255.255.0.</p> <p>The address range is used to specify the subnet of the designated NMS. Only machines with IP addresses in this range are permitted to execute GET and SET requests on the managed device. Given the example above, the machines with addresses from 192.168.1.1 through 192.168.1.254 can execute SNMP commands on the device. (The address identified by suffix .0 in a subnetwork range is always reserved for the subnet address, and the address identified by .255 in the range is always reserved for the broadcast address).</p> <p>As another example, if you enter a range of 10.10.1.128/25 machines with IP addresses from 10.10.1.129 through 10.10.1.254 can execute SNMP requests on managed devices. In this example, 10.10.1.128 is the network address and 10.10.1.255 is the broadcast address. 126 addresses would be designated.</p>

SNMP Traps Setting

SNMP traps induces asynchronous message exchange from SNMP devices such as SMT-R2000 to selected host. If monitoring devices that have many Network Management Systems (NMSs), sending query to all devices regularly is not effective. By activating SNMP event trap of AP, each device can directly send a message related with network event to a selected host on NMS or SNMP Manager. Network event includes the going up or down of network interface, connection with AP or authentication failure, system power up or down, and network topology.

SNMP traps save on network resources by eliminating redundant SNMP requests. They also make it easier for SNMP Managers to troubleshoot their network. For example, if an SNMP manager is responsible for a large network that supports many devices, and each device has a large number of objects, it is impractical to request information from every object on every device. The optimum solution is for each agent on the managed device to notify the manager of any unusual events. It does this by sending a trap of the event. After receiving the event information, the manager can choose what action, if any, to take.

Item	Description
Community name for traps	Enter the global community string associated with SNMP traps. Traps sent from the device will provide this string as a community name.
Hostname	Enter the DNS host name of a computer to which you want to send SNMP trap. An example of a DNS hostname is snmptraps.Samsung Electronics.com Since SNMP traps are sent randomly from the SNMP agent, it makes sense to specify where exactly the traps should be sent. You can add up to a maximum of three DNS hostnames. Ensure you select Enabled checkbox beside the appropriate hostname.

Update Settings

To update SNMP settings:

- Move to **Services > SNMP**.
- Configure the SNMP settings as required.
- Click the **Update** button to apply the changes.

6.3 NTP Server Setting

Network Time Protocol (NTP) is an Internet standard protocol to synchronize time between computers in a network. NTP server sends Coordinated Universal Time (UTC or Greenwich Mean Time) to client system. NTP requests time to server regularly and uses received timestamp to match clock. The timestamp will be used to indicate the date and time of each event in log messages. See <http://www.ntp.org> for more general information on NTP.

Using NTP Server / Not Using NTP Server

If AP wants to use a Network Time Protocol (NTP) server, enable the NTP setting and select the target NTP server. If you want to turn the NTP server off, deactivate the NTP setting of AP.

Item	Description
Final Recording Time	This time indicates time of receiving through NTP. The time when an event is most recently generated is displayed. However, if connection is not established with a NTP server, time may not be accurate.
Network Time Protocol (NTP)	NTP provides a way for the access point to obtain and maintain its time from a server on the network. Using an NTP server gives your AP the ability to provide the correct time of day in log messages and session information. For more information on NTP, see http://www.ntp.org Choose to either enable or disable use of a network time protocol (NTP) server. <ul style="list-style-type: none">• To enable the NTP server, click Enabled.• To disable the NTP server, click Disabled.
NTP Server	If NTP is enabled, select the NTP server you want to use. You can specify the NTP server by host name or IP address, although using the IP address is not recommended as these can change more readily.

Update Settings

To update time settings:

- Move to **Services > NTP**.
- Configure the time settings as required.
- Click the **Update** button to apply the changes.

CHAPTER 7. Maintenance

7.1 Configuration Management

Restoring Initial Factory Setup

If a problem generated from SMT-R2000 is not fixed by troubleshooting, use the Reset function. The reset function restores all setups of AP to the factory default settings.

1. Click the **Maintenance > Configuration** menu.
2. Click the Reset button.
All setups return to factory default settings. The factory default settings are listed in the table below.

Item	Default Value
Wired IP Address	192.168.111.10
Country Code	kr
802.11a (5Ghz) SSID	SMT-R2000-WLAN0
802.11b/g (2.4Ghz) SSID	SMT-R2000-WLAN1
AP Name (DNS name)	Samsung-AP
Guest Access Setup	Non-Setting
VWN Setup	Non-Setting
DHCP server	Non-Setting
IP Assignment	Static IP

Storing the Current Settings as a Backup File

Store the current setup copy of an AP as a backup file (.cbk/code> format) as follows:

1. Click the “Download configuration” link.
A file download dialog window is displayed.

2. Select the Save option from the dialog window.
A file browser appears.
3. Select a directory to store the file using the file browser, and click the Save button to store the file.
It is available to keep the existing file name (config.cbk) or rename the backup file.
However, the modified file name should be in the form of “Custom Name + config.cbk”.

Restore the Settings from Previous File Stored

Restore the previous settings from a backup file as follows:

1. Select a backup setup file to restore. Enter the file name including the full path to the Restore item, or click the Browse button to select the file.
(Such as config.cbk only a backup setup file (“Custom Name + config.cbk”) stored using the backup function for user’s database can be restored.)
2. Click the Restore Button.
The access point will reboot.
If the rebooting is completed, enter the IP address of the AP to the address window of the browser to access to the administrator web page. Then, the user can verify the modified settings restored from the backup file.

AP Rebooting

A user can reboot SMT-R2000 manually for management and troubleshooting.

1. Click the **Maintenance > configuration** menu.
2. Click the **Reboot** button.
The AP will reboot.

7.2 Firmware Upgrade

As new versions of SMT-R2000 firmware become available, you can upgrade the firmware on your devices to take advantage of new features and enhancements.

Caution: Do not upgrade the firmware from a wireless client that is associated with the access point you are upgrading. Doing so will cause the upgrade to fail. Furthermore, all wireless clients will be disassociated and no new associations will be allowed.

If you encounter this scenario, the solution is to use a wired client to gain access to the access point:

- Create a wired Ethernet connection from a PC to the access point.
- Bring up the Administration UI

Repeat the upgrade process using with the wired client.

Note: You must do this for each access point; you cannot upgrade firmware automatically across the cluster. Keep in mind that a successful firmware upgrade restores the access point configuration to the factory defaults.

To upgrade the firmware on a particular access point:

1. Move to **Maintenance > Upgrade**.
Information about the current firmware version is displayed and an option to upgrade a new firmware image is provided.
2. If you know the path to the **New Firmware Image** file, enter it in the New Firmware Image textbox. Otherwise, click the Browse button and locate the firmware image file.

Note: The firmware upgrade file supplied must be in the format <FileName>.upgrade.tar. Do not attempt to use <Filename>.bin files or other formats for the upgrade; these will not work.

Upgrade

Click **Upgrade** to apply the new firmware image.

Upon clicking **Upgrade** for the firmware upgrade, a popup confirmation window is displayed that describes the upgrade process.

Click **OK** to confirm the upgrade, and start the process.

Caution: The upgrade process may take 7-9 minutes during which time the access point will be unavailable. During upgrade process, do not turn off the power of the AP. If not, AP may be severely damaged. When upgrade is completed, AP reboots and operates with the setting before upgrade.

Checking Firmware Upgrade

To verify that the firmware upgrade completed successfully, check the firmware version shown on the Upgrade tab (and also on the Basic Settings tab). If the upgrade was successful, the updated version name or number will be indicated.



CHAPTER 8. Troubleshooting

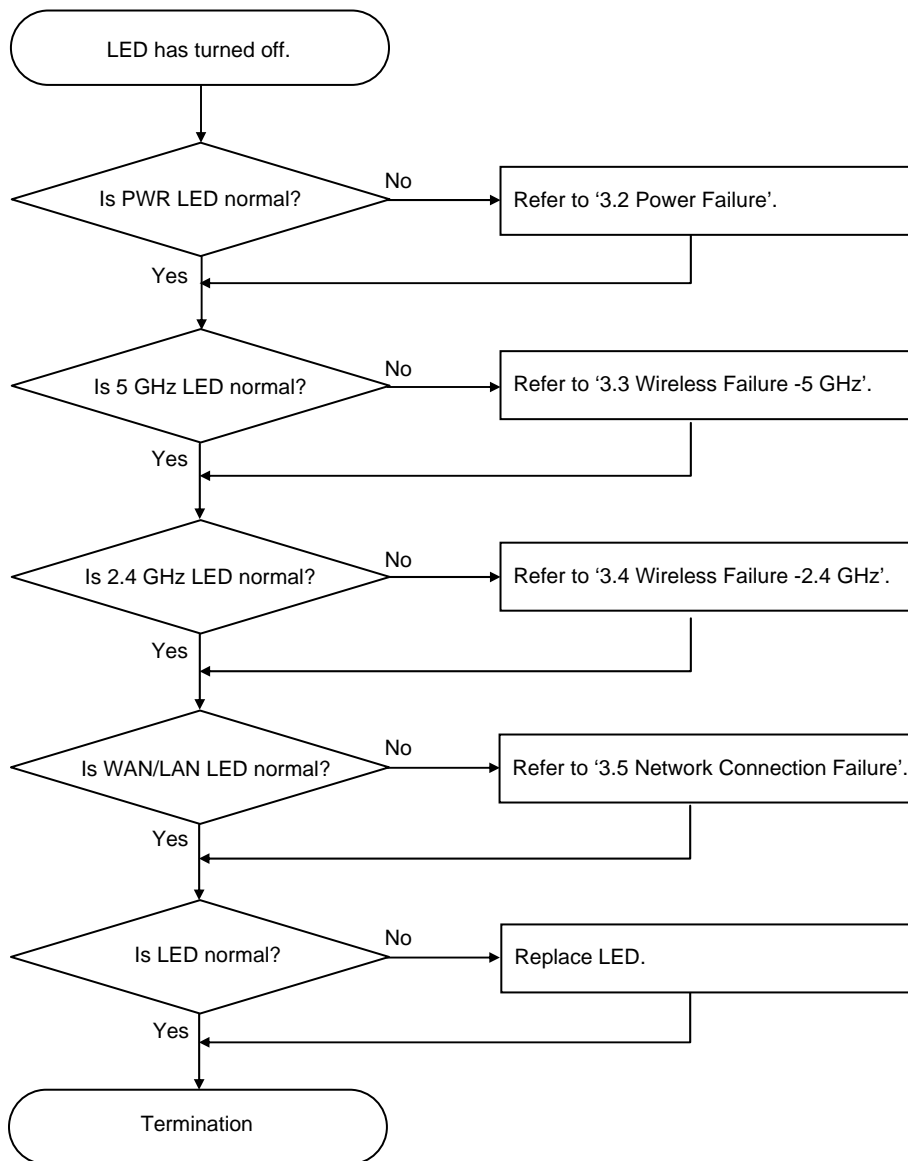
This chapter describes the troubleshooting to the failures that can occur while using SMT-R2000.

8.1 LED Failure

Failure Description

Nothing is displayed on LED even though SMT-R2000 has turned on.

Troubleshooting

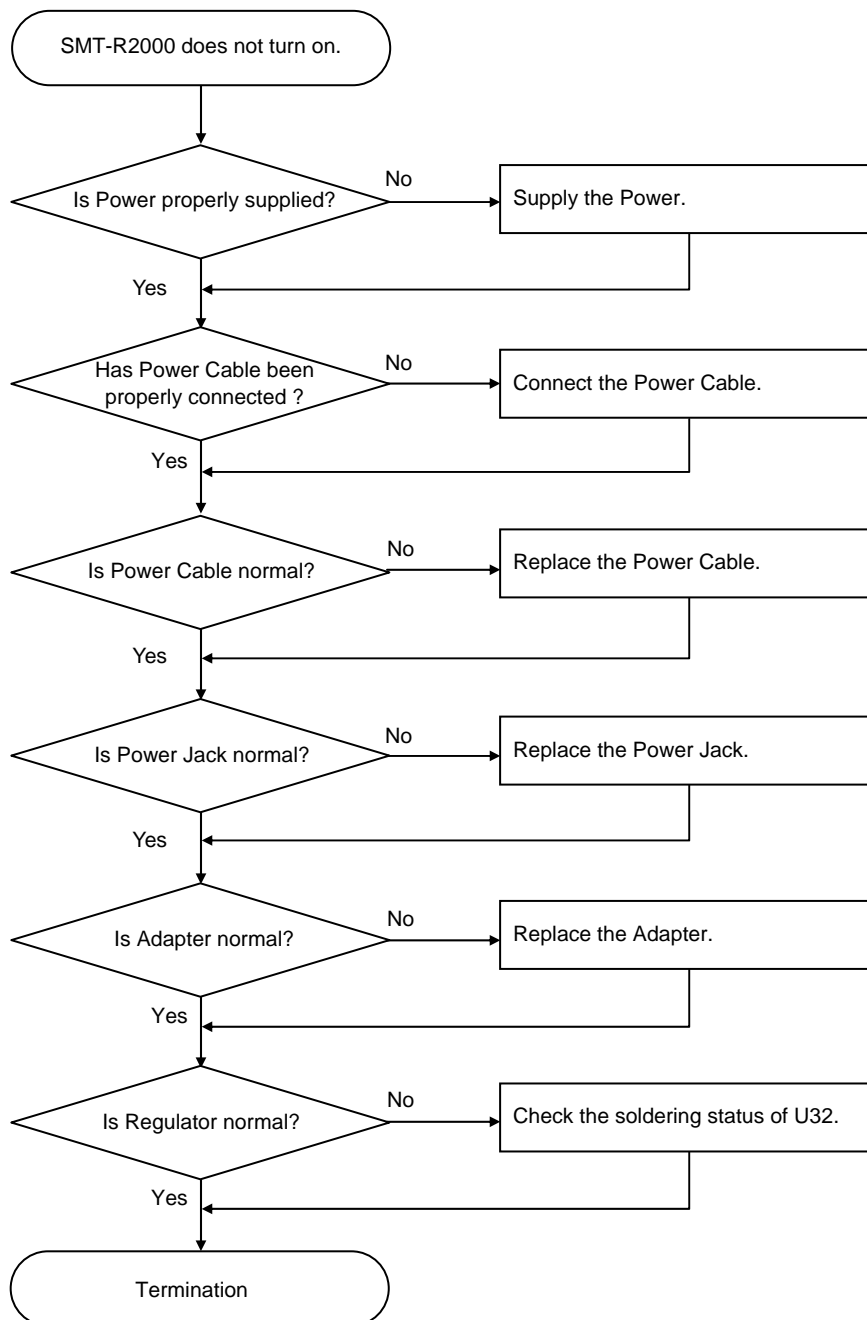


8.2 Power Failure

Failure Description

SMT-R2000's body does not turn on because the power is not supplied to it.

Troubleshooting

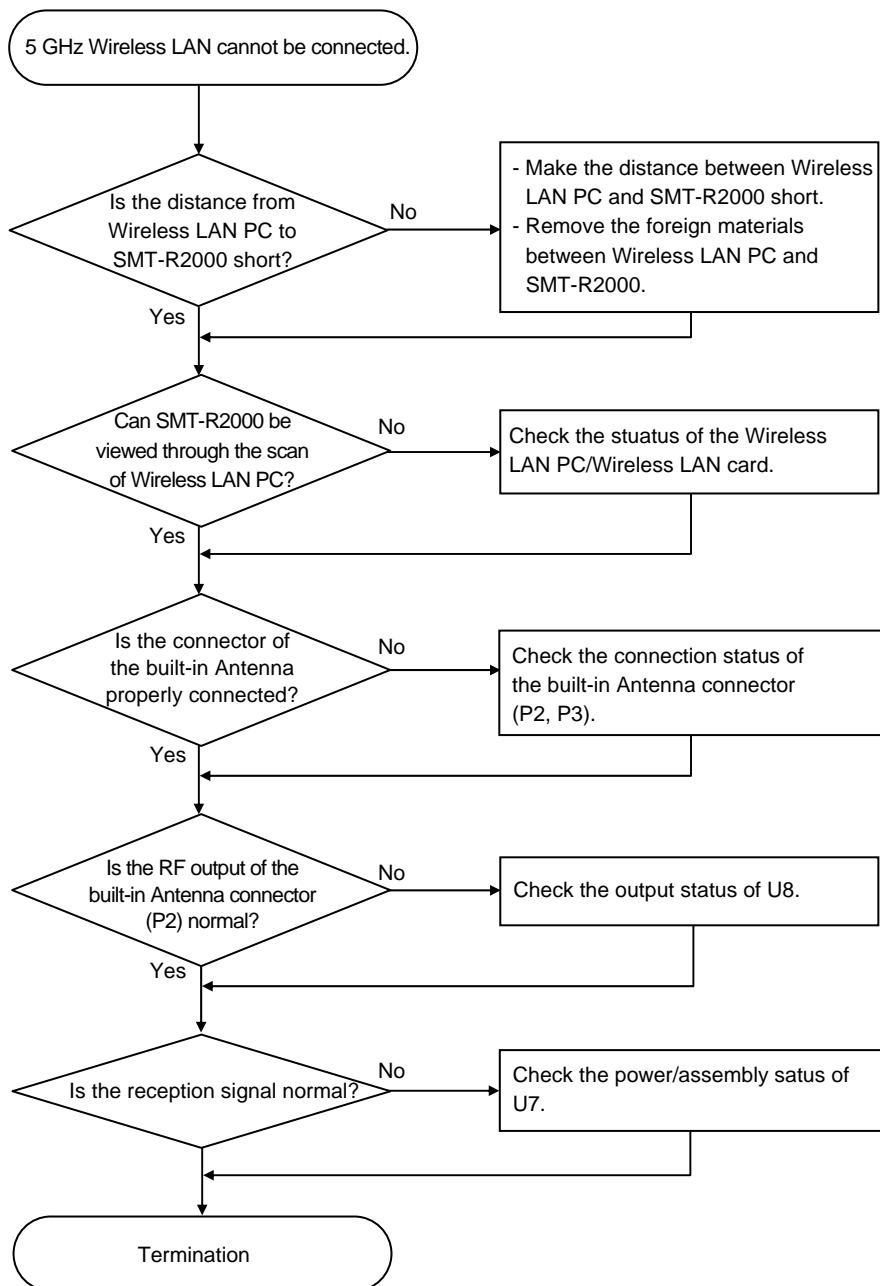


8.3 Wireless Failure -5 GHz

Failure Description

5 GHz(IEEE802.11a) Wireless LAN service cannot be used.

Troubleshooting

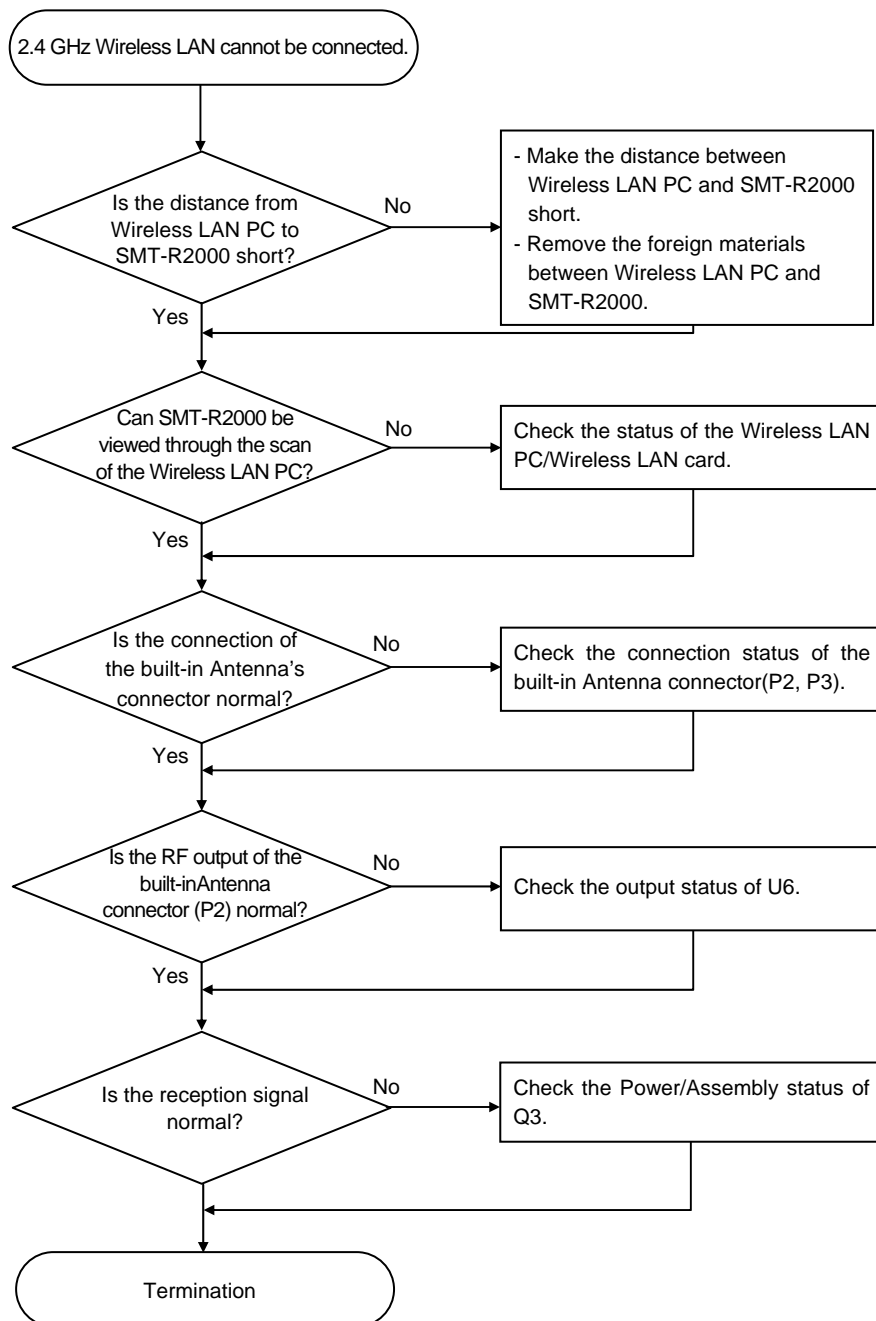


8.4 Wireless Failure -2.4 GHz

Failure Description

2.4 GHz(IEEE802.11b/g) Wireless LAN service cannot be used.

Troubleshooting

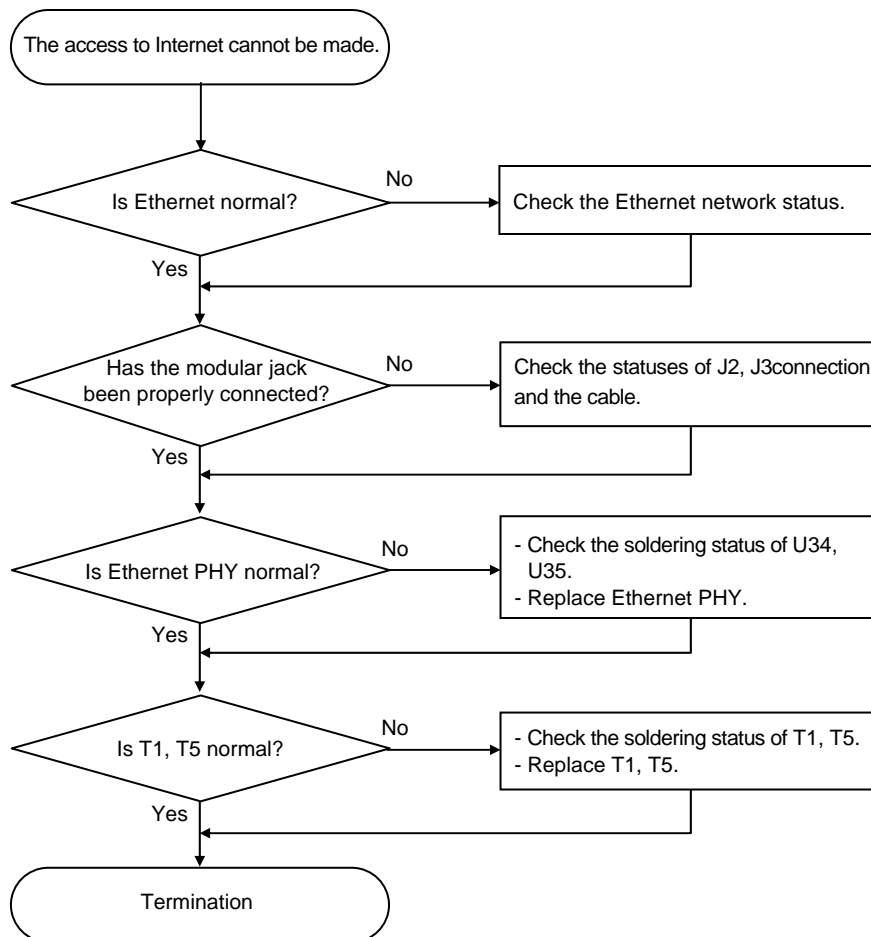


8.5 Network Connection Failure

Failure Description

The access to Internet cannot be made because the connection between SMT-R2000 and Ethernet Network is not made.

Troubleshooting



CHAPTER 9. GLOSSARY

0-9

802

IEEE 802 (IEEE Std. 802-2001) is a family of standards for peer-to-peer communication over a LAN. These technologies use a shared-medium, with information broadcast for all stations to receive. The basic communications capabilities provided are packet-based. The basic unit of transmission is a sequence of data octets (8-bits), which can be of any length within a range that is dependent on the type of LAN.

Included in the 802 family of IEEE standards are definitions of bridging, management, and security protocols.

802.1x

IEEE 802.1x (IEEE Std. 802.1x-2001) is a standard for passing EAP packets over an 802.11 wireless network using a protocol called *EAP Encapsulation Over LANs* (EAPOL). It establishes a framework that supports multiple authentication methods.

IEEE 802.1x authenticates users not machines.

802.2

IEEE 802.2 (IEEE Std. 802.2.1998) defines the LLC layer for the 802 family of standards.

802.3

IEEE 802.3 (IEEE Std. 802.3-2002) defines the MAC layer for networks that use CSMA/CA. Ethernet is an example of such a network.

802.11

IEEE 802.11 (IEEE Std. 802.11-1999) is a medium access control (MAC) and physical layer (PHY) specification for wireless connectivity for fixed, portable, and moving stations within a local area. It uses direct sequence spread spectrum (DSSS) in the 2.4 GHz ISM band and supports raw data rates of 1 and 2 Mbps. It was formally adopted in 1997 but has been mostly superseded by 802.11b.

IEEE 802.11 is also used generically to refer to the family of IEEE standards for wireless local area networks.

802.11a

IEEE 802.11a (IEEE Std. 802.11a-1999) is a PHY standard that specifies operating in the 5 GHz U-NII band using orthogonal frequency division multiplexing (OFDM). It supports data rates ranging from 6 to 54 Mbps.

802.11a Turbo

IEEE 802.11a Turbo is a proprietary variant of the 802.11a standard from Atheros Communications. It supports accelerated data rates ranging from 6 to 108Mbps. Atheros Turbo 5 GHz is IEEE 802.11a Turbo mode. Atheros Turbo 2.4 GHz is IEEE 802.11g Turbo mode.

802.11b

IEEE 802.11b (IEEE Std. 802.11b-1999) is an enhancement of the initial 802.11 PHY to include 5.5 Mbps and 11 Mbps data rates. It uses direct sequence spread spectrum (DSSS) or frequency hopping spread spectrum (FHSS) in the 2.4 GHz ISM band as well as complementary code keying (CCK) to provide the higher data rates. It supports data rates ranging from 1 to 11 Mbps.

802.11d

IEEE 802.11d defines standard rules for the operation of IEEE 802.11 wireless LANs in any country without reconfiguration. PHY requirements such as provides frequency hopping tables, acceptable channels, and power levels for each country are provided. Enabling support for IEEE 802.11d on the access point causes the AP to broadcast which country it is operating in as a part of its beacons. Client stations then use this information. This is particularly important for AP operation in the 5GHz IEEE 802.11a bands because use of these frequencies varies a great deal from one country to another.

802.11e

IEEE 802.11e is a developing IEEE standard for MAC enhancements to support QoS. It provides a mechanism to prioritize traffic within 802.11. It defines allowed changes in the Arbitration Interframe Space, a minimum and maximum Contention Window size, and the maximum length of a burst of data. IEEE 802.11e is still a draft IEEE standard (most recent version is D5.0, July 2003). A currently available subset of 802.11e is the *Wireless Multimedia Enhancements* (WMM) standard.

802.11f

IEEE 802.11f (IEEE Std. 802.11f-2003) is a standard that defines the inter access point protocol (IAPP) for access points (wireless hubs) in an extended service set (ESS). The standard defines how access points communicate the associations and reassociations of their mobile stations.

802.11g

IEEE 802.11g (IEEE Std. 802.11g-2003) is a higher speed extension (up to 54 Mbps) to the 802.11b PHY, while operating in the 2.4 GHz band. It uses orthogonal frequency division multiplexing (OFDM). It supports data rates ranging from 1 to 54 Mbps.

802.11h

IEEE 802.11h is a standard used to resolve the issue of interference which was prevalent in 802.11a. The two schemes used to minimize interference in 802.11h are Transmit Power Control (TPC) and Dynamic Frequency Selection (DFS). DFS detects other APs on the same frequency and redirects these to another channel. TPC reduces the network frequency output power of the AP, thus reducing the chance of any interference. This is a required standard in Europe, Japan, and the U.S.

802.11i

IEEE 802.11i is a comprehensive IEEE standard for security in a wireless local area network (WLAN) that describes *Wi-Fi Protected Access 2* (WPA2). It defines enhancements to the MAC Layer to counter some of the weaknesses of WEP. It incorporates stronger encryption techniques than the original *Wi-Fi Protected Access* (WPA), such as Advanced Encryption Standard (AES).

The original WPA, which can be considered a subset of 802.11i, uses *Temporal Key Integrity Protocol* (TKIP) for encryption. WPA2 is backwards-compatible with products that support the original WPA.

IEEE 802.11i / WPA2 was finalized and ratified in June of 2004.

802.11j

IEEE 802.11j standardizes chipsets that can use both the 4.9 and 5 GHz radio bands according to rules specified by the Japanese government to open both bands to indoor, outdoor and mobile wireless LAN applications. The regulations require companies to adjust the width of those channels. *IEEE 802.11j* allows wireless devices to reach some previously unavailable channels by taking advantage of new frequencies and operating modes. This is practically an attempt to mitigate the crowding on the airwaves, and has tangential relationships to *IEEE 802.11h*.

802.11k

IEEE 802.11k is a developing IEEE standard for wireless networks (WLANs) that helps auto-manage network Channel selection, client Roaming, and Access Point (AP) utilization. 802.11k capable networks will automatically load balance network traffic across APs to improve network performance and prevent under or over-utilization of any one AP. 802.11k will eventually complement the 802.11e quality of service (QoS) standard by ensuring QoS for multimedia over a wireless link.

802.1p

802.1p is an extension of the IEEE 802 standard and is responsible for QoS provision. The primary purpose of 802.1p is to prioritize network traffic at the data link/ MAC layer. 802.1p offers the ability to filter multicast traffic to ensure it doesn't increase over layer 2 switched networks. It uses tag frames for the prioritization scheme. To be compliant with this standard, layer 2 switches must be capable of grouping incoming LAN packets into separate traffic classes.

802.1Q

IEEE 802.1Q is the IEEE standard for *Virtual Local Area Networks* (VLANs) specific to wireless technologies. (See <http://www.ieee802.org/1/pages/802.1Q.html>.)

The standard addresses the problem of how to break large networks into smaller parts to prevent broadcast and multicast data traffic from consuming more bandwidth than is necessary. 802.11Q also provides for better security between segments of internal networks. The 802.1Q specification provides a standard method for inserting VLAN membership information into Ethernet frames.

A

Access Point

An *access point* is the communication hub for the devices on a WLAN, providing a connection or bridge between wireless and wired network devices. It supports a Wireless Networking Framework called Infrastructure Mode.

When one access point is connected to a wired network and supports a set of wireless stations, it is referred to as a basic service set (BSS). An extended service set (ESS) is created by combining two or more BSSs.

Ad hoc Mode

Ad hoc mode is a Wireless Networking Framework in which stations communicate directly with each other. It is useful for quickly establishing a network in situations where formal infrastructure is not required.

Ad hoc mode is also referred to as *peer-to-peer mode* or an independent basic service set (IBSS).

AES

The *Advanced Encryption Standard* (AES) is a symmetric 128-bit block data encryption technique developed to replace DES encryption. AES works at multiple network layers simultaneously.

Further information is available on the NIST Web site.

Atheros XR (Extended Range)

Atheros Extended Range (XR) is a proprietary method for implementing low rate traffic over longer distances. It is meant to be transparent to XR enabled clients and access points and is designed to interoperate with the 802.11 standard in 802.11g and 802.11a modes. There is no support for Atheros XR in 802.11b, Atheros Turbo 5 GHz, or Atheros Dynamic Turbo 5 GHz.

B

Basic Rate Set

The *basic rate set* defines the transmission rates that are mandatory for any station wanting to join this wireless network. All stations must be able to receive data at the rates listed in this set.

Beacon

Beacon frames provide the "heartbeat" of a WLAN, announcing the existence of the network, and enabling stations to establish and maintain communications in an orderly fashion. It carries the following information (some of which is optional):

- The *Timestamp* is used by stations to update their local clock, enabling synchronization among all associated stations.
- The *Beacon interval* defines the amount of time between transmitting beacon frames. Before entering power save mode, a station needs the beacon interval to know when to wake up to receive the beacon.
- The *Capability Information* lists requirements of stations that want to join the WLAN. For example, it indicates that all stations must use WEP.
- The *Service Set Identifier (SSID)*.
- The Basic Rate Set is a bitmap that lists the rates that the WLAN supports.
- The optional *Parameter Sets* indicates features of the specific signaling methods in use (such as frequency hopping spread spectrum, direct sequence spread spectrum, etc.).
- The optional *Traffic Indication Map (TIM)* identifies stations, using power saving mode, that have data frames queued for them.

Bridge

A connection between two local area networks (LANs) using the same protocol, such as Ethernet or IEEE 802.1x.

Broadcast

A *Broadcast* sends the same message at the same time to everyone. In wireless networks, broadcast usually refers to an interaction in which the access point sends data traffic in the form

of IEEE 802.1x Frames to all client stations on the network. Some wireless security modes distinguish between how unicast, multicast, and broadcast frames are encrypted or whether they are encrypted. [See also Unicast and Multicast.](#)

Broadcast Address

[See IP Address.](#)

BSS

A *basic service set* (BSS) is an Infrastructure Mode Wireless Networking Framework with a single access point. Also see extended service set (ESS) and independent basic service set (IBSS).

BSSID

In Infrastructure Mode, the *Basic Service Set Identifier* (BSSID) is the 48-bit MAC address of the wireless interface of the Access Point.

C

CCMP

Counter mode/CBC-MAC Protocol (CCMP) is an encryption method for 802.11i that uses AES. It employs a CCM mode of operation, combining the Cipher Block Chaining Counter mode (CBC-CTR) and the Cipher Block Chaining Message Authentication Code (CBC-MAC) for encryption and message integrity.

AES-CCMP requires a hardware coprocessor to operate.

CGI

The *Common Gateway Interface* (CGI) is a standard for running external programs from an HTTP server. It specifies how to pass arguments to the executing program as part of the HTTP request. It may also define a set of environment variables.

A CGI program is a common way for an HTTP server to interact dynamically with users. For example, an HTML page containing a form can use a CGI program to process the form data after it is submitted.

Channel

The *Channel* defines the portion of the radio spectrum the radio uses for transmitting and receiving. Each 802.11 standard offers a number of channels, dependent on how the spectrum is licensed by national and transnational authorities such as the Federal Communications Commission (FCC), the European Telecommunications Standards Institute (ETSI), the Korean Communications Commission, or the Telecom Engineering Center (TELEC).

CSMA/CA

Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) is a low-level network arbitration/contention protocol. A station listens to the media and attempts to transmit a packet when the channel is quiet. When it detects that the channel is idle, the station transmits the packet. If it detects that the channel is busy, the station waits a random amount of time and then attempts to access the media again. CSMA/CA is the basis of the IEEE 802.11e Distributed Control Function (DCF). See also RTS and CTS. The CSMA/CA protocol used by 802.11 networks is a variation on CSMA/CD (used by Ethernet networks). In CSMA/CD the emphasis is on collision *detection* whereas with CSMA/CA the emphasis is on collision *avoidance*.

CTS

A *clear to send* (CTS) message is a signal sent by an IEEE 802.11 client station in response to an *request to send* (RTS) message. The CTS message indicates that the channel is clear for the sender of the RTS message to begin data transfer. The other stations will wait to keep the air waves clear. This message is a part of the IEEE 802.11 CSMA/CA protocol. (See also RTS.)

D

DCF

The *Distribution Control Function* is a component of the IEEE 802.11e Quality of Service (QoS) technology standard. The DCF coordinates channel access among multiple stations on a wireless network by controlling wait times for channel access. Wait times are determined by a random backoff timer which is configurable by defining minimum and maximum contention windows. [See also EDCF.](#)

DHCP

The *Dynamic Host Configuration Protocol* (DHCP) is a protocol specifying how a central server can dynamically provide network configuration information to clients. A DHCP server "offers" a "lease" (for a pre-configured period of time-see Lease Time) to the client system. The information supplied includes the client's IP addresses and netmask plus the address of its DNS servers and Gateway.

DNS

The *Domain Name Service* (DNS) is a general-purpose query service used for translating *fully-qualified names* into Internet addresses. A fully-qualified name consists of the hostname of a system plus its domain name. For example, `www` is the host name of a Web server and `www.Samsung Electronics.com` is the fully-qualified name of that server. DNS translates the domain name `www.Samsung Electronics.com` to some IP address, for example `66.93.138.219`. A *domain name* identifies one or more IP addresses. Conversely, an IP address may map to more than one domain name. A domain name has a suffix that indicates which *top*

level domain (TLD) it belongs to. Every country has its own top-level domain, for example *.de* for Germany, *.fr* for France, *.jp* for Japan, *.tw* for Taiwan, *.uk* for the United Kingdom, *.us* for the U.S.A., and so on. There are also *.com* for commercial bodies, *.edu* for educational institutions, *.net* for network operators, and *.org* for other organizations as well as *.gov* for the U. S. government and *.mil* for its armed services.

DOM

The *Document Object Model* (DOM) is an interface that allows programs and scripts to dynamically access and update the content, structure, and style of documents. The DOM allows you to model the objects in an HTML or XML document (text, links, images, tables), defining the attributes of each object and how they can be manipulated. Further details about the DOM can be found at the W3C.

DTIM

The *Delivery Traffic Information Map* (DTIM) message is an element included in some Beacon frames. It indicates which stations, currently sleeping in low-power mode, have data buffered on the Access Point awaiting pick-up. Part of the DTIM message indicates how frequently stations must check for buffered data.

Dynamic IP Address

[See IP Address.](#)

E

EAP

The *Extensible Authentication Protocol* (EAP) is an authentication protocol that supports multiple methods, such as token cards, Kerberos, one-time passwords, certificates, public key authentication, and smart cards. Variations on EAP include EAP Cisco Wireless (LEAP), Protected EAP (PEAP), EAP-TLS, and EAP Tunnelled TLS (EAP-TTLS).

EDCF

Enhanced Distribution Control Function is an extension of DCF. EDCF, a component of the IEEE Wireless Multimedia (WMM) standard, provides prioritized access to the wireless medium.

ESS

An *extended service set* (ESS) is an Infrastructure Mode Wireless Networking Framework with multiple access points, forming a single subnetwork that can support more clients than a basic service set (BSS). Each access point supports a number of wireless stations, providing broader wireless coverage for a large space, for example, an office.

Ethernet

Ethernet is a local-area network (LAN) architecture supporting data transfer rates of 10 Mbps to 1 Gbps. The Ethernet specification is the basis for the IEEE 802.3 standard, which specifies the physical and lower software layers. It uses the CSMA/CA access method to handle simultaneous demands. Ethernet supports data rates of 10 Mbps, *Fast Ethernet* supports 100 Mbps, and *Gigabit Ethernet* supports 1 Gbps. Its cables are classified as "XbaseY", where X is the data rate in Mbps and Y is the category of cabling. The original cable was *10base5* (Thicknet or "Yellow Cable"). Some others are *10base2* (Cheapernet), *10baseT* (Twisted Pair), and *100baseT* (Fast Ethernet). The latter two are commonly supplied using *CAT5* cabling with *RJ-45* connectors. There is also *1000baseT* (Gigabit Ethernet).

ERP

The *Extended Rate Protocol* refers to the protocol used by IEEE 802.11g stations (over 20 Mbps transmission rates at 2.4GHz) when paired with Orthogonal Frequency Division Multiplexing (OFDM). Built into ERP and the IEEE 802.11g standard is a scheme for effective interoperability of IEEE 802.11g stations with IEEE 802.11b nodes on the same channel. Legacy IEEE 802.11b devices cannot detect the ERP-OFDM signals used by IEEE 802.11g stations, and this can result in collisions between data frames from IEEE 802.11b and IEEE 802.11g stations. If there is a mix of 802.11b and 802.11g nodes on the same channel, the IEEE 802.11g stations detect this via an ERP flag on the access point and enable *request to send* (RTS) and *clear to send* (CTS) protection before sending data. [See also CSMA/CA protocol.](#)

F

Frame

A *Frame* consists of a discrete portion of data along with some descriptive meta-information packaged for transmission on a wireless network. Each frame includes a source and destination MAC address, a control field with protocol version, frame type, frame sequence number, frame body (with the actual information to be transmitted) and frame check sequence for error detection. A Frame is similar in concept to a Packet, the difference being that a packet operates on the Network layer (layer 3 in the OSI model) whereas a frame operates on the Data-Link layer (layer 2 in the OSI model).

G

Gateway

A *gateway* is a network node that serves as an entrance to another network. A gateway also often provides a proxy server and a firewall. It is associated with both a router, which use headers and forwarding tables to determine where packets are sent, and a switch or bridge, which provides the

actual path for the packet in and out of the gateway. Before a host on a LAN can access the Internet, it needs to know the address of its *default gateway*.

H

HTML

The *Hypertext Markup Language* (HTML) defines the structure of a document on the World Wide Web. It uses tags and attributes to hint about a layout for the document.

An HTML document starts with an `<html>` tag and ends with a `</html>` tag. A properly formatted document also contains a `<head> ... </head>` section, which contains the metadata to define the document, and a `<body> ... </body>` section, which contains its content. Its markup is derived from the *Standard Generalized Markup Language* (SGML), which is defined in ISO 8879:1986. HTML documents are sent from server to browser via HTTP. [Also see XML](#).

HTTP

The *Hypertext Transfer Protocol* (HTTP) defines how messages are formatted and transmitted on the World Wide Web. An HTTP message consists of a URL and a command (GET, HEAD, POST, etc.), a request followed by a response.

HTTPS

The Secure Hypertext Transfer Protocol (HTTPS) is the secure version of HTTP, the communication protocol of the World Wide Web. HTTPS is built into the browser. If you are using HTTPS you will notice a closed lock icon at the bottom corner of your browser page.

All data sent via HTTPS is encrypted, thus ensuring secure transactions take place.

I

IAPP

The *Inter Access Point Protocol* (IAPP) is an IEEE standard (802.11f) that defines communication between the access points in a "distribution system". This includes the exchange of information about mobile stations and the maintenance of bridge forwarding tables, plus securing the communications between access points.

IBSS

An *independent basic service set* (IBSS) is an Ad hoc Mode Wireless Networking Framework in which stations communicate directly with each other.

IEEE

The Institute of Electrical and Electronic Engineers (IEEE) is an international standards body that develops and establishes industry standards for a broad range of technologies, including the 802 family of networking and wireless standards. (See 802, 802.1x, 802.11, 802.11a, 802.11b, 802.11e, 802.11f, 802.11g, and 802.11i.) For more information about IEEE task groups and standards, see <http://standards.ieee.org/>.

Infrastructure Mode

Infrastructure Mode is a Wireless Networking Framework in which wireless stations communicate with each other by first going through an Access Point. In this mode, the wireless stations can communicate with each other or can communicate with hosts on a wired network. The access point is connected to a wired network and supports a set of wireless stations.

An infrastructure mode framework can be provided by a single access point (BSS) or a number of access points (BSS).

Intrusion Detection

The *Intrusion Detection System* (IDS) inspects all inbound network activity and reports suspicious patterns that may indicate a network or system attack from someone attempting to break into the system. It reports access attempts using unsupported or known insecure protocols.

IP

The *Internet Protocol* (IP) specifies the format of packets, also called datagrams, and the addressing scheme. IP is a connectionless, best-effort packet switching protocol. It provides packet routing, fragmentation and re-assembly. It is combined with higher-level protocols, such as TCP or UDP, to establish the virtual connection between destination and source. The current version of IP is *IPv4*. A new version, called *IPv6* or *IPng*, is under development. *IPv6* is an attempt to solve the shortage of IP addresses.

IP Address

Systems are defined by their *IP address*, a four-byte (octet) number uniquely defining each host on the Internet. It is usually shown in form 192.168.2.254. This is called dotted-decimal notation. An IP address is partitioned into two portions: the network prefix and a host number on that network. A Subnet Mask is used to define the portions. There are two special host numbers:

The Network Address consists of a host number that is all zeroes (for example, 192.168.2.0).

The Broadcast Address consists of a host number that is all ones (for example, 192.168.2.255).

There are a finite number of IP addresses that can exist. Therefore, a local area network typically uses one of the IANA-designated address ranges for use in private networks. These address ranges are:

10.0.0.0 to 10.255.255.255

172.16.0.0 to 172.31.255.255
192.168.0.0 to 192.168.255.255

A Dynamic IP Address is an IP address that is automatically assigned to a host by a DHCP server or similar mechanism. It is called dynamic because you may be assigned a different IP address each time you establish a connection. A Static IP Address is an IP address that is hard-wired for a specific host. A static address is usually required for any host that is running a server, for example, a Web server.

IPSec

IP Security (IPSec) is a set of protocols to support the secure exchange of packets at the IP layer. It uses shared public keys. There are two encryption modes: Transport and Tunnel.

- *Transport* mode encrypts only the data portion (payload) of each packet, but leaves the headers untouched.
- The more secure *Tunnel* mode encrypts both the header and the payload.

ISP

An *Internet Service Provider (ISP)* is a company that provides access to the Internet to individuals and companies. It may provide related services such as virtual hosting, network consulting, Web design, etc.

J

Jitter

Jitter is the difference between the latency (or delay) in packet transmission from one node to another across a network. If packets are not transmitted at a consistent rate (including Latency), QoS for some types of data can be affected. For example, inconsistent transmission rates can cause distortion in VoIP and streaming media. QoS is designed to reduce jitter along with other factors that can impact network performance.

L

Latency

Latency, also known as *delay*, is the amount of time it takes to transmit a Packet from sender to receiver. Latency can occur when data is transmitted from the access point to a client and vice versa. It can also occur when data is transmitted from access point to the Internet and vice versa. Latency is caused by *fixed network* factors such as the time it takes to encode and decode a packet, and also by *variable network* factors such as a busy or overloaded network. QoS features are designed to minimize latency for high priority network traffic.

LAN

A *Local Area Network* (LAN) is a communications network covering a limited area, for example, the computers in your home that you want to network together or a couple of floors in a building. A LAN connects multiple computers and other network devices such as storage and printers. Ethernet is the most common technology implementing a LAN.

Wireless Ethernet (802.11) is another very popular LAN technology (also see WLAN).

LDAP

The *Lightweight Directory Access Protocol* (LDAP) is a protocol for accessing on-line directory services. It is used to provide an authentication mechanism. It is based on the X.500 standard, but less complex.

Lease Time

The *Lease Time* specifies the period of time the DHCP Server gives its clients an IP Address and other required information. When the lease expires, the client must request a new lease. If the lease is set to a short span, you can update your network information and propagate the information provided to the clients in a timely manner.

LLC

The *Logical Link Control* (LLC) layer controls frame synchronization, flow control, and error checking. It is a higher level protocol over the PHY layer, working in conjunction with the MAC layer.

M

MAC

The *Media Access Control* (MAC) layer handles moving data packets between NICs across a shared channel. It is a higher level protocol over the PHY layer. It provides an arbitration mechanism in an attempt to prevent signals from colliding.

It uses a hardware address, known as the *MAC address*, that uniquely identifies each node of a network. IEEE 802 network devices share a common 48-bit MAC address format, displayed as a string of twelve (12) hexadecimal digits separated by colons, for example FE:DC:BA:09:87:65.

MDI and MDI-X

Medium Dependent Interface (MDI) and *MDI crossover* (MDIX) are twisted pair cabling technologies for Ethernet ports in hardware devices. Built-in twisted pair cabling and auto-sensing enable connection between like devices with the use of a standard Ethernet cable. (For example, if a wireless access point supports MDI/MDIX, one can successfully connect a PC and that access point with an Ethernet cable rather than having to use a crossover cable).

MIB

Management Information Base (MIB) is a virtual database of objects used for network management. SNMP agents along with other SNMP tools can be used to monitor any network device defined in the MIB.

MSCHAP V2

Microsoft Challenge Handshake Authentication Protocol Version 2 (MSCHAP V2) provides authentication for PPP connections between a Windows-based computer and an Access Point or other network access device.

MTU

The *Maximum Transmission Unit* is the largest physical packet size, measured in bytes, that a network can transmit. Any messages larger than the MTU are fragmented into smaller packets before being sent.

Multicast

A *Multicast* sends the same message to a select group of recipients. Sending an e-mail message to a mailing list is an example of multicasting. In wireless networks, multicast usually refers to an interaction in which the access point sends data traffic in the form of IEEE 802.1x Frames to a specified set of client stations (MAC addresses) on the network.

Some wireless security modes distinguish between how unicast, multicast, and broadcast frames are encrypted or whether they are encrypted.

N

NAT

Network Address Translation is an Internet standard that masks the internal IP addresses being used in a LAN. A NAT server running on a gateway maintains a translation table that maps all internal IP addresses in outbound requests to its own address and converts all inbound requests to the correct internal host.

NAT serves three main purposes: it provides security by obscurity by hiding internal IP addresses, enables the use of a wide range of internal IP addresses without fear of conflict with the addresses used by other organizations, and it allows the use of a single Internet connection.

Network Address

[See IP Address.](#)

NIC

A *Network Interface Card* is an adapter or expansion board inserted into a computer to provide a physical connection to a network. Most NICs are designed for a particular type of network, protocol, and media, for example, Ethernet or wireless.

NTP

The *Network Time Protocol* assures accurate synchronization of the system clocks in a network of computers. NTP servers transmit *Coordinated Universal Time* (UTC, also known as *Greenwich Mean Time*) to their client systems. An NTP client sends periodic time requests to servers, using the returned time stamp to adjust its clock.

O

OSI

The *Open Systems Interconnection* (OSI) reference model is a framework for network design. The OSI model consists of seven layers:

- Layer 1, the Physical layer, identifies the physical medium used for communication between nodes. In the case of wireless networks, the physical medium is air, and radio frequency (RF) waves are components of the physical layer.
- Layer 2, the Data-Link layer, defines how data for transmission will be structured and formatted, along with low-level protocols for communication and addressing. For example, protocols such as CSMA/CA and components like MAC addresses, and Frames are all defined and dealt with as a part of the Data-Link layer.
- Layer 3, the Network layer, defines the how to determine the best path for information traversing the network. Packets and logical IP Addresses operate on the network layer.
- Layer 4, the Transport layer, defines connection oriented protocols such as TCP and UDP.
- Layer 5, the Session layer, defines protocols for initiating, maintaining, and ending communication and transactions across the network. Some common examples of protocols that operate on this layer are network file system (NFS) and structured query language (SQL). Also part of this layer are communication flows like single mode (device sends information bulk), half-duplex mode (devices take turns transmitting information in bulk), and full-duplex mode (interactive, where devices transmit and receive simultaneously).
- Layer 6, the Presentation layer, defines how information is presented to the application. It includes meta-information about how to encrypt/decrypt and compress/decompress the data. JPEG and TIFF file formats are examples of protocols at this layer.
- Layer 7, the Application layer, includes protocols like hypertext transfer protocol (HTTP), simple mail transfer protocol (SMTP), and file transfer protocol (FTP).

P

Packet

Data and media are transmitted among nodes on a network in the form of *packets*. Data and multimedia content is divided up and packaged into *packets*. A packet includes a small chunk of the content to be sent along with its destination address and sender address. Packets are pushed out onto the network and inspected by each node. The node to which it is addressed is the ultimate recipient. -->

Packet Loss

Packet Loss describes the percentage of packets transmitted over the network that did not reach their intended destination. A 0 percent package loss indicates no packets were lost in transmission. QoS features are designed to minimize packet loss.

PHY

The Physical Layer (PHY) is the lowest layer in the network layer model (see OSI). The Physical Layer conveys the bit stream - electrical impulse, light or radio signal -- through the network at the electrical and mechanical level. It provides the hardware means of sending and receiving data on a medium, including defining cables, NICs, and physical aspects. Ethernet and the 802.11 family are protocols with physical layer components.

PID

The *Process Identifier* (PID) is an integer used by Linux to uniquely identify a process. A PID is returned by the `fork()` system call. It can be used by `wait()` or `kill()` to perform actions on the given process.

Port Forwarding

Port Forwarding creates a 'tunnel' through a firewall, allowing users on the Internet access to a service running on one of the computers on your LAN, for example, a Web server, an FTP or SSH server, or other services. From the outside user's point of view, it looks like the service is running on the firewall.

PPP

The *Point-to-Point Protocol* is a standard for transmitting network layer datagrams (IP packets) over serial point-to-point links. PPP is designed to operate both over asynchronous connections and bit-oriented synchronous systems.

PPPoE

Point-to-Point Protocol over Ethernet (PPPoE) is a specification for connecting the users on a LAN to the Internet through a common broadband medium, such as a single DSL or cable modem line.

PPtP

Point-to-Point Tunneling Protocol (PPtP) is a technology for creating a *Virtual Private Network* (within the *Point-to-Point Protocol (PPP)*). It is used to ensure that data transmitted from one VPN node to another are secure.

Proxy

A *proxy* is server located between a client application and a real server. It intercepts requests, attempting to fulfill them itself. If it cannot, it forwards them to the real server. Proxy servers have two main purposes: improve performance by spreading requests over several machines and filter requests to prevent access to specific servers or services.

PSK

Pre-Shared Key (PSK), see Shared Key.

Public Key

A *public key* is used in public key cryptography to encrypt a message which can only be decrypted with the recipient's private or secret key. Public key encryption is also called asymmetric encryption, because it uses two keys, or Diffie-Hellman encryption. Also see Shared Key.

Q

QoS

Quality of Service (QoS) defines the performance properties of a network service, including guaranteed throughput, transit delay, and priority queues. QoS is designed to minimize Latency, Jitter, Packet Loss, and network congestion, and provide a way of allocating dedicated bandwidth for high priority network traffic.

The IEEE standard for implementing QoS on wireless networks is currently in-work by the 802.11e task group. A subset of 802.11e features is described in the WMM specification.

R

RADIUS

The *Remote Authentication Dial-In User Service (RADIUS)* provides an authentication and accounting system. It is a popular authentication mechanism for many ISPs.

RC4

A symmetric stream cipher provided by RSA Security. It is a variable key-size stream cipher with byte-oriented operations. It allows keys up to 2048 bits in length.

Roaming

In IEEE 802.11 parlance, *roaming clients* are mobile client stations or devices on a wireless network (WLAN) that require use of more than one Access Point (AP) as they move out of and into range of different base station service areas. IEEE 802.11f defines a standard by which APs can communicate information about client associations and disassociations in support of roaming clients.

Router

A *router* is a network device which forwards packets between networks. It is connected to at least two networks, commonly between two local area networks (LANs) or between a LAN and a wide-area network (WAN), for example, the Internet. Routers are located at gateways-places where two or more networks connect.

A router uses the content of headers and its tables to determine the best path for forwarding a packet. It uses protocols such as the Internet Control Message Protocol (ICMP), Routing Information Protocol (RIP), and Internet Router Discovery Protocol (IRDP) to communicate with other routers to configure the best route between any two hosts. The router performs little filtering of data it passes.

RSSI

The *Received Signal Strength Indication* (RSSI) an 802.1x value that calculates voltage relative to the received signal strength. RSSI is one of several ways of measuring and indicating *radio frequency* (RF) signal strength. Signal strength can also be measured in mW (milliwatts), dBms (decibel milliwatts), and a percentage value.

RTP

Real-Time Transport Protocol (RTP) is an Internet protocol for transmitting real-time data like audio and video. It does not guarantee delivery but provides support mechanisms for the sending and receiving applications to enable streaming data. RTP typically runs on top of the UDP protocol, but can support other transport protocols as well.

RTS

A *request to send* (RTS) message is a signal sent by a client station to the access point, asking permission to send a data packet and to prevent other wireless client stations from grabbing the radio waves. This message is a part of the IEEE 802.11 CSMA/CA protocol. (See also RTS Threshold and CTS.)

RTS Threshold

The *RTS threshold* specifies the packet size of a request to send (RTS) transmission. This helps control traffic flow through the access point, and is especially useful for performance tuning on an access point with a many clients.

S

Shared Key

A *shared key* is used in conventional encryption where one key is used both for encryption and decryption. It is also called *secret-key* or *symmetric-key* encryption.

Also see Public Key.

SNMP

The *Simple Network Management Protocol* (SNMP) was developed to manage and monitor nodes on a network. It is part of the TCP/IP protocol suite.

SNMP consists of managed devices and their agents, and a management system. The agents store data about their devices in *Management Information Bases* (MIBs) and return this data to the SNMP management system when requested.

SNMP Traps

SNMP traps enable the asynchronous communication from network devices to managed agents. Setting SNMP traps saves on network resources and eliminates redundant SNMP requests.

SSID

The *Service Set Identifier* (SSID) is a thirty-two character alphanumeric key that uniquely identifies a wireless local area network. It is also referred to as the *Network Name*. There are no restrictions on the characters that may be used in an SSID.

Static IP Address

[See IP Address.](#)

STP

The *Spanning Tree Protocol* (STP) is an IEEE 802.1 standard protocol (related to network management) for MAC bridges that manages path redundancy and prevents undesirable loops in the network created by multiple active paths between client stations. Loops occur when there are multiple routes between access points. STP creates a tree that spans all of the switches in an extended network, forcing redundant paths into a standby or blocked state. STP allows only one active path at a time between any two network devices (this prevents the loops), but establishes the redundant links as a backup if the initial link should fail. If STP costs change, or if one

network segment in the STP becomes unreachable, the spanning tree algorithm reconfigures the spanning tree topology and reestablishes the link by activating the standby path. Without STP in place, it is possible that both connections may be simultaneously live, which could result in an endless loop of traffic on the LAN.

Subnet Mask

A *Subnet Mask* is a number that defines which part of an IP address is the network address and which part is a host address on the network. It is shown in dotted-decimal notation (for example, a 24-bit mask is shown as 255.255.255.0) or as a number appended to the IP address (for example, 192.168.2.0/24).

The subnet mask allows a router to quickly determine if an IP address is local or needs to be forwarded by performing a bitwise AND operation on the mask and the IP address. For example, if an IP address is 192.168.2.128 and the netmask is 255.255.255.0, the resulting Network address is 192.168.2.0.

The bitwise AND operator compares two bits and assigns 1 to the result only if both bits are 1. The following table shows the details of the netmask:

IP address	192.168.2.128	11000000 10101000 00000010 10000000
Netmask	255.255.255.0	11111111 11111111 11111111 00000000
Resulting network address	192.168.2.0	11000000 10101000 00000010 00000000

Supported Rate Set

The *supported rate set* defines the transmission rates that are available on this wireless network. A station may be able to receive data at any of the rates listed in this set. All stations must be able to receive data at the rates listed in the Basic Rate Set.

SVP

SpectraLink Voice Priority (SVP) is a QoS approach to Wi-Fi deployments. SVP is an open specification that is compliant with the IEEE 802.11b standard. SVP minimizes delay and prioritizes voice packets over data packets on the Wireless LAN, thus increasing the probability of better network performance.

T

TCP

The *Transmission Control Protocol* (TCP) is built on top of Internet Protocol (IP). It adds reliable communication (guarantees delivery of data), flow-control, multiplexing (more than one

simultaneous connection), and connection-oriented transmission (requires the receiver of a packet to acknowledge receipt to the sender). It also guarantees that packets will be delivered in the same order in which they were sent.

TCP/IP

The Internet and most local area networks are defined by a group of protocols. The most important of these is the *Transmission Control Protocol over Internet Protocol* (TCP/IP), the de facto standard protocols. TCP/IP was originally developed by Defense Advanced Research Projects Agency (DARPA, also known as ARPA, an agency of the US Department of Defense).

Although TCP and IP are two specific protocols, TCP/IP is often used to refer to the entire protocol suite based upon these, including ICMP, ARP, UDP, and others, as well as applications that run upon these protocols, such as telnet, FTP, etc.

TKIP

The *Temporal Key Integrity Protocol* (TKIP) provides an extended 48-bit initialization vector, per-packet key construction and distribution, a Message Integrity Code (MIC, sometimes called "Michael"), and a re-keying mechanism. It uses a RC4 stream cipher to encrypt the frame body and CRC of each 802.11 frame before transmission. It is an important component of the WPA and 802.11i security mechanisms.

ToS

TCP/IP packet headers include a 3-to-5 bit *Type of Service* (ToS) field set by the application developer that indicates the appropriate type of service for the data in the packet. The way the bits are set determines whether the packet is queued for sending with minimum delay, maximum throughput, low cost, or mid-way "best-effort" settings depending upon the requirements of the data. The ToS field is used by the SMT-R2000 to provide configuration control over *Quality of Service* (QoS) queues for data transmitted from the AP to client stations.

U

UDP

The *User Datagram Protocol* (UDP) is a transport layer protocol providing simple but unreliable datagram services. It adds port address information and a checksum to an IP packet.

UDP neither guarantees delivery nor does it require a connection. It is lightweight and efficient. All error processing and retransmission must be performed by the application program.

Unicast

A *Unicast* sends a message to a single, specified receiver. In wireless networks, unicast usually refers to an interaction in which the access point sends data traffic in the form of IEEE 802.1x

Frames directly to a single client station MAC address on the network. Some wireless security modes distinguish between how unicast, multicast, and broadcast frames are encrypted or whether they are encrypted. [See also Multicast and Broadcast.](#)

URL

A *Uniform Resource Locator* (URL) is a standard for specifying the location of objects on the Internet, such as a file or a newsgroup. URLs are used extensively in HTML documents to specify the target of a hyperlink which is often another HTML document (possibly stored on another computer). The first part of the URL indicates what protocol to use and the second part specifies the IP address or the domain name where that resource is located.

For example, `ftp://ftp.Samsung Electronics.com/downloads/myfile.tar.gz` specifies a file that should be fetched using the FTP protocol; `http://www.Samsung Electronics.com/index.html` specifies a Web page that should be fetched using the HTTP protocol.

V

VLAN

A *virtual LAN* (VLAN) is a software-based, logical grouping of devices on a network that allow them to act as if they are connected to a single physical network, even though they may not be. The nodes in a VLAN share resources and bandwidth, and are isolated on that network. The SMT-R2000 supports the configuration of a wireless VLAN. This technology is leveraged on the access point for the "virtual" guest network feature.

VPN

A *Virtual Private Network* (VPN) is a network that uses the Internet to connect its nodes. It uses encryption and other mechanisms to ensure that only authorized users can access its nodes and that data cannot be intercepted.

W

WAN

A *Wide Area Network* (WAN) is a communications network that spans a relatively large geographical area, extending over distances greater than one kilometer. A WAN is often connected through public networks, such as the telephone system. It can also be connected through leased lines or satellites. The Internet is essentially a very large WAN.

WDS

A *Wireless Distribution System* (WDS) allows the creation of a completely wireless infrastructure. Typically, an Access Point is connected to a wired LAN. WDS allows access points to be connected wirelessly. The access points can function as wireless repeaters or bridges.

WEP

Wired Equivalent Privacy (WEP) is a data encryption protocol for 802.11 wireless networks. All wireless stations and access points on the network are configured with a static 64-bit (40-bit secret key + 24-bit initialization vector (IV)) or 128-bit (104-bit secret key + 24-bit IV) Shared Key for data encryption. It uses a RC4 stream cipher to encrypt the frame body and CRC of each 802.11 frame before transmission.

Wi-Fi

A test and certification of interoperability for WLAN products based on the IEEE 802.11 standard promoted by the Wi-Fi Alliance, a non-profit trade organization.

WINS

The *Windows Internet Naming Service* (WINS) is a server process for resolving Windows-based computer names to IP addresses. It provides information that allows these systems to browse remote networks using the *Network Neighborhood*.

Wireless Networking Framework

There are two ways of organizing a wireless network:

- Stations communicate directly with one another in an Ad hoc Mode network, also known as an independent basic service set (IBSS).
- Stations communicate through an Access Point in an Infrastructure Mode network. A single access point creates an infrastructure basic service set (BSS) whereas multiple access points are organized in an extended service set (ESS).

WLAN

Wireless Local Area Network (WLAN) is a LAN that uses high-frequency radio waves rather than wires to communicate between its nodes.

WMM

Wireless Multimedia (WMM) is a IEEE technology standard designed to improve the quality of audio, video and multimedia applications on a wireless network. Both access points and wireless clients (laptops, consumer electronics products) can be WMM-enabled. WMM features are based on a subset of the WLAN IEEE 802.11e draft specification. Wireless products that are built to the standard and pass a set of quality tests can carry the "Wi-Fi certified for WMM" label to

ensure interoperability with other such products. For more information, see the WMM page on the Wi-Fi Alliance Web site: <http://www.wi-fi.org/OpenSection/wmm.asp>.

WPA

Wi-Fi Protected Access (WPA) is a Wi-Fi Alliance version of the draft IEEE 802.11i standard. It provides more sophisticated data encryption than WEP and also provides user authentication. WPA includes TKIP and 802.1x mechanisms.

WPA2

Wi-Fi Protected Access (WPA2) is an enhanced security standard, described in IEEE 802.11i, that uses Advanced Encryption Standard (AES) for data encryption.

The original WPA uses Temporal Key Integrity Protocol (TKIP) for data encryption. WPA2 is backwards-compatible with products that support the original WPA.

WPA2, like the original WPA, supports an *Enterprise* and *Personal* version. The Enterprise version requires use of IEEE 802.1x security features and *Extensible Authentication Protocol* (EAP) authentication with a RADIUS server.

The Personal version does not require IEEE 802.1x or EAP. It uses a *Pre-Shared Key* (PSK) password to generate the keys needed for authentication.

WRAP

Wireless Robust Authentication Protocol (WRAP) is an encryption method for 802.11i that uses AES but another encryption mode (OCB) for encryption and integrity.

X

XML

The *Extensible Markup Language* (XML) is a specification developed by the W3C. XML is a simple, flexible text format derived from *Standard Generalized Markup Language* (SGML), which is defined in ISO 8879:1986, designed especially for electronic publishing.