Ed. 00

SMT-R2000
Administration Guide

SAMSUNG ELECTRONICS

COPYRIGHT

TRADEMARKS

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

This manual should be read and used as a guideline for properly installing and operating the product.

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

If you need updated manuals or have any questions concerning the contents of the manuals, contact our **Document Center** at the following address or Web site:

Address: Document Center 18th Floor IT Center. Dong-Suwon P.O. Box 105, 416, Maetan-3dong Yeongtong-gu, Suwon-si, Gyeonggi-do, Korea 442-600

Homepage: http://www.samsungdocs.com

INTRODUCTION

Purpose

This Guide describes input field, function setting and monitoring on Web based User Interface for SMT-R2000. This information is provided for the people who install and administrate SMT-R2000 for the construction of IT infra network for home & small and mid-sized company.

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.

Features, Supported Browsers and Restrictions of Guide

Guide for SMT-R2000 administration page provides the information on all items and function available on user interface.

The information of Guide corresponds with each menu item on the user interface for SMT-R2000 administrator. For the help for the setting of the current tab, click the **Help** button of the current tab or the '**More . . .**' link at the bottom of the help panel on the user interface.

- Click a link(blue underlined text) to check a relevant comment.
- Use the Back/Forward button to move a page(link *history*).
- Click the 'TOC' icon to check all help items.

Recommended Settings, Cautions and Warning


The information following an arrow(basically, in the table) means its recommended setting for Access Point(AP) option.

- **Note** provides the feature and the description for the related item and the information for its comment.
- **Caution** provides the information on the important property of AP setting, the combination of setting, and the procedures that have bad influences for events, network connection, and security.

Notation format

This guide adopts the following notation format:

Italic	Terminologies, new terminologies, and titles
`Screen Font`	Texts, URLs, IP addresses, MAC addresses, Unix files, commands, directory names, and user-typed command-line entries
`Screen Font Italic`	Variables
Bold Font	Menu titles, window names, and button names

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

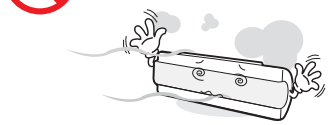
Indication for prohibiting an action for a product

Instruction

Indication for commanding a specifically required action

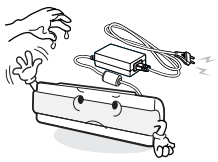
WARNING

Power



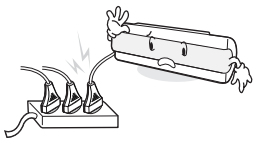
Do not install the product in a humid or dusty area.

This is to prevent electrocution and fire.



Do not touch the plug with wet hands.

This is to prevent electrocution and fire.

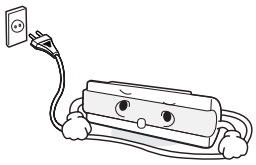


Do not use with product lying down.

This is to ensure normal operation.

Insert the power plug fully and firmly into the outlet.

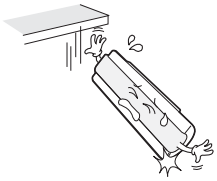
This is to prevent electrocution and fire.



Unplug the power cable when not using the product for a long time.

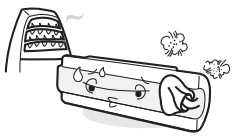
This is to prevent electrocution and fire.

Installation/Storage



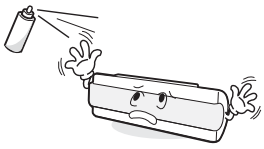
Be careful not to drop the product.

This is to prevent product damage



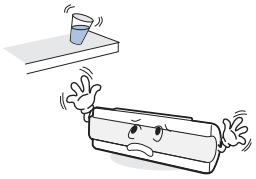
Do not install the product near heating apparatus(e.g., heater and cigarette fire).

This is to prevent electrocution and fire.



Do not use or keep combustible sprays or flammable objects near this product.

This is to prevent electrocution and fire.

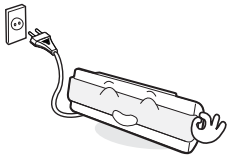


Do not place water cups, chemicals, or metals above the product.

This is to prevent electrocution and fire.

CAUTION

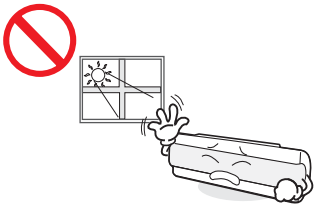
Power



Connect the power adapter provided with the product, to the power connection port.

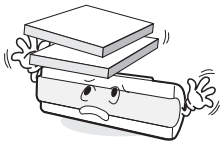
Using adapters other than that provided may seriously damage the product or cause fire or electrocution.

Installation/Storage



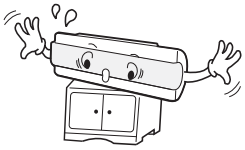
Do not install the product under direct sunlight.

This is to prevent parts of the product from being damaged.



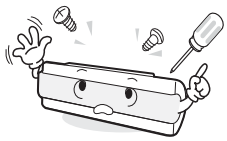
Do not place heavy objects on top of the product.

This is to prevent product damage..



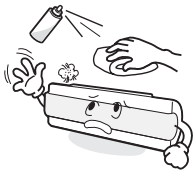
Do not install the product on unstable places.

This is protect the product to falling.



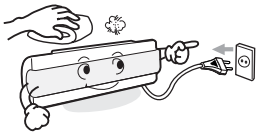
Do not disassemble, repair or modify the product without proper authorization.

Please contact your reseller or service center for repairs..



Do not clean the product with chemicals such as wax, benzene, alcohol, thinner, insecticide, air freshener, lubricant, and detergent.

Doing so may discolor or damage the product.



Clean the product with a dry cloth after unplugging the power cord.

This is to prevent product damage.

This page is intentionally left blank.

TABLE OF CONTENTS

INTRODUCTION I

Purpose I
Conventions I
Features, Supported Browsers and Restrictions of Guide II
Recommended Settings, Cautions and Warning II
Notation format II

SAFETY CONCERNS III

Symbols III
Warning IV
Caution V

CHAPTER 1. Basic Settings 1-1

1.1 Summary of Basic AP Setup Status 1-1
1.2 Network Setup 1-2
1.3 Update of Basic Setup 1-2
1.4 Summary of Basic Setup Status 1-3
1.5 Change of Web page Language and Setup 1-3
1.5.1 Locale 1-3
1.5.2 Font Size 1-3
1.5.3 Color Schemes 1-3

CHAPTER 2. Managing Access Points and Clusters 2-1

2.1 Understanding Clustering 2-1
2.1.1 What is a Cluster? 2-1
2.1.2 How Many APs Can a Cluster Support? 2-2
2.1.3 What Kinds of APs Can Cluster Together? 2-2
2.1.4 Which Settings are shared as Part of the Cluster Configuration and Which Are Not? 2-2
2.1.5 Cluster Mode 2-3
2.1.6 Standalone Mode 2-4

2.1.7 Auto-Sync of Cluster Configuration 2-5

2.2 Understanding Access Point Settings 2-6

2.3 Modifying the Location Description 2-6

2.4 Removing an Access Point from the Cluster 2-7

2.5 Adding an Access Point to a Cluster 2-7

2.6 Navigating to Configuration Information for a Specific AP and Managing Standalone APs 2-8

2.6.1 Navigating to an AP by Using its IP Address in a URL 2-8

CHAPTER 3. Ethernet Settings 3-1

3.1 DNS Name Setting 3-1

3.2 Use Guest Access 3-1

3.2.1 Internal LAN and Guest Network Setting 3-1

3.2.2 Whether to Use Guest Access 3-2

3.2.3 Specifying a Physical or Virtual Guest Network 3-2

3.3 Enabling or Disabling Virtual Wireless Networks on the AP 3-3

3.4 Configuring LAN or Internal Interface Ethernet Settings 3-4

3.5 Configuring Guest Interface Ethernet (Wired) Settings 3-5

3.6 Update Settings 3-5

CHAPTER 4. Wireless settings 4-1

4.1 802.11h Regulatory Domain Control 4-1

4.2 Setting the Wireless 4-2

4.3 'Internal' Wireless LAN Setting 4-3

4.4 'Guest' Wireless LAN setting 4-3

4.5 Update setting 4-4

CHAPTER 5. Security settings 5-1

5.1 Blocking Network via Station Isolation 5-1

5.2 SSID View, Station Isolation, Security Mode 5-2

5.2.1 None (Plain-text) 5-2

5.2.2 Static WEP 5-3

5.2.3 IEEE 802.1x 5-5

5.2.4 WPA Personal 5-6

5.2.5 WPA Enterprise 5-7

5.3 Update settings 5-8

CHAPTER 6. Virtual Wireless Network Settings 6-1

6.1 VLAN Setting 6-1

6.2 Update settings 6-3

CHAPTER 7. Radio Settings 7-1

7.1 FCC CONCERNS 7-4

7.1.1 FCC Compliance Statement 7-4

7.1.2 FCC Compliance Statement 7-4

7.2 Notice for European Community 7-5

7.2.1 Countries of Operation & Conditions of Use 7-5

7.2.2 GHz Operations: 7-5

7.2.3 GHz Operation: 7-6

7.2.4 Operation Using 5 GHz Channels in the European Community 7-6

7.2.5 Transmit Power Control (TPC) for 5 GHz operation 7-7

7.3 Updating Settings 7-7

CHAPTER 8. MAC Address Filtering settings 8-1

8.1 Using MAC Filtering 8-1

8.2 Settings Update 8-2

CHAPTER 9. Load Balancing settings 9-1

9.1 Load Balancing Settings 9-1

9.2 Update settings 9-2

CHAPTER 10. Port Forwarding settings 10-1

10.1 Using Port Forward 10-1

10.2 Update Settings 10-2

CHAPTER 11. Port Control settings 11-1

11.1 Using Port Control 11-1

11.2 Update Settings 11-2

CHAPTER 12. Quality of Service (QoS) settings 12-1

12.1 QoS Setup 12-1

12.1.1 AP EDCA Parameter Setup 12-2

12.1.2 Wi-Fi Multimedia 12-3
12.1.3 Station EDCA Parameter Setup 12-4
12.1.4 Retry Number Setup 12-5
12.1.5 Priority Setup 12-5
12.2 Update settings 12-6

CHAPTER 13. Wireless Distribution System (WDS) Settings 13-1

13.1 WDS settings 13-1
13.1.1 Setting WDS Link Security Mode to None 13-3
13.1.2 Setting WDS Link Security Mode to WEP 13-3
13.1.3 Setting WDS Link Security Mode to WPA(PSK) 13-4
13.2 Update Settings 13-4

CHAPTER 14. Simple Network Management Protocol (SNMP) settings 14-1

14.1 SNMP Setting 14-1
14.1.1 SNMP Traps Setting 14-2
14.2 Update Settings 14-3

CHAPTER 15. Network Time Protocol Server settings 15-1

15.1 Using NTP Server/Not Using NTP Server 15-1
15.2 Update Settings 15-2

CHAPTER 16. View Interface Information 16-1

16.1 Ethernet (Wired) Settings 16-1
16.2 Wireless Settings 16-1

CHAPTER 17. View Event Logs 17-1

17.1 For Remote Login 17-1
17.2 Log Relay Host Setting 17-2
17.3 Activation/Deactivation of Log Relay Function > Event Page 17-3
17.4 Storing Settings 17-3
17.5 Event 17-3

CHAPTER 18. View Transmit/Receive Statistics 18-1

CHAPTER 19. View Accessed Client Terminal List 19-1

19.1 Link Integrity Monitoring 19-1

19.2 What is difference between Association and Session? 19-1

CHAPTER 20. View Neighboring AP List 20-1

CHAPTER 21. AP Configuration Management 21-1

21.1 Restoring Initial Factory Setup 21-1

21.2 Storing the Current Settings as a Backup File 21-2

21.3 Restore the Settings from Previous File Stored 21-2

21.4 AP Rebooting 21-2

CHAPTER 22. Firmware Upgrade 22-1

22.1 Update 22-2

22.2 Checking Firmware Upgrade 22-2

This page is intentionally left blank.

CHAPTER 1. Basic Settings

1.1 Summary of Basic AP Setup Status

Item	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	Shows the MAC address of an AP. 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. This address is an address to be known to other Networks. To check Guest or Internal interface of AP, refer to **Status > Interface.**
Firmware Version	Show the version information of a firmware currently installed in AP. Whenever the new version of SMT-R2000 firmware is released, the firmware is upgraded to enable to use AP with the strengthened function. For the method to upgrade of a firmware, refer to Firmware Upgrade.
Country Code	Chooses AP-using country. When you change the country code, beware of channel setup. NOTE: When you change the country code, you must reboot after completing the update.
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.

1.2 Network Setup

Items	Description
Current Password	Enter the current administrator password. Before you change the password, you must enter the current password exactly. If the password is correct, the check mark is displayed and the following items can be changed.
New Password	Enter a new administrator password. The letters you entered are displayed as '*' not to show to others. The administrator's password should be alphabetical string with 8-letter at maximum length. As the first step for Radio LAN security, it is recommended to change the administrator password.
Confirmation of New Password	Re-enter the administrator password to confirm the new administrator password.
802.11a, 802.11b/g (SSID)	Enter the name of radio Network as a string. This name will be applied to all APs over the network. Whenever APs are added, the APs will share this SSID. *Service Set Identifier*(SSID) is an alphabetical and numerical string with 32 letters at maximum length. 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.

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.

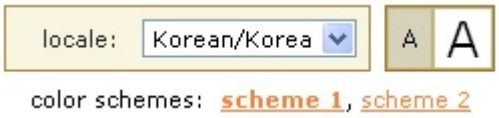
1.3 Update of Basic Setup

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

1.4 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.

1.5 Change of Web page Language and Setup



The design panels 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

1.5.1 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.

1.5.2 Font Size

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

configuration	Description
	Normal
	Large

1.5.3 Color Schemes

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

configuration	Description
Scheme 1	Changes the colors into Grey and Blue.
Scheme 2	Changes the colors into Grey and White.

This page is intentionally left blank.

CHAPTER 2. Managing Access Points and Clusters

The Samsung SMT-R2000 shows current basic configuration settings for clustered access points(location, IP address, MAC address, status, and availability) and provides a way of navigating to the full configuration for specific APs if they are cluster members. Standalone access points or those which are not members of this cluster do not show up in this listing. To configure standalone access points, you must discover(via Kickstart) or know the IP address of the access point and by using its IP address in a URL(`http://IPAddressOfAccessPoint`).


NOTE

The Samsung SMT-R2000 is not designed for multiple, simultaneous configuration changes. If you have a network that includes multiple access points, and more than one administrator is logged on to the Administration Web pages and making changes to the configuration, all access points in the cluster will stay in sync but there is no guarantee that all configuration changes specified by multiple users will be applied.

2.1 Understanding Clustering

A key feature of the Samsung SMT-R2000 is the ability to form a dynamic, configuration-aware group(called a *cluster*) with other Samsung Reference APs in a network in the same subnet. Access points can participate in a self-organizing cluster which makes it easier for you to deploy, administer, and secure your wireless network. The cluster provides a single point of administration and lets you view the deployment of access points as a single wireless network rather than a series of separate wireless devices.

2.1.1 What is a Cluster?

A cluster is a group of access points which are coordinated as a single group via Samsung SMT-R2000 administration. You cannot create multiple clusters on a single wireless network(SSID). Only one cluster per wireless network is supported.

2.1.2 How Many APs Can a Cluster Support?

Up to twelve access points are supported in a cluster at any one time. If a new AP is added to a network with a cluster that is already at full capacity, the new AP is added in *stand-alone mode*. Note that when the cluster is full, extra APs are added in stand-alone mode regardless of the configuration policy in effect for new access points.
For related information, see Cluster Mode, Standalone Mode, and Set Configuration Policy for New Access Points.

2.1.3 What Kinds of APs Can Cluster Together?

A single Samsung SMT-R2000 can form a cluster with itself(a ‘cluster of one’) and with other Samsung Reference APs of the same model. In order to be members of the same cluster, access points must be:

- Of the same radio configuration(all one-radio APs or all two-radio APs)
- Of the same band configuration(all single-band APs or all dual-band APs)
- On the same LAN

Having a mix of APs on the network does not adversely affect Samsung SMT-R2000 clustering in any way. However, it is helpful to understand the clustering behavior for administration purposes:

- Access points of the same model will form a cluster.
- Access points of other brands will not join the cluster. These APs should be administered with their own associated Administration tools.

2.1.4 Which Settings are shared as Part of the Cluster Configuration and Which Are Not?

Most configuration settings defined via the Samsung SMT-R2000 Administration Web pages will be propagated to cluster members as a part of the *cluster configuration*.

Settings Shared in the Cluster Configuration

The cluster configuration includes:

- Network name(SSID)
- Administrator password
- Configuration policy
- User accounts and authentication
- Wireless interface settings
- Guest Welcome screen settings
- Network Time Protocol(NTP) settings
- Radio settings
- Security settings

- QoS queue parameters
- MAC address filtering

Only Mode, Channel, Fragmentation Threshold, RTS Threshold and Rate Sets are synchronized across the cluster. Beacon Interval, DTIM Period, Maximum Stations, and Transmit Power do not cluster.


NOTE

When Channel Planning is enabled, the radio Channel is not synced across the cluster. See Stopping/Starting Automatic Channel Assignment.

When Channel Planning is enabled, the radio Channel is not synced across the cluster. See Stopping/Starting Automatic Channel Assignment

Settings Not Shared by the Cluster

The few exceptions(settings *not* shared among clustered access points) are the following, most of which by nature must be unique:

- IP addresses
- MAC addresses
- Location descriptions
- Load Balancing settings
- WDS bridges
- Ethernet(Wired) Settings, including enabling or disabling Guest access
- Guest interface configuration

Settings that are not shared must be configured individually on the Administration pages for each access point. To get to the Administration pages for an access point that is a member of the current cluster, click on its IP Address link on the **Cluster** > **Access Points** page of the current AP.

2.1.5 Cluster Mode

When an access point is a cluster member, it is considered to be in cluster mode. You define whether you want new access points to join the cluster or not via the configuration policy you set in the Basic Settings.(See Setting Configuration Policy for New Access Points.) You can re-set an access point in cluster mode to standalone mode.(See Removing an Access Point from the Cluster.)


NOTE

When the cluster is full(twelve APs is the limit), extra APs are added in *stand-alone mode* regardless of the configuration policy in effect for new access points. See How Many APs Can a Cluster Support?.

2.1.6 Standalone Mode

The Samsung SMT-R2000 can be configured in *standalone* mode. In standalone mode, an access point is not a member of the cluster and does not share the cluster configuration, but rather requires manual configuration that is not shared with other access points.(See Set Configuration Policy for New Access Points and Removing an Access Point from the Cluster.)

Standalone access points are not listed on the **Cluster** > **Access Points** tab in the Administration UIs of APs that are cluster members. You need to know the IP address for standalone access points in order to configure and manage it directly.(See Navigating to an AP by Using its IP Address in a URL.)

The **Basic Settings** tab for a standalone access point indicates only that the current mode is standalone and provides a button for adding the access point to a cluster. If you click on any of the **Cluster** tabs on the Administration pages for an access point in standalone mode, you will be redirected to the Basic Settings page because Cluster settings do not apply to standalone APs.


NOTE

When the cluster is full (twelve APs is the limit), extra APs are added in *stand-alone mode* regardless of the configuration policy in effect for new access points. See How Many APs Can a Cluster Support?.

You can re-enable cluster mode on a standalone access point.(See Adding an Access Point to a Cluster.)

For purposes of ease-of-use, the clustering component is designed to let new devices join a cluster without strong authentication. However, communications of all data between access points in a cluster is protected against casual eavesdropping using Secure Sockets Layer(typically referred to as SSL). The assumption is that the private wired network to which the devices are connected is secure. Both the cluster configuration file and the user database are transmitted among access points using SSL.

2.1.7 Auto-Sync of Cluster Configuration

If you are making changes to the AP configuration that require a relatively large amount of processing(such as adding several new users), you may encounter a synchronization progress bar after clicking ‘Update’ on any of the Administration pages. The progress bar indicates that the system is busy performing an auto-synch of the updated configuration to all APs in the cluster. The Administration Web pages are not editable during the auto-synch.

Note that auto-synchronization always occurs during configuration updates that affect the cluster, but the processing time is usually negligible. The auto-sync progress bar is displayed only for longer-than-usual wait times.

2.2 Understanding Access Point Settings

The **Access Points** tab provides information about all access points in the cluster.

From this tab, you can view location descriptions, IP addresses, enable(activate) or disable(deactivate) *clustered* access points, and remove access points from the cluster. You can also modify the location description for an access point.

The IP address links provide a way to navigate to configuration settings and data on an access point.
Stand-alone access points(those which are not members of the cluster) are not shown on this page.

The following table describes the access point settings and information display in detail.

Field	Description
Location	Description of where the access point is physically located.
MAC Address	Media Access Control(MAC) address of the access point. 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 the access point. The address shown here is the MAC address for the bridge(`br0`). This is the address by which the AP is known externally to other networks. To see MAC addresses for Guest and Internal interfaces on the AP, see the **Status > Interfaces** tab.
IP Address	Specifies the IP address for the access point. Each IP address is a link to the Administration Web pages for that access point. You can use the links to navigate to the Administration Web pages for a specific access point. This is useful for viewing data on a specific access point to make sure a cluster member is picking up cluster configuration changes, to configure advanced settings on a particular access point, or to switch a standalone access point to cluster mode.

2.3 Modifying the Location Description

To make modifications to the location description:

1) Navigate to the **Basic Settings** tab.
2) Update the Location description in section 1 under ‘Review Description of this Access Point.’
3) Click the **Update** button to apply the changes.

2.4 Removing an Access Point from the Cluster

To remove an access point from the cluster, do the following.

1) Click the checkbox next to the access point so that the box is checked.
2) Click the **Remove** button to remove the access point from the Cluster.

The change will be reflected under Status for that access point; the access point will now show as *standalone*(instead of *cluster*).

In some situations it is possible for the cluster to become out of sync. If after removing an access point from the cluster, the AP list still reflects the deleted AP or shows an incomplete display; refer to the information on Cluster Recovery in Appendix B: Troubleshooting in the Administrators Guide.

2.5 Adding an Access Point to a Cluster

To add an access point that is currently in standalone mode back into a cluster, do the following.

1) Go to the Administration Web pages for the standalone access point.(See Navigating to an AP by Using its IP Address in a URL.)
   The Administration Web pages for the standalone access point are displayed.

2) Click the **Basic Settings** tab in the Administration pages for the standalone access point.
   The **Basic Settings** tab for a standalone access point indicates that the current mode is standalone and provides a button for adding the access point to a cluster(group).

If you click on any of the Cluster tabs on the Administration pages for an access point in standalone mode, you will be redirected to the Basic Settings page because Cluster settings do not apply to stand-alone APs.

3) Click the **Join Cluster** button.
   The access point is now a cluster member. It's Status(Mode) on the **Cluster** > **Access Points** tab now indicates 'cluster' instead of 'standalone'.

In some situations it is possible for the cluster to become out of sync. If after removing an access point from the cluster, the AP list still reflects the deleted AP or shows an incomplete display; refer to the information on Cluster Recovery in Appendix B: Troubleshooting in the Administrators Guide.

2.6 Navigating to Configuration Information for a Specific AP and Managing Standalone APs

In general, the Samsung SMT-R2000 is designed for central management of *clustered* access points. For access points in a cluster, all access points in the cluster reflect the same configuration. In this case, it does not matter which access point you actually connect to for administration.

There may be situations, however, when you want to view or manage information on a particular access point. For example, you might want to check status information such as client associations or events for an access point. Or you might want to configure and manage features on an access point that is running in *standalone* mode. In these cases, you can navigate to the Administration Web interface for individual access points by clicking the IP address links on the **Access Points** tab.

All clustered access points are shown on the **Cluster > Access Points** page. To navigate to clustered access points, you can simply click on the IP address for a specific cluster member shown in the list.

2.6.1 Navigating to an AP by Using its IP Address in a URL

You can also link to the Administration Web pages of a specific access point, by entering the IP address for that access point as a URL directly into a Web browser address bar in the following form:

`http://IPAddressOfAccessPoint`

where *IPAddressOfAccessPoint* is the address of the particular access point you want to monitor or configure.
For standalone access points, this is the only way to navigate to their configuration information.
If you do not know the IP address for a standalone access point, use Kickstart to find all APs on the network and you should be able to derive which ones are standalone by comparing Kickstart findings with access points listed on the **Cluster > Access Points** tab. The APs that Kickstart finds that are not shown on this tab are probably standalone APs.

CHAPTER 3. Ethernet Settings

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


NOTE

In this page, 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.

3.1 DNS Name Setting

Item	Description
DNS Name	Enter the DNS name for the access point in the text box. This is the host name. It may be provided by your ISP or network administrator, or you can provide your own. The rules for system names are: - 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.

3.2 Use Guest Access

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

3.2.1 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.)

3.2.2 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. - To allow guest access, click **Enabled**. - To disable Guest Access, click **Disabled**.

3.2.3 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 connect 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.) - Select **Disabled** to disable Guest Access - If you connected this access point to two separate networks for a ‘physically secure’ solution, then choose **Ethernet Port 2** from the drop-down menu to set up your Guest network on the second Ethernet port. - If the access point is using only one physical connection to your internal LAN(extra port is not in use), and then choose **VLAN on 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.

(Continued)

Item	Description
Guest Access	 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.

3.3 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	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.) - Select Disabled to disable the VLAN for the Internal network, and for any additional virtual networks on this access point. When user disable the VWN it is possible that VWN can be added in **manage > VWN** menu. In that case, SMT-R2000 doesn't use VLAN but add VWN into internal network.

3.4 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	MAC address of internal interface for AP Ethernet port. Only reading is available and this item cannot change.
VLAN ID	If you choose to configure Internal and Guest networks by 'VLANs', this field will be enabled. Provide a number between 1 and 4094 for the Internal VLAN. 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.
Connection Type	You can select 'DHCP' or 'Static IP'. *Dynamic Host Configuration Protocol*(DHCP) 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. 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 name server. If you select 'DHCP', the Samsung AP will acquire its IP Address, subnet mask, and DNS and gateway information from the DHCP Servers. Otherwise, if you select 'Static IP', fill in the items described in 'Static IP Settings.' **CAUTION** 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. 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.
Static IP Address	If you chose 'Static IP' as the Connection Type, these fields will be enabled. Enter the target static IP address into the text box.
Subnet Mask	Enter the **Subnet Mask** in the text boxes. You must obtain this information from your ISP or network administrator.

(Continued)

Item	Description
Default Gateway	Enter the **Default Gateway** in the text boxes.
DNS Name Server	*Domain Name Service*(DNS) converts Domain name (ex. www.SamsungElectronics.com) of network resource into IP address(e.g., 66.93.138.219). DNS server is called *Name server*. There are usually two Name servers; a Primary Name server and a Primary Name server. You can choose **Dynamic** or **Manual** mode. - 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.

3.5 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	If you choose to configure Internal and Guest networks by 'VLANs', this field will be enabled. Provide a number between 1 and 4094 for the Guest VLAN.

3.6 Update Settings

To update Ethernet settings:

1) Move to **Manage** > **Ethernet Settings**.
2) Configure the ethernet settings as required.
3) Click the **Update** button to apply the changes.

This page is intentionally left blank.

CHAPTER 4. 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).

4.1 802.11h Regulatory Domain Control

Item	Description
802.11h Regulatory Domain Control	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. 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). - 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.  NOTE 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 SMT-R2000, 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.

4.2 Setting the Wireless

The radio interface allows you to set the radio Channel and 802.11 modes 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	Indicates the Media Access Control(MAC) addresses for the interface. 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.
Mode	The *Mode* defines the *Physical Layer*(PHY) standard being used by the radio → 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. **Single-Band AP:** For the Single-Band AP, select one of these modes: - IEEE 802.11b - IEEE 802.11g **Dual-Band AP:** For the dual band AP, select one of these modes: a mode for each Radio Interface. - IEEE 802.11b - IEEE 802.11g - IEEE 802.11a
Channel	Select the **Channel**. The range of channels and the default is determined by the **Mode of** the radio interface. 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). When setting to 'Auto', AP automatically selects the idlest channel. When DFS is supported in IEEE802.11a(when the 'supports IEEE802.11h' message is displayed), the channel is always set to AUTO.

4.3 '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	Shows the MAC address(es) for Internal interface for this access point. This is a read-only field that you cannot change. 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 *Basic Service Set Identifiers(*BSSIDs) for a single access point. The MAC address(es) shown for the 'Internal' access point is the BSSID(s) for the 'Internal' interface. For the two-radio AP, two MAC addresses are shown: one for each Radio on the Internal interface.
SSID	Enter the **SSID** for the internal WLAN. The *Service Set Identifier*(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 *Network Name*. There are no restrictions on the characters that may be used in an SSID.

4.4 '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	Shows the MAC address for the Guest interface for this access point. This is a read-only field that you cannot change. 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 *Basic Service Set Identifiers(*BSSID) for a single access point. The MAC address(es) shown for the 'Guest' access point is the BSSID(s) for the 'Guest' interface. For the two-radio AP, two MAC addresses are shown: one for each Radio on the Guest interface.
SSID	Enter the **SSID** for the *guest network*. The *Service Set Identifier*(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 *Network Name*. 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.

4.5 Update setting

To update wireless settings:

1) Move to **Manage > Wireless Settings**
2) Configure the wireless settings as required.
3) Click the **Update** button to apply the changes.

CHAPTER 5. Security settings

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.

5.1 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 hoses of AP.

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.)

5.2 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.)

Items	Description
Broadcast SSID	In order to activate the item of **Broadcast SSID**, select the checkbox. IN the default setup, AP contains the *Service Set Identifier*(SSID) into Beacon frame to transmit it. 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.
Station Isolation	Select the checkbox if activating the Station Isolation item. - If the Station Isolation item is **uncheck**, the radio client can communicate with other clients via AP. - 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.
Security Mode	Select one of the following **security modes**. - None(Plain-text) - Static WEP - IEEE 802.1x - WPA Enterprise - WPA Personal To Guest network, only the 'None(Plain-text)' security mode can be set.(For this information, refer to Guest Access Setup.) Other security modes besides the Plain-text mode are applied only to the 'Internal' network.

5.2.1 None (Plain-text)

*None(*Or Plain-text) mode means that the client does not encrypt the data when it communicate with SMT-R2000.

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

Guest Network

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

This feature makes 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.

5.2.2 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 in 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 WEP key by selecting one of the followings: - 64 bit - 128 bit
Key types	Designate the type of WEP key by selecting one of the followings: - 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. The client should set the same WEP key in the same index as designated in AP.(Refer to Static WEP Key Setup Rules.) **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.

(Continued)

Item	Description
Authentication	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. Designate the authentication algorithm to be used by selecting one of followings: - Open System - shared Key NOTE: You can select either of Open System checkbox or the public key checkbox. 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. Note that just because a client station is allowed to *associate* 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. **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. Open System and Shared key. The cases of selecting both of two algorithms are as follows: - 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

- 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 AP in order to descramble the data transmitted from AP into the client.
- 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 descramble 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, ASCHI type, and only the figure should be entered in the key value.

5.2.3 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(PEAPO and MSCHAP V2).

If using the external RADIUS server, you should have the options for the various authentication modes, such as the certicate, 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. *Radius IP* 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 ‘*’ character so that other cannot see it. This value is not transmitted into the network.

5.2.4 WPA Personal

Wi-Fi Protected Access Personal is Wi-Fi Alliance IEEE 802.11i standard that includes a *Counter mode/CBC-MAC 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 certicate.

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. - WPA - WPA2 - Both **WPA.** Select WPA if all clients in the network support the early WPA and if there is no client supporting a new WPA2. **WPA2.** Select WPA2 that supports the security in the level of IEEE 802.11i standard if all clients in the network support WPA2. **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.
Cipher Suites	Select the cipher suite you want to use: - TKIP - CCMP(AES) - Both **Temporal Key Integrity Protocol(**TKIP) is a default value. TKIP is an encryption method safer than the WEP key encryption. TKIP 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. **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(CBC-CTR) mode and Cipher Block Chaining Message Authentication Code(CBC-MAC) for the encryption and the integrity checkup. If either of TKIP or CCMP(AES) is selected, Pair wise cipher is AES, and GroupWise cipher is TKIP. Pair wise 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:

(Continued)

Item	Description
Cipher Suites	- A valid TKIP key - A valid CCMP(AES) key The client not set as WPA Personal cannot access AP.
Key	The key value corresponding to *Pre-shared Key*, which is a public key for the WPA Personal mode. Minimum 8 characters up to 63 characters can be entered.

5.2.5 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 times should be selected:

Item	Description
WPA Version	Select the security mode of the client that the AP will support. - WPA - WPA2 - Both **WPA.** Select WPA if all clients in the network support the early WPA and there is no client supporting the WPA2. **WPA2.** Select WPA2 that supports the security in the level of IEEE802.11i standard if all clients in the network support WPA2. **Both.** Select 'Both'' if the client supporting WPA2 and the one supporting only WPA are mixed. If this option is selected, all of WPA client and the WPA2 client can access the network and be authenticated.
Cipher Suites	Select the encryption algorithm that you will use. - TKIP - CCMP(AES) - Both **Temporal Key Integrity Protocol**(TKIP) is a default value. 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.

(Continued)

Item	Description
Cipher Suites	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. **Counter mode/CBC-MAC Protocol**(CCMP) is an encryption method for IEEE 802.11i that uses the **Advanced Encryption Standard**(AES). CCMP uses CCM combined with Cipher Block Chaining Counter(CBC-CTR) mode and Cipher Block Chaining Message Authentication Code(CBC-MAC) for the encryption and the checkup of the message integrity. If all of TKIP 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: - A valid TKIP RADIUS IP address and valid shared Key - A valid CCMP(AES) IP address and valid shared Key The client that is not set in WPA Enterprise mode cannot access AP. 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 should have one of the followings: - A valid TKIP RADIUS IP address and RADIUS Key - A valid CCMP(AES) IP address and RADIUS Key
Radius IP	Enter the Radius IP in the text box. *Radius IP* is the IP Address of RADIUS.
Radius Key	Enter the Radius Key in the text box. *Radius Key* 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. This value is not absolutely transmitted into the network.

5.3 Update settings

The security setup can be updated as follows:

1) Move to the **security** menu.
2) Set a desired security item.
3) Click the **update** button to apply the changes.

CHAPTER 6. Virtual Wireless Network Settings

6.1 VLAN Setting


NOTE

- 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	You can enable or disable a configured network. To enable the specified network, check the **Enabled** checkbox beside the appropriate VWN. To disable the specified network, uncheck the **Enabled** checkbox beside the appropriate VWN. If you disable the specified network, you will lose the VLAN ID you entered.
VLAN ID	Provide a number between 1 and 4094 for the Internal VLAN. 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. Check with the Administrator regarding the VLAN and DHCP configurations.

(Continued)

Item	Description
SSID	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. The *Service Set Identifier*(SSID) is an alphanumeric string of up to 32 characters. 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.
Broadcast SSID	Select the **Broadcast SSID** setting by selecting the **Broadcast SSID** checkbox. By default, the access point broadcasts the *Service Set Identifier*(SSID) in its beacon frames. You can 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 exact network name configured in the supplicant before it will be able to connect. 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: - 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	Select the **Security Mode** for this VLAN. Select one of the following: - None(Plain-text) - Static WEP - IEEE 802.1x - WPA Enterprise - WPA Personal NOTE: The Security mode you set here is specifically for this Virtual Network. Other networks continue to use the security modes already configured: - 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'.

6.2 Update settings

To update VLAN settings:

1) Move to **Manage > VWN**.
2) Configure the VLAN settings as required.
3) **Click the Update button to apply the changes.**

This page is intentionally left blank.

CHAPTER 7. 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).
Mode	A *mode* defines a standard of *Physical Layer*(PHY) used for wireless settings. SMT-R2000 can be operated as a single-band AP or dual-band AP. **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. - IEEE802.11a - IEEE802.11b - IEEE 802.11g NOTE: For SMT-R2000, the IEEE802.11a mode can be set up only in Radio 1, and the IEEE802.11b or IEEE80211g mode can be set up only in Radio 2.

(Continued)

Item	Description
Mode	**Dual-Band AP:** For Dual-Band AP, use the following combination: - IEEE 802.11a/IEEE 802.11b - IEEE 802.11a/IEEE 802.11g - IEEE 802.11a/IEEE 802.11b/IEEE 802.11g NOTE: For two-radio AP, each radio can be set up as a different mode by selecting a radio from the Radio item.
External Antenna	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**.
Channel	A channel means a part of a radio spectrum used by a radio for data transmission and reception. The range of a channel and basic channel are determined by the radio interface mode. 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.
Beacon Interval	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). The unit of *beacon interval* is 'ms', and a value can be entered between 20 and 2000.
DTIM Period	*Delivery Traffic Information Map*(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. The DTIM period indicates how often to transfer DTIM messages after loading to beacon messages. Designate a value between 1 and 255. 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.
Maximum Stations	Designate the maximum number of clients to allow accessing to AP.(0~2007)

(Continued)

Item	Description
Transmit Power	Enter the transfer power of AP in the unit of %. The default value is 100%. **Recommendations:** - 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. - 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.
Rate Sets	Set up the basic rate that the Supported rate Set of an AP and an AP broadcast to a network AP. - 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	It is available to improve the performance of all networks by limiting the number of packets transferred through a network. 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. - Click the **Enabled** button to activate the Multicast and Broadcast Rate Limiting option. - Click the **Disabled** button to activate the Multicast and Broadcast Rate Limiting option. 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'.

7.1 FCC CONCERNS

7.1.1 FCC Compliance Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.
This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

1) This device requires the user or installer to properly enter the current Reorient or relocate the receiving antenna.
2) Increase the separation between the equipment and receiver.
3) Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
4) Consult the dealer or an experienced radio/TV technician for help.

7.1.2 FCC Compliance Statement

The antenna(s) used for this device must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter.

RF Exposure Statement:

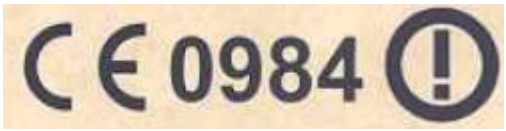
This device is restricted to indoor use only within the 5.15-5.25 GHz band to reduce any potential for harmful interference to co-channel MSS operations

Do Not	Any changes or modifications to the equipment not expressly approved by the party responsible for compliance could void user's authority to operate the equipment.

The wired LAN hub providing power over the Ethernet (PoE) in accordance with IEEE 802-3af shall be a UL Listed device with the output evaluated as a Limited Power Source as defined in UL60950-1.

Unit is intended for installation in a Network Environment 0 as defined in IEC TR 62102. As such, associated Ethernet wiring shall be limited to inside the building."

7.2 Notice for European Community



This device complies with the EMC directive 89/336/EEC, Low Voltage Directive 73/23/EEC and R&TTE Directive 1999/5/EC.
Compliance with these directives implies conformity to harmonized European standards(European Norms) that are listed on the EU Declaration of Conformity that has been issued by SAMSUNG for this device.

7.2.1 Countries of Operation & Conditions of Use

This device may be used in the following EU and EFTA countries: Austria, Belgium, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Slovak Republic, Slovenia, Spain, Sweden, Switzerland and the United Kingdom.

Requirements for indoor vs. outdoor operation, licensing and allowed channels of operation apply in some countries as described below:

The user must use the configuration utility provided with this device to ensure. The channels of operation are in conformance with the spectrum usage rules For EU and EFTA countries as described below.

7.2.2 GHz Operations:

1) This device may be operated indoors or outdoors in all EU and EFTA countries using the 2.4 GHz band(Channels 1-13), except where noted below.
2) In Italy, a license is required for outdoor use. Verify with your dealer or directly with the General Direction for Frequency Planning and Management(Direzione Generale Pianificazione e Gestione Frequenze).
   E'necessaria una concessione ministeriale anche per l'uso del prodotto. Verifici per favore con il proprio distributore o direttamente presso la Direzione Generale Pianificazione e Gestione Frequenze.
3) In France, this device may use the entire 2400-2483.5 MHz band(Channels 1 through 13) for indoor applications. For outdoor use, only the 2454-2483.5 MHz frequency band(Channels 10 through 13) may be used. For the latest requirements, see http://www.art-telecom.fr.

L'utilisation de cet equipement(2.4 GHz wireless LAN) est soumise a certaines restrictions: cet equipement peut etre utilise a l'interieur d'un batiment en utilisant toutes les frequences de 2400 a 2483.5 MHz(Chaine 1-13). Pour une utilisation en evironnement exterieur, vous devez utiliser les frequencies comprises entre 2454 a 2483.5 MHz(Chaine 10-13). Pour les dernieres restrictions, voir http://www.art-telecom.fr.

7.2.3 GHz Operation:

1) This device requires the user or installer to properly enter the current country of operation in the 5 GHz Radio Configuration Window as described in the Management and configuration Guide, before operating this device.
2) This device will automatically limit the allowable channels determined by the current country of operation. Incorrectly entering the country of operation may result in illegal operation and may cause harmful interference to other systems. The user is obligated to ensure the device is operating according to the channel limitations, indoor/outdoor restrictions and license requirements for each European Community country as described in this document.
3) This device employs a radar detection feature required for European Community and EFTA country operation in the 5 GHz band. This feature is automatically enabled when the country of operation is correctly configured for any European Community or EFTA country. The presence of nearby radar operation may result in temporary interruption of operation of this device. The radar detection feature will automatically restart operation on a channel free of radar.
4) This device is restricted to indoor use when operated in EU and EFTA countries using the 5.15-5.35 GHz band(Channels 36, 40, 44, 48, 52, 56, 60, and 64). See the table below for the allowed 5 GHz channels in each band.

7.2.4 Operation Using 5 GHz Channels in the European Community

The user/installer must use the provided configuration utility to check the current channel of operation and make necessary configuration changes to ensure operation occurs in conformance with European National spectrum usage laws and described below and elsewhere in this document.

Frequency Band(MHz)	Allowed Channels	Usage	Maximum EIRP(mW)
5150-5250	36, 40, 44, 48	Indoor use only	200
5250-5350	52, 56, 60, 64	Indoor use only	200
5470-5725	100, 104, 108, 112,116, 120, 124, 128, 132, 136, 140	Indoor or outdoor use	1000

7.2.5 Transmit Power Control (TPC) for 5 GHz operation

This device employs Transmit Power Control(TPC) to reduce the potential for interference to other communication systems operating in the 5 GHz frequency bands. The TPC feature implemented in this Wireless LAN device must be configured by the end-user when operating in any European Community or EFTA country. The end-user must follow the procedures explained in the Management and Configuration Guide in order to operate this device in accordance with European regulatory requirements for Transmit Power control.

The TPC procedure should be repeated when relocating this wireless device within the current wireless network or to a wireless network in a new location.

7.3 Updating Settings

Update the wireless settings as follows:

1) Move to **Manage** > **Radio**.
2) Set up the wireless settings item required.
3) Click the **Update** button to apply the modification.

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.

This page is intentionally left blank.

CHAPTER 8. MAC Address Filtering settings

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.

8.1 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	Click a button from the following buttons to set up the MAC address **filter**. - Accesses only permitted for terminals on the list - All terminals on the list blocked - Mac filtering not used
Stations List	Enter a 48-bit MAC address and click the **Add** button to add the MAC address to the terminal list. Then the MAC address will be added to the terminal list. Select the 48-bit MAC address and click the **Delete** button to remove the MAC address from the terminal list. A user can also allow or block a client in the list to access to an AP through filter settings.

8.2 Settings Update

Update the MAC filtering settings as follows:

1) Move to the **MAC filtering** page.
2) Set up the MAC filtering item as desired.
3) Click the **Update** button to apply the modifications.

CHAPTER 9. Load Balancing settings

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.

9.1 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. If this item is set up as '0', the AP allows all accesses regardless of the utilization rate.

(Continued)

Item	Description
Utilization for Disassociation	The utilization rate limit is related to wireless bandwidth utilization. Set up the bandwidth utilization rate limit(%) that indicates when disconnect the client access. If the utilization rate of an AP exceeds the limit, the AP disconnects the client access. If setting up this item as 0, all client accesses are not disconnected regardless of the utilization rate.
Stations Threshold for Disassociation	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 regardless of the value of 'Utilization for Disassociation'. Theoretically, the maximum number of simultaneously accessible clients is 2007. 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.

9.2 Update settings

Update the load balancing settings as follows:

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

CHAPTER 10. Port Forwarding settings

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.

10.1 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	The Port Forward list shows the list currently set up. Select an item to delete and click the Delete button to delete from the list. Select an item to add and click the Add button to add to the list. - Port Forwarding UDP list - Port Forwarding TCP list
Local IP address	Enter an internal 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.

10.2 Update Settings

Update the Port Forward settings as follows:

1) Move to **Manage > Port Fowarding**.
2) Set up the Port Forwarding item as desired.
3) Click the **Update** button to apply the modification.

CHAPTER 11. Port Control settings

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.

11.1 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 allows or blocks that a WAN IP or Local terminal accesses to a specific service port through port-control settings.

Item	Description
Protocol Port Filtering	The Protocol Port Filtering shows the list served by the current WAN IP settings. For the list, there are Telnet, HTTP, FTP, ICMP, and ping. - A user can allow or block WAN IP access by selecting Unblock or Block.
UDP/TCP Port Filtering List	The Port filtering list shows the current list settings. Select the desired item and click the Delete button to delete from the list. Select the desired item and click the Add button to add to the list. - 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.

11.2 Update Settings

Update the Port Forward settings as follows:

1) Move to the **Manage > Port Control** Control page.
2) Set up the Port Control item as desired.
3) \Click the **Update** button to apply the modification.

CHAPTER 12. Quality of Service (QoS) settings

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, vedio, and streaming media.

12.1 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.

- In case of Guest Interface, QoS Queue setup affects the whole AP load(Both of BSS).
- In case of Dual Band AP, these setups are applied to all 2.4 GHz and 5 Hz 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

12.1.1 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	Queue is defined according to the data types that are to be transmitted from AP into the clients. **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. **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. **Data 2(best effort)** This data needs the middle-level priority, performance, and delay time. Most IP data are transmitted into this queue. **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. For more information, refer to QoS Queues and Parameters to Coordinate Traffic Flow of IEEE 802.11e.
AIFS (Inter-Frame Space)	*Arbitration Inter-Frame Spacing*(AIFS) means the wait time(ms) for the *data frame*. AIFS is the value between 1 and 255. For more information, refer to DCF Control of Data Frames and Interframe Spaces of IEEE802.11.
cwMin (Minimum Contention Window)	This parameter is the input value of the algorithm that determines the early random backoff wait time('window') value. 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. The random figure that is firstly generated will be the one between 0 and the value defined at this item. 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 Maximum Contention Window item. 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'. For more information, refer to IEEE802.11 Random Backoff and Minimum / Maximum Contention Windows.

(Continued)

Item	Description
cwMax (Maximum Contention Window)	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. Once the random backoff value reaches the Maximum Contention Window value, the retry will be repeated until it reaches the maximum retry number. 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`'. For more information, refer to Random Backoff and Minimum / Maximum Contention Windows of IEEE 802.11.
Max. Burst Length	**AP EDCA Parameter Only**(Max. Burst Length option is applied only to the traffic that is transmitted from AP into the client.) 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. The valid Max. Burst Length values are the ones between 0.0 and 999.9.

12.1.2 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 trasmitted from the client into AP.

If WMM is set as 'non-used', the station EDCA parameter option will be released.

Even though WMM is set as 'non-used', you can stil set some of the AP EDCA parameter options.

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

12.1.3 Station EDCA Parameter Setup

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

Item	Description
Queue	Queue is defined according to the data types transmitted from the client into AP. **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. **Data 1(Video)** This data is the video data that needs the high priority and little delay time. The video data affected by time is transmitted into this queue. **Data 2(best effort)** This data needs the intermediate level priority, performance, and delay time. Most IP data are transmitted into this queue. **Data 3(Background)** This data needs the lowest priority and the high performance. The bulk data that need the maximum performance and that are little affected by time, such as FTP data, are transmitted into this queue. For more information, refer to QoS Queues and Parameters to Coordinate Traffic Flow of IEEE 802.11e.
AIFS (Inter-Frame Space)	*Arbitration Inter-Frame Spacing*(AIFS) means the wait time(ms) for the *data frame*. For more information, refer to DCF Control of Data Frames and Interframe spaces of IEEE802.11.
cwMin (Minimum Contention Window)	This parameter is the input value of the algorithm that determines the early random backoff wait time('window') value. The value designated at the *Minimum Contention Window* item is the maximum one of the early random backoff wait time that is to be determined by the algorithm. The random figure firstly generated will be the ones between 0 and the value defined at this item. 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 random backoff(window) doubles. This process will be repeated until the value reaches the value defined at the Maximum Contention Window item. For more information, refer to Random Backoff and Minimum / Maximum Contention Windows of IEEE 802.11.

(Continued)

Item	Description
cwMax (Maximum Contention Window)	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. 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. Once the Maximum Contention Window size is reached, retries will continue until a maximum number of retries allowed is reached. For more information, refer to Random Backoff and Minimum / Maximum Contention Windows of IEEE 802.11.
TXOP Limit	**Station EDCA Parameter Only**(TXOP Limit option is applied only to the traffic transmitted from the client into AP.) *Transmission Opportunity*(TXOP) means the time interval that the WME client becomes to have the right to transmit the data.

12.1.4 Retry Number Setup

AP has been set, as its default setup, to peprmit the retransmission number for the IP Data Packets into the determined value(Defalut: 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 Pakcet by Destination Ports can register up to 16 lists.

12.1.5 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.

12.2 Update settings

The QoS setup can be updated as follows:

1) Move to **Service** > **QoS**.
2) Set the necessary QoS items.
3) Click **'Update'** to apply the changes

CHAPTER 13. 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.

13.1 WDS settings

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


NOTE

- 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	The Samsung AP is available as a one-radio or two-radio access point. **One-Radio AP:** On the one-radio version of SMT-R2000, this field is not included on the WDS tab.

(Continued)

Item	Description
Radio	**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.
Local Address	Indicates the Media Access Control(MAC) addresses for this access point. 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 the access point or interface. **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. **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`).
Remote Address	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. 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. 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.
Bridge with	Network to be connected to WDS link. By default, internal network is used.

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

Encrytion Type	Description
None	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.
WEP	Specify whether you want *Wired Equivalent Privacy*(WEP) encryption enabled for the WDS link. *Wired Equivalent Privacy*(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 secret key + 24-bit IV) Shared Key for data encryption. For more information on WEP security, see Static WEP
WPA(PSK)	Specify whether you want *WPA(PSK)* encryption enabled for the WDS link. Wi-Fi Protected Access Pre-Shared Key, WPA(PSK) is a more secure form of encryption than WEP. When you use WPA(PSK) encryption, each AP on your network must be set with the same unique key, otherwise the APs will not be able to communicate with one another. Fore more information on WPA(PSK) security, see WPA Personal.

13.1.1 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.

13.1.2 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: - 64 bits - 128 bits
Key Type	If WEP is enabled, specify the WEP key type: - 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.

(Continued)

Item	Description
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 A-F). These are the RC4 encryption keys shared with the stations using the access point.

13.1.3 Setting WDS Link Security Mode to WPA(PSK)

If you select **WPA/PSK** 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	WPA(PSK)
SSID	Enter an appropriate name for the new WDS link you have created. This SSID should be different from the other SSIDs used by this AP. However, it is important that the same SSID is also entered at the other end of the WDS link. If this SSID is not the same for both APs on the WDS link, they will not be able to communicate and exchange data. The SSID can be any alphanumeric combination.
Key	Enter a unique shared key for the WDS bridge. This unique shared key must also be entered for the AP at the other end of the WDS link. If this key is not the same for both APs, they will not be able to communicate and exchange data.

13.2 Update Settings

To update WDS settings:

1) **Move to** Manage > WDS
2) **Configure the WDS settings as required.**
3) **Click the** Update **button to apply the changes.**

CHAPTER 14. Simple Network Management Protocol (SNMP) settings

14.1 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	You can select whether to use SNMP in a network. Default is SNMP is not used. - To enable SNMP, click **Enabled.** - To disable SNMP, click **Disabled.** You must click **Update** to save your settings. NOTE: If you do not enable SNMP, all remaining fields on the SNMP page will be disabled.
Read-only community name for permitted GETs	Enter a read-only community name. 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. The community name can be in any alphanumeric format.
Port number the SNMP agent will listen to	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. Enter the port number on which you want the SNMP agents to listen to requests.
Restrict the source of SNMP requests to only the designated hosts or subnets	You can restrict the source of permitted SNMP requests. - To restrict the source of permitted SNMP requests, click **Enabled**. - To permit any source submitting an SNMP request, click **Disabled**.

(Continued)

Item	Description
Hostname or subnet of Network Management System	Set DNS host name or subnet of a device that can perform GET/SET request. 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. To specify a subnet, enter one or more subnetwork address ranges in the form *AddressRange/MaskLength* where *AddressRange* is an IP address and *MaskLength* is the number of mask bits. Both formats NetAddress/NetMask and NetAddress/MaskLength 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`. 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). 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.

14.1.1 SNMP Traps Setting

SNMP taps 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 the **Enabled** checkbox beside the appropriate hostname.

14.2 Update Settings

To update SNMP settings:

1) Move to **Services > SNMP.**
2) Configure the SNMP settings as required.
3) **Click the Update button to apply the changes.**

This page is intentionally left blank.

CHAPTER 15. Network Time Protocol Server settings

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.

15.1 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: - 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.

15.2 Update Settings

To update time settings:

1) Move to **Service** > **NTP**.
2) Configure the time settings as required.
3) Click the **Update** button to apply the changes.

CHAPTER 16. View Interface Information

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.

16.1 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.

16.2 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.

This page is intentionally left blank.

CHAPTER 17. View Event Logs

A user can verify current events generated in SMT-R2000 on this page.(see Event).

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)

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.

17.1 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.

17.2 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/sysklogd` file.
   ```
   SYSLOGD='-r'
   ```
   Information on syslogd command option can be obtained using the man page.(Enter man `syslogd` 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/sysklogd restart
   ```


NOTE

The syslog 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.

17.3 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:

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

17.4 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.

17.5 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.

This page is intentionally left blank.

CHAPTER 18. View 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. 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. 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.
VLAN ID	Virtual LAN(VLAN) ID 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. VLANs can be used to establish internal and guest networks on the same access point.
Name(SSID)	Wireless network name. Also known as the SSID, this alphanumeric key uniquely identifies a wireless local area network. The SSID is set on the Basic Settings tab.(See Provide Administrator Password and Wireless Network Name.)
Transmit and Receive Information	
Total Packets	Indicates total packets sent(in Transmit table) or received(in Received table) by this access point.

(Continued)

Item	Description
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.

CHAPTER 19. View Accessed Client Terminal List

To view all client stations accessed to a specific AP, use **Status > Station Access** menu on the Administrator Web page of AP to be monitored.

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

19.1 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).

19.2 What is difference between Association 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 loam between APs and manage sessions.

For the information on *Sessions* Monitoring, refer to Understanding Session Monitoring Information.

This page is intentionally left blank.

CHAPTER 20. View Neighboring AP List

Through ‘Neighboring AP List’ you can confirm the real-time statistics of All APs within the range of AP showing on the administrator's Web page.

Item	Description
MAC Address	Shows the MAC address of a neighboring AP. MAC address is a Hardware address, which is a unique identifier depending on network nodes.
Radio	**Two-Radio APs** If an AP searching neighboring APs is Two-radio AP, the relevant AP can be confirmed in this page. Radio item informs the Radio searching neighboring APs. - wlan0(Radio One) - wlan1(Radio Two) **One-Radio APs** This item does not appear in the neighboring AP list of One-radio AP.
Beacon Interval	Shows Beacon interval used in the AP. AP transfers a Beacon frame at a regular interval to report the presence of radio Network. In default, the AP transfers a Beacon frame per 100 m/sec(or 10 frames per second). Users can set the Beacon interval in **Manage > Radio** item.(See Configuring Radio Settings.)
Type	Shows device types. - **AP** indicates a device that that supports IEEE 802.11 Wireless Networking Framework of Infrastructure Mode. - **Ad hoc** indicates a terminal that is operating in Ad hoc Mode. Terminals are set as the ad hoc mode for direct communication with other terminals without general AP. The Ad-hoc mode is IEEE 802.11 Wireless Networking Framework called *peer-to-peer* mode or *Independent Basic Service Set*(IBSS).

(Continued)

Item	Description
SSID	*Service Set Identifier* of AP. SSID is a unique identifier of radio LAN and a alphabetical string with at most 32 letters. SSID has the same meaning as *Network Name*. SSID can be set in the Basic Settings menu(see Configuring Basic Settings) or **Manage > Wireless Settings** menu(see Setting the Wireless Interface.) The Guest Network and the Internal Network operating at the same AP should have different two-SSID.
Privacy	Tells if peripheral devices use the security policy. - **Off** indicates that the security mode of the peripheral device is set as 'None'(no security). - **On** indicates that the peripheral device uses the security policy. Users can set the security policy of AP in the Security menu. For more information on security setting, refer to Configuring Security.
WPA	Tells whether AP sets the security mode as 'on' or 'off'.
Band	Tells IEEE 802.11 mode used in AP(for example, IEEE 802.11a, IEEE 802.11b, and IEEE 802.11g.) The values that can be checked by this item are as follows: - 2.4 indicates IEEE 802.11b or IEEE 802.11g mode. - 5 indicates IEEE 802.11a mode. - 5 Turbo indicates Atheros Turbo 5 GHz mode.
Channel	Shows the current channel of AP. Channel means a part of the Radio Spectrum that radio uses for data exchange. Channel can be set in the Radio Settings menu(see Configuring Radio Settings.)
Rate	Shows the current transfer rate(Mbps) for AP. The current rate is one of the transfer rate always listed in the Supported Rates entry.
Signal	Indicates the intensity(dB) of a signal emitted by AP.
# of Beacons	Shows the number of all Beacon frames transferred after the latest booting of AP.
Last Beacon	Shows the date and time of the Beacon frame that AP has most recently transferred.
Rates	Shows the supported rate set and basic(advertised) rate set that neighboring AP supports. Its unit is megabits per second(Mbps). All supported rates are listed and basic rates are displayed as bold. The transfer rate can be set in the Radio Settings menu(see Configuring Radio Settings.) The displayed transfer rate of AP is a transfer rate listed in the Radio Settings menu of the relevant AP.

CHAPTER 21. AP Configuration Management

21.1 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 returns to factory default settings. The factory default settings are listed in the table below.

Items	Default Value
Wired IP Address	192.168.111.10
Country Code	NN
802.11a(5 Ghz) SSID	SMT-R2000-WLAN0
802.11b/g(2.4 Ghz) 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

21.2 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'.

21.3 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.

21.4 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.

CHAPTER 22. Firmware Upgrade

As new versions of SMT-R2000 firmware become available, you can upgrade the firmware on your devices to take advantages 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 files of other formats for the upgrade; these will not work.

22.1 Update

1) Click **Update** to apply the new firmware image.
2) Upon clicking **Update** 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.

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

22.2 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.

SMT-R2000
Administration Guide

SAMSUNG ELECTRONICS