WEC8500/WEC8050 (APC)

Operation Manual

Disclaimer

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

Publication Information

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

Copyright 2015

Trademarks

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

INTRODUCTION

Purpose

This manual describes the overview, management, and setup of WEC8500/WEC8050 that is a Samsung Wireless Enterprise (W-EP) Access Point Controller (APC). This manual is written for WEC8500 version 2.4.19R and WEC8050 version 2.4.19R.

Document Content and Organization

This manual consists of ten Chapters, three Annexes, and a list of Abbreviations.

CHAPTER 1. Access Point Controller System Overview

This chapter describes the main functions, network configuration, external configuration and service scenario of APC.

CHAPTER 2. Basic System Configuration

This chapter describes how to configure to use Command Line Interface (CLI) and Web UI.

CHAPTER 3. Data Network Function

This chapter describes how to set up the data network such as interface, Virtual Local Area Network (VLAN), L3, or Quality of Service (QoS), etc. of APC.

CHAPTER 4. AP Connection Management

This chapter describes the connection management function of APC and Samsung W-EP wireless LAN Access Point (AP).

CHAPTER 5. WLAN Management

This chapter describes how to set up the Wireless Local Area Network (WLAN) of APC.

CHAPTER 6. Wi-Fi Configuration

This chapter describes how to configure the Wireless Fidelity (Wi-Fi) of APC, QoS, and country code.

CHAPTER 7. WLAN Additional Service

This chapter describes how to set up WLAN additional services available in the APC.

CHAPTER 8. Security

This chapter describes how to set up security related setting such as Remote Authentication Dial-In User Service (RADIUS) server available in the APC, unauthorized AP detection and blocking function, guest access, WEB pass-through, Network Address Translation (NAT), firewall function, etc.

CHAPTER 9. IP Application

This chapter describes the Internet Protocol (IP) application functions available in the APC such as Domain Naming Service (DNS), Network Time Protocol (NTP), File Transfer Protocol (FTP)/sFTP, or Telnet/SSH.

CHAPTER 10. System Management

This chapter describes the various system management functions available in the APC.

ANNEX A. CLI Command Structure

Command structure available in the CLI of APC.

ANNEX B. Open Source Announcement (WEC8500/WEC8050)

Open source list used in the APC and its license notice.

ANNEX C. Open Source Announcement (WEA302/WEA303/WEA312/ WEA313 (Future Release)/WEA403/WEA412)

Open source list used in the Samsung W-EP wireless LAN AP and its license notice.

ABBREVIATION

Describes the acronyms used in this manual.

Conventions

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

NOTE

NOTE

Indicates additional information as a reference.

Console Screen Output

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

Revision History

VERSION	DATE OF ISSUE	REMARKS
5.2	02.2015.	Updated for US Market to support software V2.4.19R
5.1	08.2014.	Updated for US Market
5.0	05. 2014.	- Updated the content overall in accordance with the package version 2.0.0
4.0	01. 2014.	- Changed contents • 1.3.1 WEC8500 Configuration and Functions • 4.2.6.3 Tech Support Information
3.0	10. 2013.	- Updated the content overall in accordance with the package version (WEC8500 version 1.4.4, WEC8050 version 1.0.0) - Added contents for WEC8050
2.0	06. 2013.	- Updated the content overall in accordance with the package version 1.3.0 - Added contents • 3.4.6 OS-AWARE • 7.4.2 DPC Configuration • 7.4.3 DCS Configuration • 7.4.4 CHDC Configuration - Changed contents • 7.10 Clustering • 10.8.2 System Upgrade
1.0	03. 2013.	First Version

TABLE OF CONTENTS

LIST OF FIGURES

CHAPTER 1. Access Point Controller System Overview

1.1 APC Overview

The Samsung Access Pointer Controller (APC) comprehensively manages the user information and traffics while managing an Access Point (AP), i.e. a device that provides wireless connection service for a user terminal in a Wi-Fi environment. There are two types depending on the AP capacity; WEC8500 and WEC8050. It comprehensively manages all the APs and provides services in a wireless LAN environment. Because AP and APC are connected in tunneling, all the user traffics are exchanged and processed.

The APC is typically installed at a position where it can be connected to a backbone switch, core switch or router in a network of enterprise environment and it controls a wireless LAN AP and provides the functions for Wireless LAN (WLAN) services such as handover and QoS, security/authentication, etc. The Samsung WEC8500 provides its services up to 500 APs. It can provide its services up to 10,000 connected user devices. Meanwhile, the WEC8050 can accommodate maximum 75 APs and provides the service to maximum 1500 user devices.

The APC provides a WLAN network environment through AP management and also provides various communication services required by enterprise customers in a wireless environment by interoperating with other enterprise solutions. It provides Wireless Enterprise (W-EP) solution in an enterprise environment by making the collaboration applications such as telephone, message, or communicator, etc., that has been used in a legacy wire environment, be able to be used in a wireless terminal such as smart phone, tablet PC, or notebook.

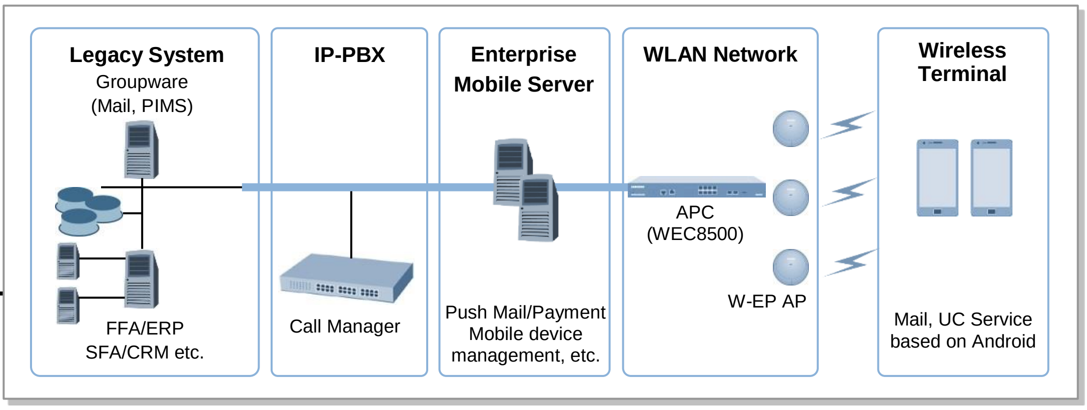


Figure 1. System Structure for Wireless Enterprise Solution

The Samsung W-EP solution, as shown in figure, comprehensively includes various enterprise applications which are provided by wire/wireless infrastructure products and wireless terminals. The WLAN network, a wireless infrastructure solution that provides mobility in an enterprise environment, consists of W-EP wireless LAN Access Point (AP), W-EP AP Controller (APC), and Wireless Enterprise WLAN Manager (WEM). (Future Release)

The Samsung APC and W-EP wireless LAN AP are core devices that provide various services such as user authentication, wireless management, voice and data service, etc. in the 802.11-based Wi-Fi environment. The WEM provides convenient configuration environment, various statistics, and event information to an operator. (Future Release)

NOTE

Term

In this manual, the WEC8500/WEC8050 and APC commonly represent Samsung AP Controller. In addition, the AP means Samsung W-EP wireless LAN AP.

1.2 Network Configuration

The network configuration of Samsung W-EP solution that includes APC is shown below.

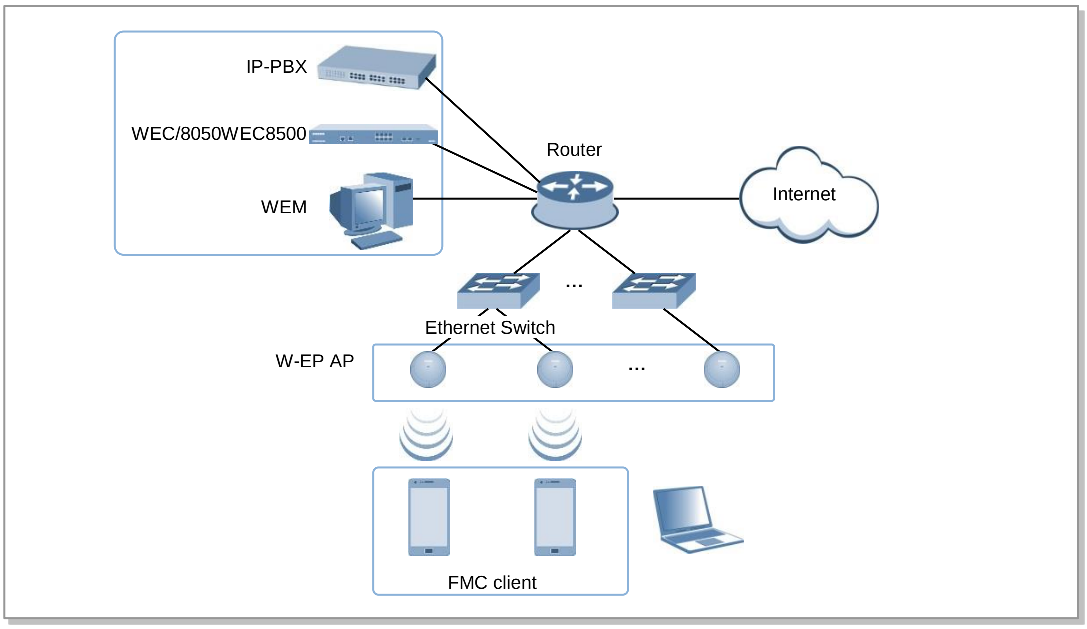


Figure 2. W-EP Network Configuration

IP-PBX

As an enterprise call manager, it is a switch required to provide the Fixed Mobile Convergence (FMC) function to a wireless terminal (optional).

APC (WEC8500/WEC8050)

The APC manages all the W-EP wireless LAN APs installed in an enterprise communication environment and it also manages user information and traffics.
Because the W-EP wireless LAN network configuration uses a centralized structure where all the wireless user traffics are in tunneling through the APC, the APC is one of the most important elements related to traffic management and throughput in the W-EP environment.
An APC is typically installed at a position where it can be connected to a backbone switch, core switch or router in a network. It controls the W-EP wireless LAN AP and provides handover, QoS, and security/authentication functions.

WEM (Future Release)

In the W-EP wireless LAN environment, various services are provided through a complex network configuration. As many users are involved, its management is complex and difficult. A normal network administrator can hardly handle any problematic issue as well as a normal management task. The WEM is a Network Management System (NMS) that efficiently manages this kind of W-EP wireless LAN network and service environment.
It manages a WLAN network, retrieves and configures the status of APC or W-EP wireless

LAN AP.

W-EP AP (W-EP Wireless LAN AP)

The W-EP wireless LAN AP is a device that provides wireless connection service to a user terminal. It should be installed by considering the service area or region that will be provided in an enterprise environment. Typically, the number of W-EP wireless LAN APs is determined by considering the size of installation area and the number of users to secure service coverage.

Ethernet Switch

Typically, because an AP is installed in a user area, use a Power over Ethernet (PoE) switch that does not use a power line for the beauties of environment, etc. Install the W-EP wireless LAN APs by considering current consumption and the power capacity PoE switch. In addition, because power drop may occur if the distance between the switch and W-EP wireless LAN AP, the relationship between distance and power must be considered. Typically, the distance between these two must be 100 m or less in order to avoid power drop.

Wireless terminal/WeVoIP Client

Terminal that provides the 802.11a/b/g/n interface such as smart phone, tablet PC, or notebook computer, etc. In an Android smart phone, an enterprise Voice over IP (VoIP) application equipped with the Samsung voice engine is called a WeVoIP client (The WeVoIP client is an option).

Wireless additional service

In the W-EP environment, various application services are required as well as basic wireless connection services.

The Wireless Enterprise Security (WES) provides a security service that is one of the most important elements in an enterprise environment. The WES can seamlessly receive wireless connection service through the security services such as unauthorized terminal, unauthorized AP, or ad hoc connection blocking, etc.

Location service that manages the location of a terminal in a wireless environment is also an application service required in an enterprise environment. With this, it is possible to manage the location of an effective user or an unauthorized user.

IP application service

The IP application servers required in an existing wire network including Dynamic Host Configuration Protocol (DHCP) server, DNS server, web server, or RADIUS authentication server are also used in the W-EP environment. Especially, the DHCP server and RADIUS authentication server play a critical role in the wireless environment.

1.3 APC Configuration and Functions

1.3.1 WEC8500 Configuration and Functions

The Configuration and the purpose of each item of WEC8500 are as follows:

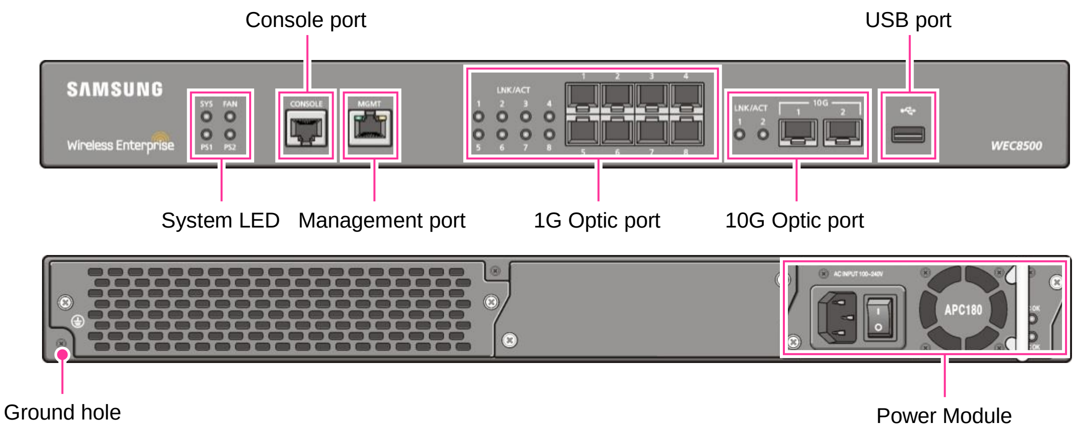


Figure 3. WEC8500 Interface-Front/Back

System LED

System LED indicates the various statuses of system. Each LED displays the following information.

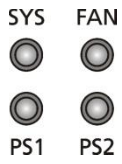


Figure 4. System LED Configuration

LED	Status	Description
SYS	Green	The system is operating normally
	Orange	The system is now booting
	Red	Preparing the system for booting
FAN (fan module)	Green	The installed FAN module is operating normally
	Orange	The system is now booting
	Red	Fan module fault has occurred
PS1 (power module 1)	Green	Normal operation of installed power module 1
	Red	Power is turned off or a fault occurred while the power module 1 is installed.
	Off	Power module 1 is not installed.
PS2 (power	Green	Normal operation of installed power module 2

LED	Status	Description
module 2)	Red	Power is turned off or a fault occurred while the power module 2 is installed.
	Off	Power module 2 is not installed.

Console port (RS232C)

A console port is used to check the operational status of WEC8500 or for input through the CLI. Its basic requirements are as follows:

- Baud rate: 115200 bps
- Character size: 8 characters
- Parity: None
- Stop bit: 1, Data bit: 8
- Flow control: None

Management port (1 GE UTP)

The WEC8500 provides a 10/100/1000BASE-T port (RJ-45) for management purpose. It is working in 10/100 Mbps half duplex/full duplex mode or in 1000 Mbps full duplex mode. Because it supports the automatic MDI/MDI-X function, you can use a straight-through cable for all the network connections to a PC, server, switch, or network hub.

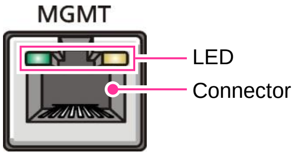


Figure 5. Management Port Configuration

Configuration item	Status	Description
LED	Green	Turned on for link connection
	Orange	Blinking for data exchange
Connector	-	Connector for UTP cable connection

When connecting a cable to the management port, make sure to check if the cable complies with the 10 BASE-T, 100 BASE-TX, or 1000 BASE-T.

- Cable type: UTP or STP cable using RJ-45 connector
  - 10 BASE-T: Category 3 or higher
  - 100 BASE-TX: Category 5 or higher
  - 1000 BASE-T: Category 5 or higher (Category 5e or higher is recommended)
- Isolate from wireless frequency disturbing waves
- Shut down electrical surge

- Separate the electrical wiring of a switch or related devices and the electromagnetic area of network data line
- Cable or connector and safe connection without damaged cable sheath

NOTE

The 1000 BASE-T standard does not support the forced mode.
The auto-negotiation function must be always used for 1000 BASE-T port or trunk connection.

Optic port

It provides two 10 GbE Optic ports and eight 1 GbE Optic ports and the operational status of each port is displayed in LED.

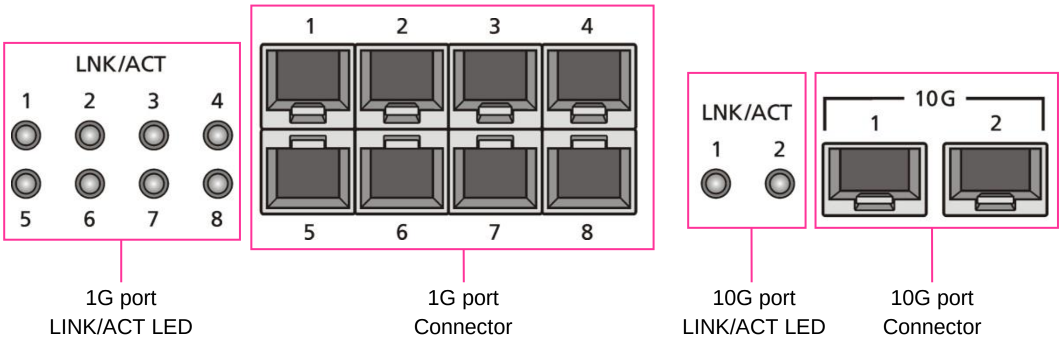


Figure 6. Optic port configuration

Configuration item	Port/LED	Description
10 GE ports	LINK/ACT 1, LINK/ACT 2	LINK/ACT status of each port - Turned on for link connection - Blinking for data exchange
	10G 1, 10G 2	10 GbE Optic module connector
1 GE port	LINK/ACT 1~LINK/ACT 8	LINK/ACT status of each port - Turned on for link connection - Blinking for data exchange
	1G 1~1G 8	1 GbE Optic module connector

USB port (Host 2.0)

The WEC8500 provides a USB host port that supports the upgrade of WEC8500 operation software.
A typical USB memory stick is supported.

Power module

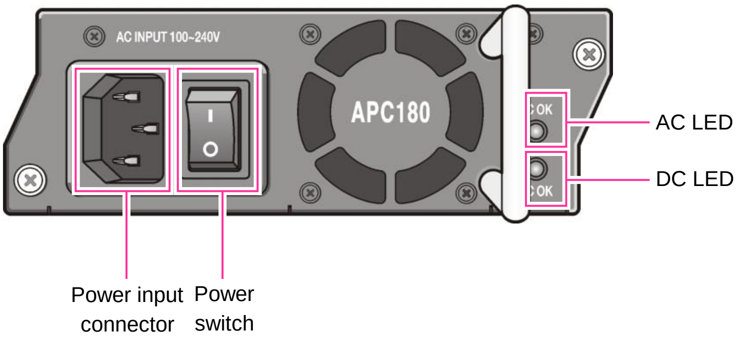


Figure 7. Power module configuration

Configuration item	Description
Power input connector	Connector to connect the power cable to
Power switch	Switch to turn on/off power
AC LED	Turned on when there is a normal AC power input.
DC LED	Turned on when there is a normal DC power output.

1.3.2 WEC8050 Configuration and Functions

The configuration and the purpose of each item of WEC8050 are as follows:

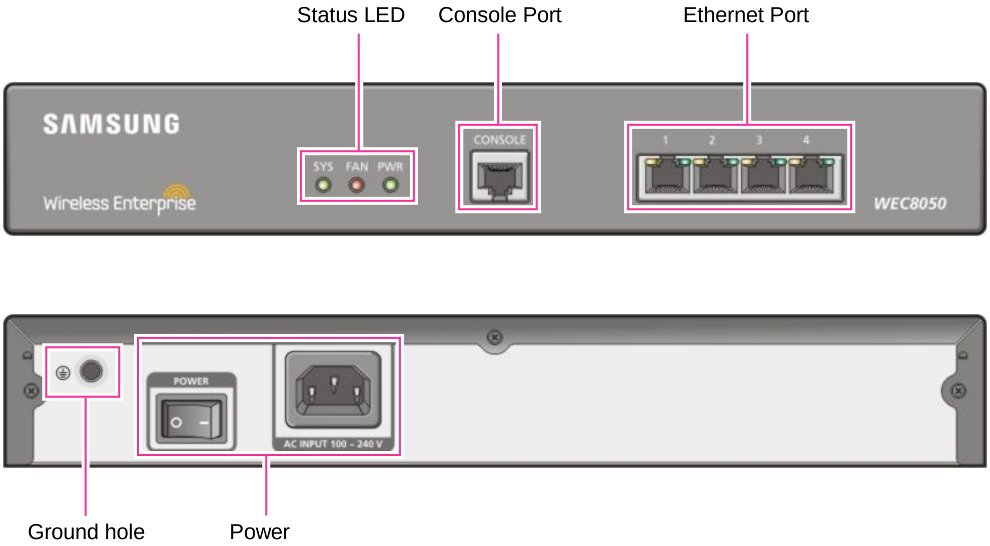


Figure 8. WEC8050 interface-Front/Back

Status LED

This LED indicates the various statuses of system. Each LED displays the following information.

Figure 9. Status LED configuration

LED	Status	Description
SYS	Green	The system is operating normally
	Orange	The system is now booting
	Red	Preparing the system for booting
FAN	Green	The installed FAN module is operating normally
	Orange	The system is now booting
	Red	Fan fault
PWR	Green	The power is supplied normally
	Off	The power is turned off or not supplied

Console port (RS232C)

A console port is provided to check the operational status of WEC8050 or for input through the CLI.
Its basic requirements are as follows:

- Default baud rate: 115200 bps
- Character size: 8 Characters
- Parity: None
- Stop bit: 1, Data bit: 8
- Flow control: None

Ethernet port

It has 4 10/100/1000 Base-T ports.

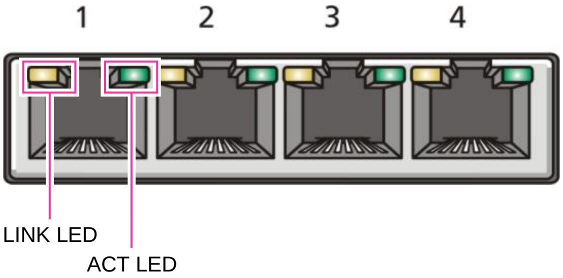


Figure 10. Ethernet Port Configurations

LED	Status	Description
ACT	Orange blinking	Blinking while data exchanging
	Off	No data exchanging
LINK	Green	Link connection display
	Off	No link connection

1.4 APC Application Configuration and Service Scenario

1.4.1 Basic Configuration

To provide wireless connection service using a wireless LAN in the W-EP environment, the W-EP wireless LAN AP that helps a terminal connect to the network through wireless and an APC that controls the terminal are basically required. Especially, the role of APC is critical to guarantee QoS of various services and provide high level of security functions in an Enterprise communication environment. As various elements are required in the W-EP environment, it is necessary to intuitively or organically manage each element via WEM. (Future Release)

In addition, the IP application servers including authentication server, DHCP server, or DNS server which is a basic network configuration element in a wire enterprise environment are also interoperated to provide more convenient and various mobile services to users. One outstanding example is the WeVoIP service that provides enterprise level VoIP in a wireless LAN. With this, the wire/wireless integrated voice service can be provided.

An example of service configuration diagram using the W-EP wireless LAN system is shown in the below figure. The configuration diagram is based on Samsung APC (WEC8500).

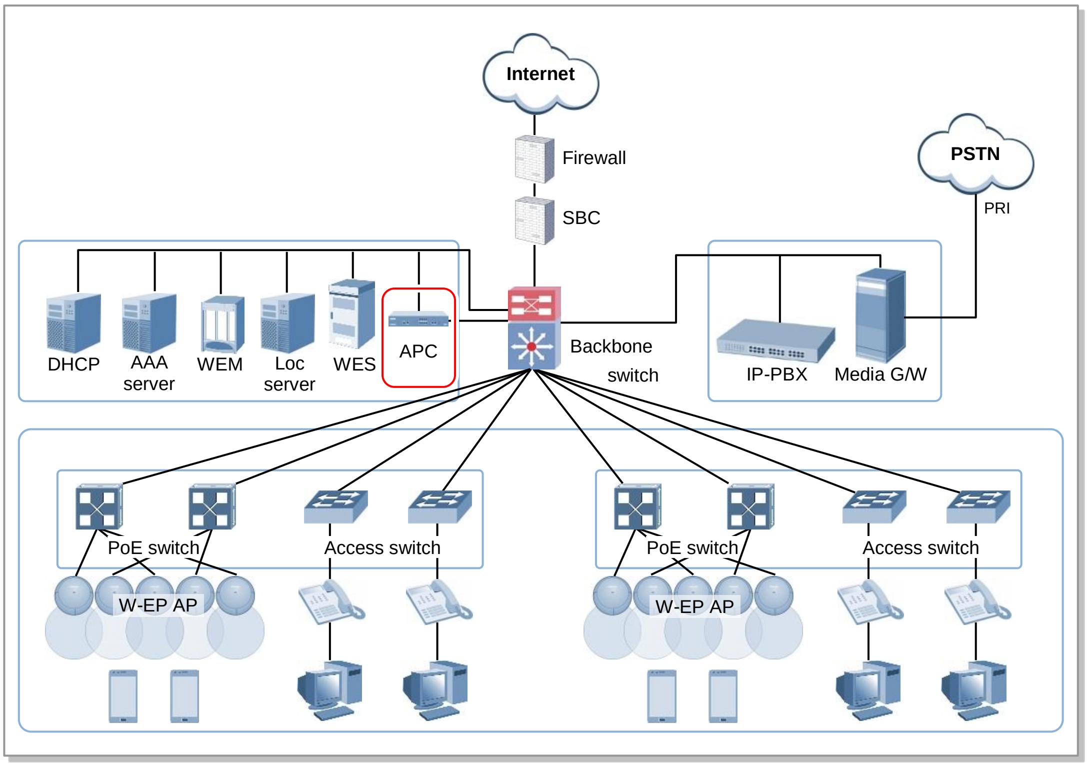


Figure 11. Basic Configuration of W-EP Wireless LAN System

The basic W-EP wireless LAN network configuration is a centralized structure where all the wireless user traffics go through tunneling between APC and W-EP wireless LAN AP. Therefore, the network information such as subnet information allocated to a wireless user depends on the configuration of backbone network where the APC is connected.

This provides the following advantages during network configuration and setup.

- Installing the APC is just adding it to a legacy data center or backbone network. Therefore, the possibility of physical change of core network can be reduced. In addition, separate design of wire/wireless network is easy using the APC as a boundary.
- No dramatic network change is required to install the W-EP wireless LAN AP. An AP installed in a user area is located in various local network environments in a wide region. Although it is unavoidable to install or expand a PoE switch, the modification of local network where wire users are already configured can be minimized.
- Because the APC relays all the user traffics, it can restrict a wireless attacker’s effects and provide differentiated service for each user.

1.4.2 Configuration of Multiple APC for Redundancy

The APC provides the redundancy function to guarantee QoS for various services and provide service stability in the W-EP environment.
An example of service configuration diagram for redundancy is shown in the below figure.

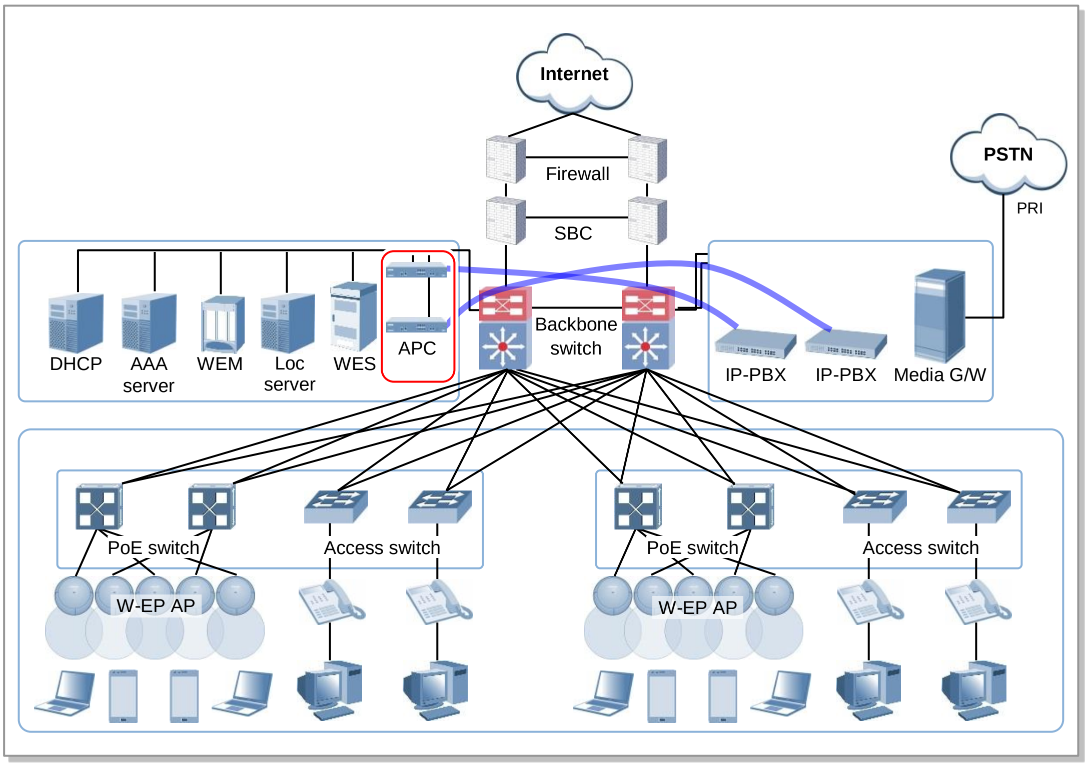


Figure 12. Example of W-EP Wireless LAN System Configuration for Redundancy

In this configuration, several APC s are used to minimize service disruption caused by a disconnected APC and to enhance service sustainability. Basically, two or more APC s must be installed in the same site for APC redundancy. The redundancy configuration includes active-active configuration, active-standby configuration, and many-to-one configuration. An operator can select a configuration based on the number of available APC s and redundancy level.

1.4.3 Clustering Configuration using Multiple APC (WEC8500)

The W-EP environment has various area sizes, user density and number of users. If only a single APC is required for service and management, the complexity of network configuration or management is not high. However, if the capacity of a single APC is not sufficient, multiple APC s must be installed for service. The WEC8500 is a Samsung APC model providing the clustering environment.

To set up a wireless LAN network in an environment where multiple WEC8500s are installed, the integrated management system and user service must be provided through clustering configuration between the WEC8500s. This allows inter APC handover.

The WEC8500s configured in a cluster provides a service just like a single WEC8500 through periodic information exchange.

NOTE

Inter APC handover

The inter APC handover is a handover between APCs. A clustering group is used to provide this function and this clustering group means a virtual area.

Maximum six WEC8500s can be bound to a single group. An APC in a group cannot be added to another group.

It provides layer 3 handover and the handover is supported when a terminal moves to an APC which have different subnets. A serving APC is called as an anchor APC and a target APC is called as a foreign APC. The control path and also the tunnel for data traffic between APCs provide security using IPSec.

The inter APC handover provides this function both in the standard Wi-Fi handover and Samsung’s unique AirMove method.

1.4.3.1 Configuration of Distributed Clustering Service

The configuration of distributed clustering is to install each WEC8500 in a building or a local site according to its capacity. This option can be used when there is no integrated backbone configuration in a site or networks are separated for each building. It is suitable for a site where several buildings are apart from each other.

An example of service configuration diagram is shown in the below figure.

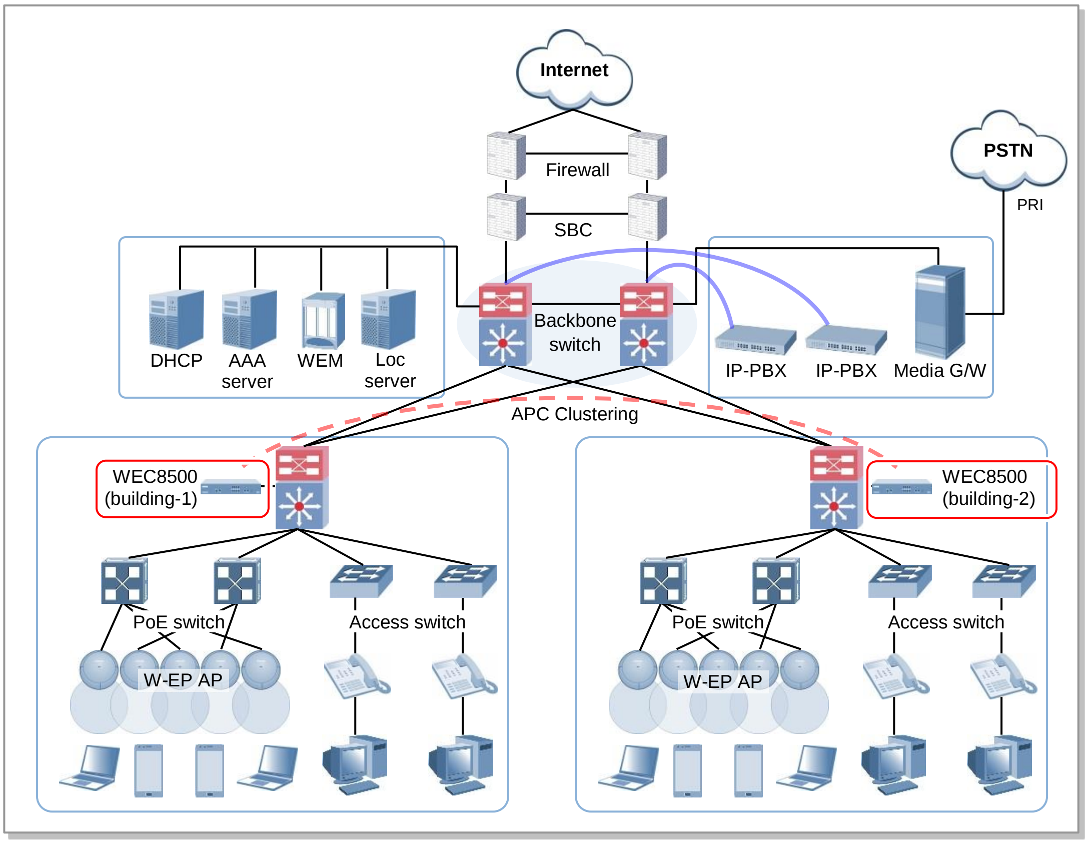


Figure 13. Example of W-EP Wireless LAN System Configuration for Distributed Clustering Service

1.4.3.2 Configuration of Centralized Clustering Service

In the centralized cluster configuration, all the WEC8500s in a site are installed in the center. This is suitable when all the networks in a site are configured around the backbone. This option is suitable for a site where several buildings are close to each other or a large building where a seamless handover service is required using one or more WEC8500s. Better performance can be obtained if there is a single backbone network and it is preferable in terms of installation or maintenance because its service configuration is simple.

An example of service configuration diagram is shown in the below figure.

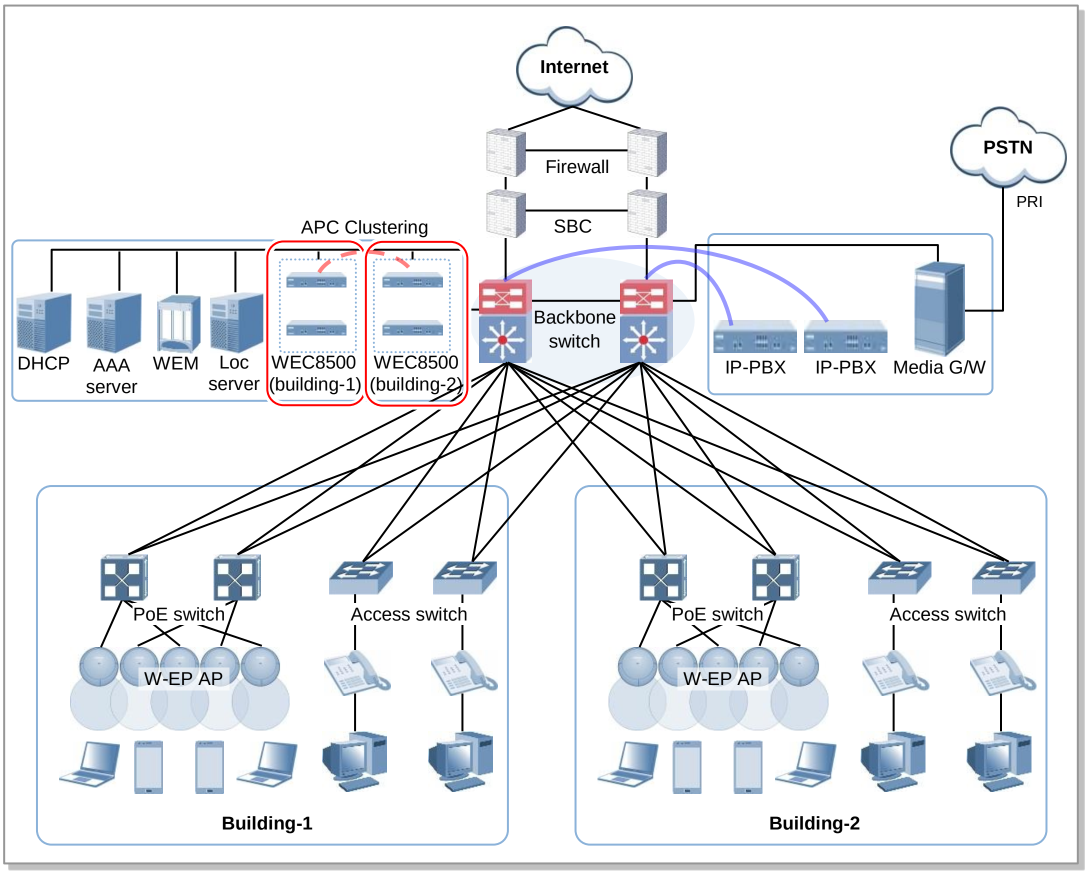


Figure 14. Example of W-EP Wireless LAN System Configuration for Centralized Clustering Service

1.4.4 Configuration of Multiple Sites Consisting of Headquarter and Branches

The W-EP wireless LAN network environment usually consists of one headquarter and several branches.
In this case, there are two types of network configuration.

- Hierarchical type: A APC is installed in a branch as well as headquarter.
- Branch AP type: A APC is installed only in a headquarter and only a W-EP wireless LAN AP is installed in a branch.

In the hierarchical type, it is advantageous that each branch can use each different service policy. However, the management in headquarter is complex and many low-capacity APCs must be installed, so the branch AP type is commonly used.
The branch AP type has the same structure as a basic W-EP wireless LAN configuration. A single difference is that a W-EP wireless LAN AP installed in a branch is located at a remote place. The APC in headquarter provides a wireless LAN service in the headquarter building and also provides a wireless LAN service to a remote W-EP wireless LAN AP installed in a branch. As the APC in headquarter manages all the W-EP wireless LAN APs using the same policy, it is easy to use and cost-effective.

An example of service configuration diagram for the branch AP type is shown in the below figure.

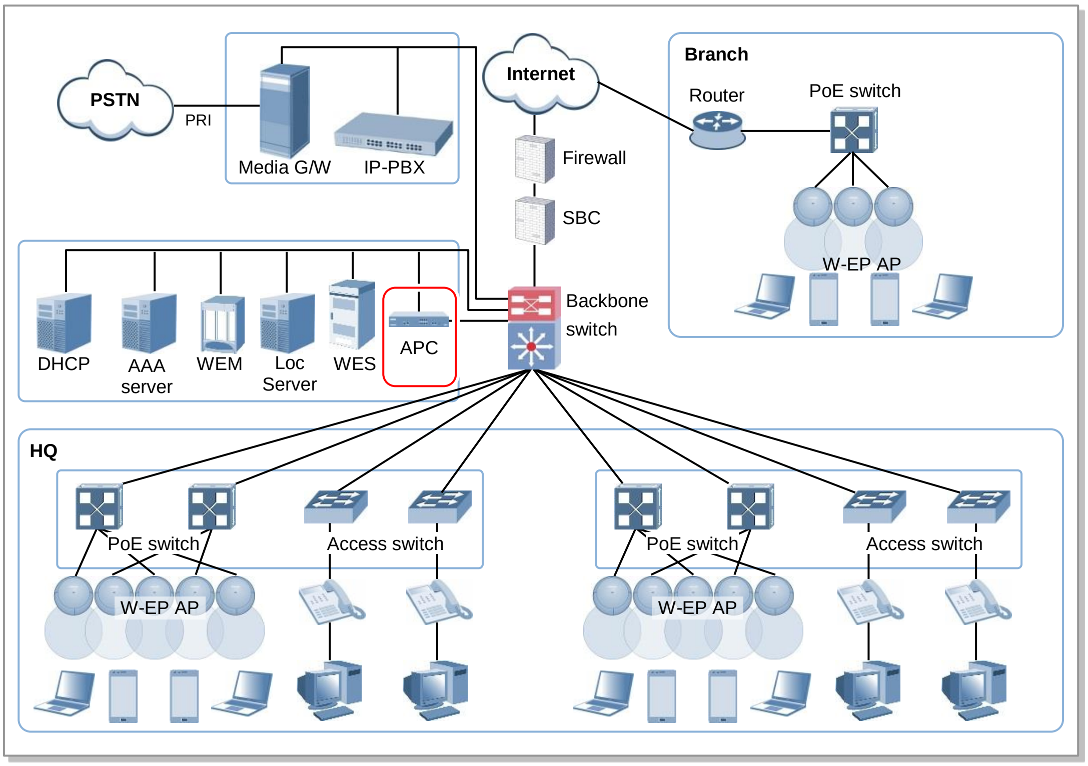


Figure 15. Example of W-EP Wireless LAN System Configuration for Multiple Sites consisting of Headquarter and Branches

If user traffics are concentrated on a single centralized APC when there are many branches or they are far from headquarter, performance may be deteriorated due to the time delay of packet transmission, etc. Therefore, use different operation schemes according to the location of W-EP wireless LAN AP in the configuration of headquarter and branches.
In other words, the local W-EP wireless LAN AP in a headquarter does traffic tunneling to an APC and the branch AP installed in a branch switches a user traffic directly to a destination address without tunneling to the APC. Even at this time, the APC in headquarter manages all the W-EP wireless LAN APs and users.

1.5 NAT Configuration between AP and APC

The APC system provides the same services even when the APC or AP is in a NAT environment.

If the APC system is in a NAT environment and obtaining a public IP address is difficult, the APC can be configured to use a private IP address by enabling port mapping on the existing NAT equipment, so that it can provide services to APs on the public IP network and APs existing under other NAT networks.

Using this feature requires that the NAT equipment be applied with the following port settings:

Service	TCP Port	UDP Port	Description
General	20, 21	-	FTP Server
	22	-	Secure Shell
	23	-	Telnet
	80, 443	-	HTTP Web Server
	123	123	NTP
AP-APC Connection	-	5246, 5247	CAPWAP

An example of service configuration diagram for the NAT environment is illustrated below.

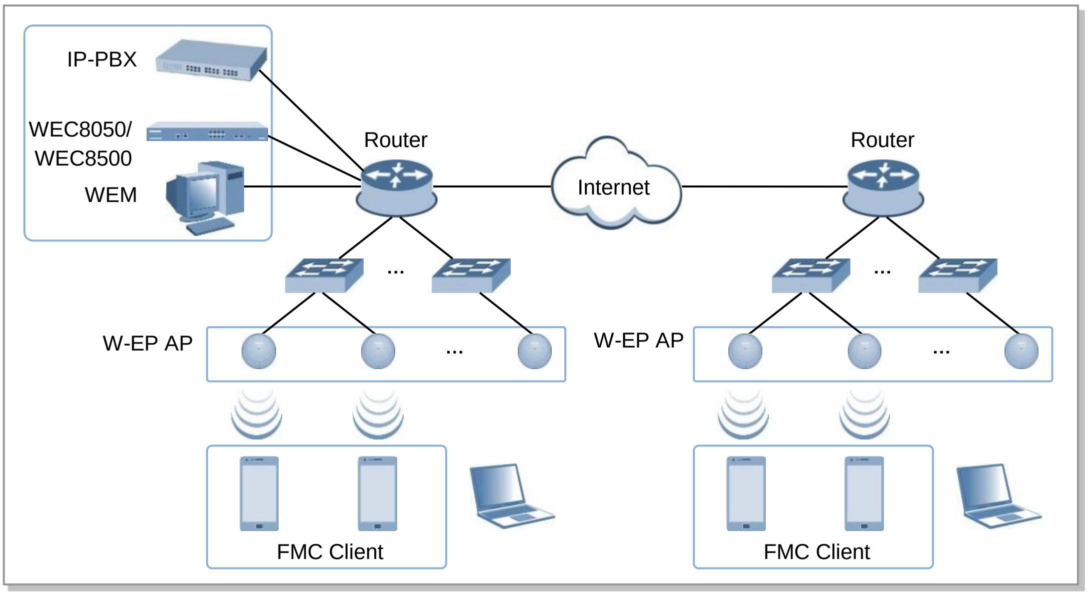


Figure 16. AP-APC NAT Environment Configuration Diagram

CHAPTER 2. Basic System Configuration

In this chapter, the basic system configuration using web and Command Line Interface (CLI) is introduced and how to use CLI and Web UI is described.

2.1 Basic System Configuration

2.1.1 CLI Connection

Connecting to APC using CLI is as follows:

- Direct connection to the system console port (Baud rate: 115200, Uncheck all Flow Control settings)
- Telnet or SSH connection through an Ethernet port (Telnet and SSH are disabled by default. You have to manually enable them from the GUI.)

When the booting of APC is completed, log into the system as follows:

1) For the first connection, log in using ID: 'samsung' and Password: 'samsung'.

```
USERNAME : samsung
PASSWORD : samsung

THIS IS YOUR FIRST LOGIN AFTER USER ACCOUNT HAS BEEN CREATED.

YOU MUST CHANGE YOUR PASSWORD.

 ENTER LOGIN PASSWORD           : samsung
 ENTER NEW PASSWORD             : ********
 CONFIRM NEW PASSWORD           : ********
 PASSWORD SUCCESSFULLY CHANGED
WEC8500 #
```

2) After the first login, you must change the password. Use the changed password for the next login.

NOTE

The default ID of APC is set to 'samsung' that has an administrator privilege.

2.1.2 Managing Operator Account

An operator who has an administrator privilege (level 1) can create or delete a new operator account. When creating an account, specify the account's privilege level (level 1-4).

To set up operator account related functions, go to configure mode by executing the following command.

```
WEC8500# configure terminal
WEC8500/configure #
```

Adding or deleting an account

The commands used to create or delete an account are as follows:

- mgmt-user [USERNAME] [USERLEVEL] description [DESCRIPTION]: Adds a user
- no mgmt-user [USERNAME]: Deletes a user

Parameter	Description
USERNAME	User ID
USERLEVEL	User level
DESCRIPTION	Adds user information

```
WEC8050/configure# mgmt-user test 1 description "test account"

 PASSWORD                  : *********
 CONFIRM PASSWORD          : *********
 USER(test) CREATED.

WEC8050/configure# no mgmt-user test
user(test) deleted.
```

Retrieving account information

To check user account information use the 'show mgmt-users' command.

Changing Password

Use the 'password' command to change the password for your account.
The 'password' command must be executed in the highest user mode.

```
WEC8500# password
 CURRENT PASSWORD          : ********
 NEW PASSWORD              : ********
 CONFIRM NEW PASSWORD      : ********
```

2.1.3 APC Management Port Configuration

To connect to the APC remotely using telnet/SSH or web, it is necessary to set up an IP address to the management port.

Set up the management port as follows:

1) Go to configure → 'mgmt0' interface configuration mode of CLI.

Note: Management Port is available in WEC 8500 only. It is pre-configured with an IP address of 192.168.1.2/24. If you wish to change the IP address, follow these instructions:

```
WEC8500# configure terminal
WEC8500/configure# interface mgmt0
```

2) Set up an IP address.

```
WEC8500/configure/interface mgmt0# ip address 100.100.100.1/24
```

2.1.4 SNMP Community Configuration

To connect to the web server of APC, it is necessary to add Simple Network Management Protocol (SNMP) community through CLI. For more information, see '10.1 SNMP Configuration'.

2.1.5 CLI Basic Usage

The CLI is a text command based interface used to change or retrieve the system settings. Several users can change the settings at the same time using the CLI of the same system. Because privilege per user is already configured, a user can execute a command allowed by the user's privilege. Various commands are available for each system function. For more information, see ANNEX 'CLI Command Structure'.

Command Help

The CLI provides a help for all the commands. To see a help for a command and parameter, enter '?'. Based on an input character, it shows a help for a command or parameter that can be entered.

Category	Description
?	Displays the command list and help at the current level
Command ?	Displays the parameter and help required for a command

A usage example is given below.

```
WEC8500# show ?

     80211a                   Display 802.11a network settings
     80211bg                  Display 802.11bg network settings
     80211h                   Display 802.11h configuration
     access-list              List IP access lists
     alarm                    Show alarm information
     ap                       Show ap information
     ap-debug                 Show ap debug information
     ...
     vap                      Show vap information
     version                  Show package version information
     vlan                     Display VLAN information
     vqm                      Show vqm command
     vrrp                     VRRP information
     wids                     Wids command
     wips                     Wips command
     wireless-acl-list        Show wireless-acl-list
     wlan                     Show wlan information

WEC8500#
```

Command automatic completion function

The CLI supports the command automatic completion function using the TAB key. When you press the TAB key after entering the first few characters of a command, the rest characters of the command that starts with the entered characters is automatically entered. If there are several commands that start with the entered characters, press the TAB key to jump to the next command. The below example shows the ‘show’, ‘save’, or ‘ssh’ command is entered in order by entering ‘s’ and pressing the TAB key.

```
WEC8500# s
```

[When the TAB key is pressed]

```
WEC8500# show
```

[When the TAB key is pressed once again]

```
WEC8500# save
```

Command error

When a command that is not supported by the system is entered, an error message is displayed.

```
WEC8500# command-unknown
         ^
Error : Command ‘command-unknown’  does not exist
```

When a parameter that is not supported by a command is entered, an error message according to the situation is displayed.

```
WEC8500# configure test
                   ^
% Invalid parameter (mandatory)
```

Command modes

When the ‘exit’ command is entered, the mode is changed to the upper command mode.

2.2 Using Web UI

2.2.1 Web UI Connection

To use the WEC, i.e. Web UI of APC system, the IP address of ethernet port must be set up. When connecting to the IP address of APC ethernet port in a web browser, the below login window is displayed. Log in using a default connection account ‘samsung’.
Note: You must first change the default password via CLI connection.

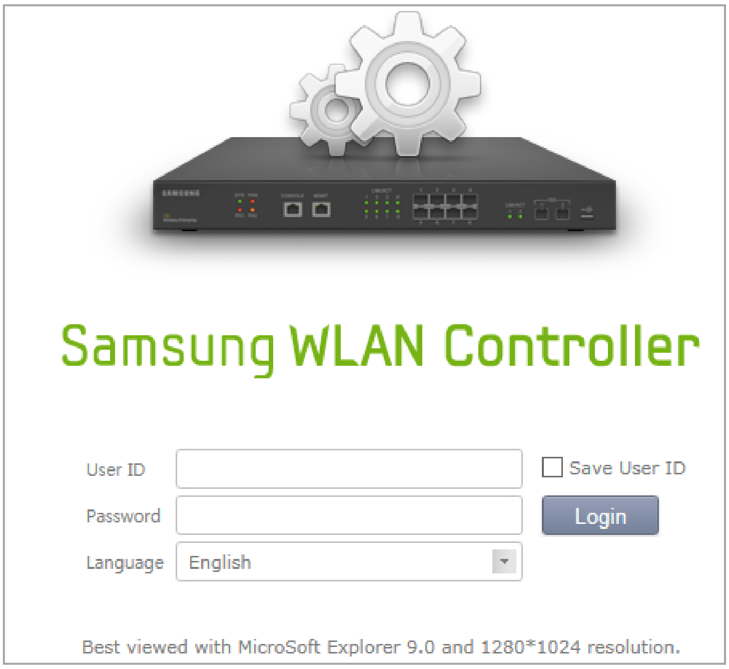


Figure 17. Web UI Connection Window

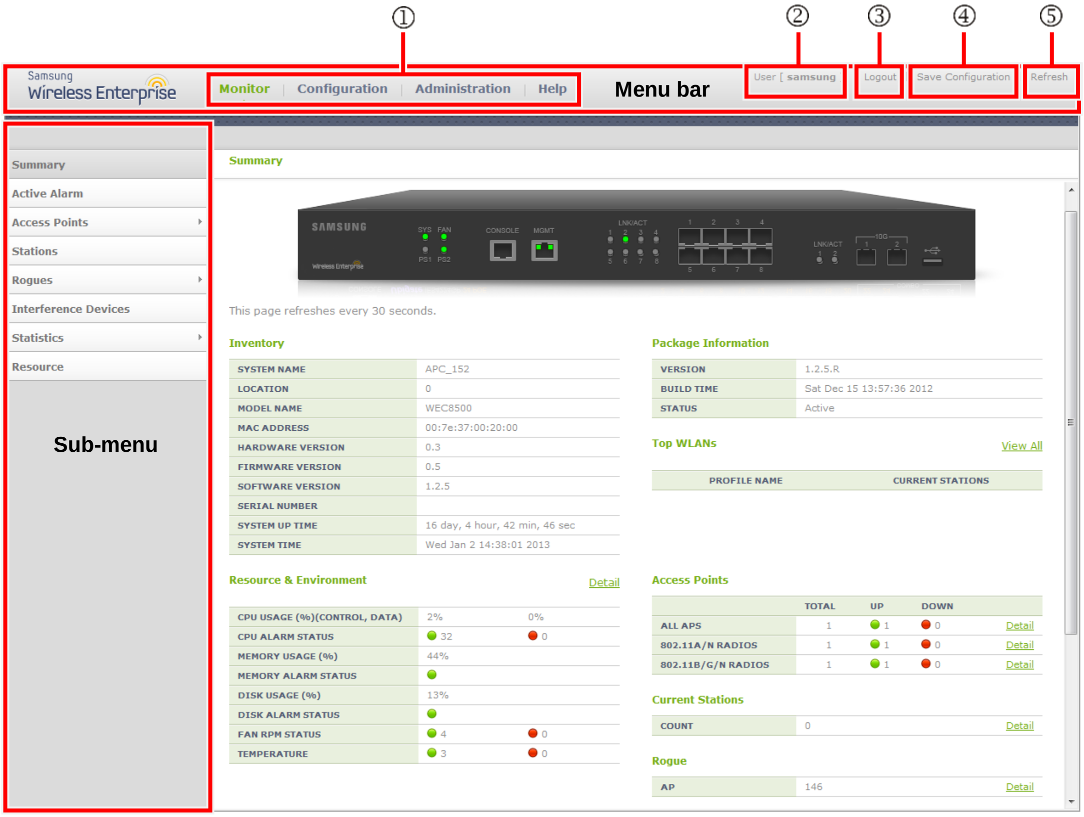
Note: WEC 8050 does not have a Management Port. We need to setup one of the 4 Ethernet ports as a Management port by CLI connection (Baud rate: 115200, Uncheck all Flow Control settings).

Example:

```
WEC8050# configure terminal
WEC8050/configure# interface ge4
WEC8050/configure/interface ge4# no switchport
WEC8050/configure/interface ge4# ip address 192.168.1.2/24
WEC8050/configure/interface ge4# end
WEC8050# save local
```

2.2.2 WEC Main Window

The WEC Main window is a screen that appears first after connecting to an APC and it consists of menu bar, sub-menus, and detail windows of each menu.



Summary

This page refreshes every 30 seconds.

Inventory

SYSTEM NAME	APC_152
LOCATION	0
MODEL NAME	WEC8500
MAC ADDRESS	00:7e:37:00:20:00
HARDWARE VERSION	0.3
FIRMWARE VERSION	0.5
SOFTWARE VERSION	1.2.5
SERIAL NUMBER	
SYSTEM UP TIME	16 day, 4 hour, 42 min, 46 sec
SYSTEM TIME	Wed Jan 2 14:38:01 2013

Package Information

VERSION	1.2.5.R
BUILD TIME	Sat Dec 15 13:57:36 2012
STATUS	Active

Top WLANs View All

PROFILE NAME	CURRENT STATIONS

Resource & Environment Detail

CPU USAGE (%)(CONTROL, DATA)	2%	0%
CPU ALARM STATUS	● 32	● 0
MEMORY USAGE (%)	44%	
MEMORY ALARM STATUS	●	
DISK USAGE (%)	13%	
DISK ALARM STATUS	●	
FAN RPM STATUS	● 4	● 0
TEMPERATURE	● 3	● 0

Access Points

	TOTAL	UP	DOWN	
ALL APS	1	● 1	● 0	Detail
802.11A/N RADIOS	1	● 1	● 0	Detail
802.11B/G/N RADIOS	1	● 1	● 0	Detail

Current Stations

COUNT	0	Detail

Rogue

AP	146	Detail

Figure 18. WEC Main Window

Menu bar

The menu bar consists of the following items:

- ①: Provides detail configuration or retrieval function for each item. When you select each item, lower menus in the sub-menus area are displayed.
- ②: Displays a user login ID.
- ③: Logs out from the WEC.
- ④: Saves the current configuration information into the system.
- ⑤: Refreshes the screen.

Sub-menus

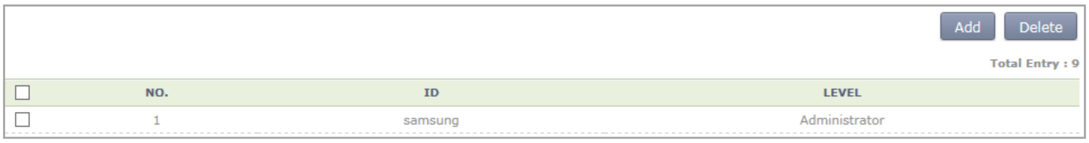
This provides the detail menus for Monitor, Configuration, Administration, or Help in the menu bar.

2.2.3 Managing Operator Account

To add a operator account in Web UI, follow the below procedure.

In the menu bar of **<WEC Main window>**, select **<Administration>** and then select **<Local Management Users>** menu in the sub menu. The subtree shows the **<APC>** and **<AP>** menu items. Select **<APC>**.

You can add or delete a operator account in the WEC.

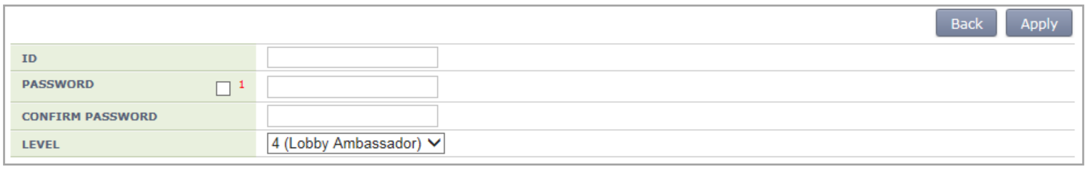


Total Entry : 9

□	NO.	ID	LEVEL
□	1	samsung	Administrator

Figure 19. Operator Account Management Window

1) To add an account, click the **<Add>** button.



ID	
PASSWORD □ 1	
CONFIRM PASSWORD	
LEVEL	4 (Lobby Ambassador)

Figure 20. Operator Account Addition Window

2) Enter an item according to each parameter description, and click the **<Apply>** button.
   - ID: Username to add
   - PASSWORD: User’s initial password
   - CONFIRM PASSWORD: Re-enter the initial password
   - LEVEL: User privilege
     - 1 (Administrator): Administrator privilege that allows to execute all the commands
     - 2 (Operator): Can change system configuration.
     - 3 (Monitor): Can retrieve system status.
     - 4 (Lobby Ambassador): Temporary user

CHAPTER 3. Data Network Function

In this chapter, how to set up the data network functions of APC including VLAN, link aggregation, and layer 3 protocol is described.

3.1 Port Configuration

The APC port is configured with a physical interface.

- Physical interface of 11 ports except WEC8500 console port
- Physical interface of 4 ports except WEC8050 console port

3.1.1 Port management

NOTE

The WEC8500 Management port is used to manage the WEC8500. It does not support VLAN and its interface name is ‘mgmt0’. The 8 ports at the right side of Management port are 10/100/1000 BASE T-ports and their names are GE1-8.

To the right side of the 10/100/1000 BASE T-ports, there are two Gigabit ports, i.e. XE1 and XE2.

Configuration using CLI

To configure the port related function, enter into the interface mode by entering the ‘interface [INTERFACE_NAME]’ command in the configure mode.
An example of entering into the interface setup mode of the management port is shown below.

```
WEC8500# configure terminal
WEC8500/configure# interface mgmt0
WEC8500/configure/interface mgmt0#
```

The port related CLI commands are as follows:

[auto-nego, speed, duplex]

The commands used to configure an auto-nego, speed, and duplex addresses are shown below. To delete the configuration, enter the ‘no’ parameter.

```
WEC8500/configure/interface ge1# speed-duplex ?
  10-full                     Set 10Mb/s full-duplex
  10-half                     Set 10Mb/s half-duplex
  100-full                    Set 100Mb/s full-duplex
  100-half                    Set 100Mb/s half-duplex
  1000-full                   Set 1000Mb/s full-duplex
  1000-half                   Set 1000Mb/s half-duplex
  auto-nego                   Set auto negotiation speed/duplex
```

[admin status]

This is a command that makes the port not working. The ‘no’ parameter is used to restart the port.

```
shutduown
no shutdown
```

[flow control]

This is a command that operates flow control to the port. The ‘no’ parameter is used to stop the flow control.

```
flowcontrol on
no flowcontrol on
```

[switch port]

This is a command that changes the port to the L2 mode. The ‘no’ parameter is used to change it to the L3 mode.

```
switchport
no switchport
```

[ip address]

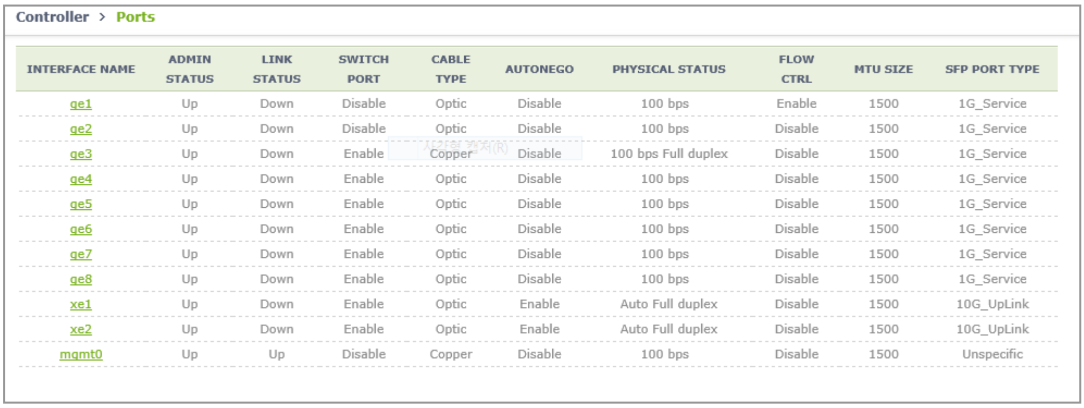
This is a command that configures a static IP address. To delete the configuration, enter the ‘no’ parameter.

- ip address {A.B.C.D/mask length}
- no ip address {A.B.C.D} {A.B.C.D}
- no ip address {A.B.C.D/mask length}

Configuration using Web UI

In the menu bar of **<WEC Main window>**, select **<Configuration>** and then select the **<Controller>** → **<Ports>** menu in the sub-menus. Operator can configure the ports.

The Ports initial window is shown below.
Operator can check the current status of each port.



Controller > Ports

INTERFACE NAME	ADMIN STATUS	LINK STATUS	SWITCH PORT	CABLE TYPE	AUTONEGO	PHYSICAL STATUS	FLOW CTRL	MTU SIZE	SFP PORT TYPE
ge1	Up	Down	Disable	Optic	Disable	100 bps	Enable	1500	1G_Service
ge2	Up	Down	Disable	Optic	Disable	100 bps	Disable	1500	1G_Service
ge3	Up	Down	Enable	Copper	Disable	100 bps Full duplex	Disable	1500	1G_Service
ge4	Up	Down	Enable	Optic	Disable	100 bps	Disable	1500	1G_Service
ge5	Up	Down	Enable	Optic	Disable	100 bps	Disable	1500	1G_Service
ge6	Up	Down	Enable	Optic	Disable	100 bps	Disable	1500	1G_Service
ge7	Up	Down	Enable	Optic	Disable	100 bps	Disable	1500	1G_Service
ge8	Up	Down	Enable	Optic	Disable	100 bps	Disable	1500	1G_Service
xe1	Up	Down	Enable	Optic	Enable	Auto Full duplex	Disable	1500	10G_UpLink
xe2	Up	Down	Enable	Optic	Enable	Auto Full duplex	Disable	1500	10G_UpLink
mgmt0	Up	Up	Disable	Copper	Disable	100 bps	Disable	1500	Unspecific

Figure 21. Port Management Window

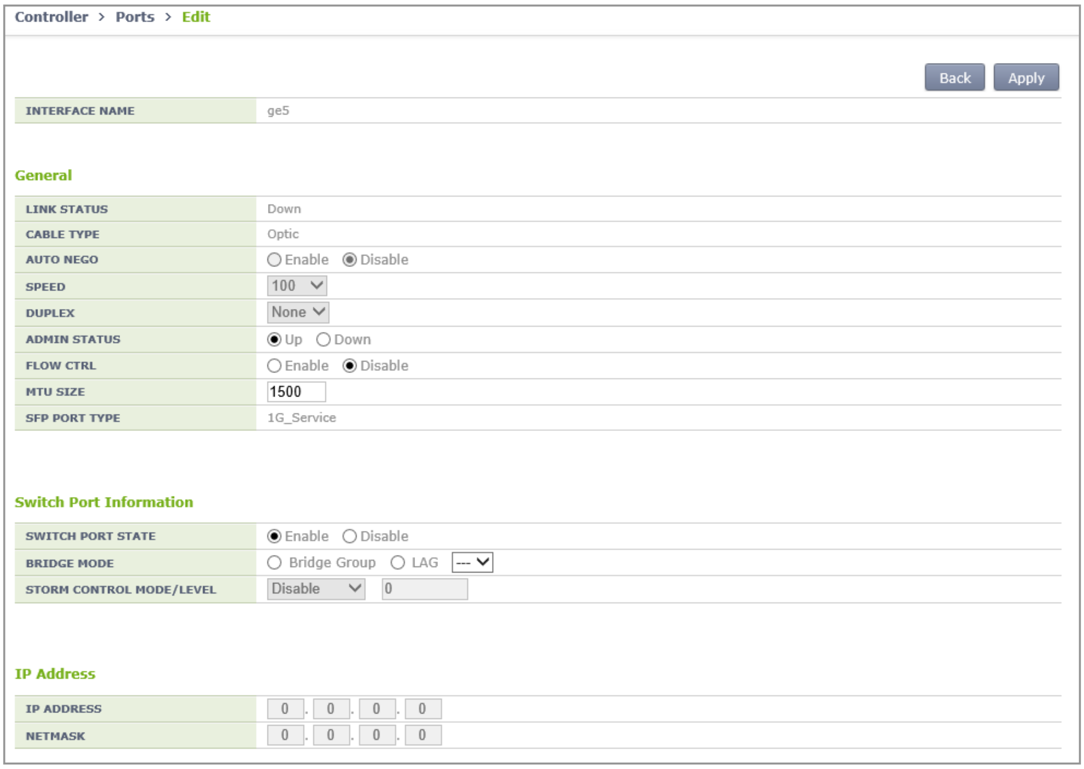
NOTE

The auto-nego, speed, or duplex can be configured only when the cable type is Copper.

They cannot be configured if the cable type is Optic (The auto-nego should always be enabled whether the cable type is copper or optic).

[Port Configuration Change]

1) In the Ports initial window, click the <INTERFACE NAME> button to go to port configuration change window.
2) In the port configuration change window, the auto-nego, speed, duplex, admin status, flow control, mtu size, switch port, or ip address, etc. can be configured.



INTERFACE NAME	ge5

General

LINK STATUS	Down
CABLE TYPE	Optic
AUTO NEGO	○ Enable ● Disable
SPEED	100
DUPLEX	None
ADMIN STATUS	● Up ○ Down
FLOW CTRL	○ Enable ● Disable
MTU SIZE	1500
SFP PORT TYPE	1G_Service

Switch Port Information

SWITCH PORT STATE	● Enable ○ Disable
BRIDGE MODE	○ Bridge Group ○ LAG ---
STORM CONTROL MODE/LEVEL	Disable 0

IP Address

IP ADDRESS	0 . 0 . 0 . 0
NETMASK	0 . 0 . 0 . 0

Figure 22. Port Configuration Change Window

3.2 Interface Configuration

The WEC8500 interface consists of the following physical interface and virtual interface.

- Physical interface of 11 ports except console port
- 1024 virtual interfaces using VLAN

There are two types of WEC8050 interface as shown below; physical interface and virtual interface.

- Physical interface of 4 ports except console port
- 128 virtual interfaces using VLAN

3.2.1 Interface management

NOTE

The WEC8500 Management port is used to manage the WEC8500. It does not support VLAN and its interface name is ‘mgmt0’. The 8 ports at the right side of Management port are 10/100/1000 BASE T-ports and their names are GE1-8.

To the right side of the 10/100/1000 BASE T-ports, there are two Gigabit ports, i.e. XE1 and XE2.

Configuration using CLI

To configure the interface related function, go to the interface mode by entering the ‘interface [INTERFACE_NAME]’ command in the configure mode. An example of entering into the interface mode of the management port is shown below.

```
WEC8500# configure terminal
WEC8500/configure# interface mgmt0
WEC8500/configure/interface mgmt0#
```

The interface related CLI commands are as follows:

[ip address]

This is a command that configures a static IP address. The ‘no’ parameter is used to delete the configuration.

- ip address {A.B.C.D/mask length}
- no ip address {A.B.C.D} {A.B.C.D}
- no ip address {A.B.C.D/mask length}

[ip address dhcp]

This is a command that configures a dynamic IP address using DHCP. The ‘no’ parameter is used to delete the configuration.

- ip address dhcp
- no ip address dhcp

[shutdown]

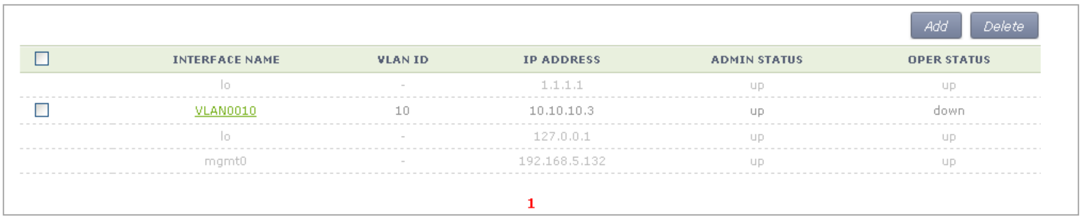
This is a command that makes the interface not working. The ‘no’ parameter is used to restart the interface.

- shutdown
- no shutdown

Configuration using Web UI

In the menu bar of <**WEC Main window**>, select <**Configuration**> and then select the <**Controller**> → <**Interfaces**> menu in the sub-menus. You can configure an interface and VLAN.

The Interface initial window is shown below.

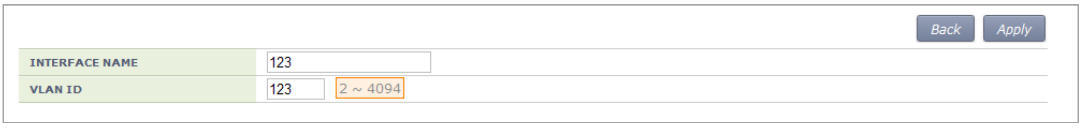


□	INTERFACE NAME	VLAN ID	IP ADDRESS	ADMIN STATUS	OPER STATUS
	lo	-	1.1.1.1	up	up
□	VLAN0010	10	10.10.10.3	up	down
	lo	-	127.0.0.1	up	up
	mgmt0	-	192.168.5.132	up	up

Figure 23. Interfaces Window (1)

[Adding VLAN]

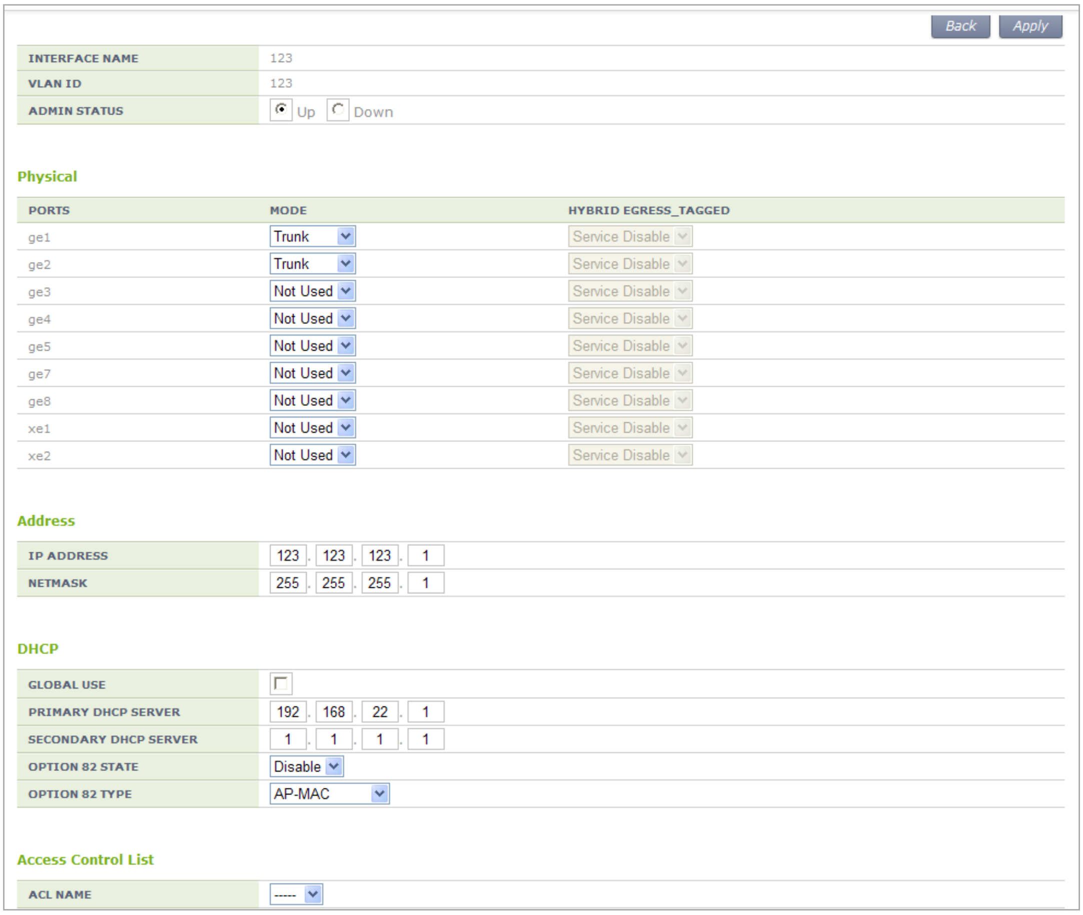
1) In the Interface initial window, click the <**Add**> button to go to VLAN creation window.
2) Enter an INTERFACE NAME and VLAN ID in the VLAN creation window.
   The INTERFACE NAME describes a VLAN to create and English characters without a space, numbers, and ‘_’ can be used. The VLAN ID is the number from 1 to 4094 and it specifies a unique VLAN value.
   Click the <**Apply**> button to go to detail configuration screen.



INTERFACE NAME	123
VLAN ID	123 2 ~ 4094

Figure 24. Interfaces Window (2)

3) Perform detail configuration in the VLAN detail configuration window.
If you specify PRIMARY DHCP SERVER or SECONDARY DHCP SERVER in the DHCP area, you can specify the configuration of a DHCP server.
After configuration, click the <**Apply**> button to apply it to the system.



INTERFACE NAME	123
VLAN ID	123
ADMIN STATUS	● Up ○ Down

Physical

PORTS	MODE	HYBRID EGRESS_TAGGED
ge1	Trunk	Service Disable
ge2	Trunk	Service Disable
ge3	Not Used	Service Disable
ge4	Not Used	Service Disable
ge5	Not Used	Service Disable
ge7	Not Used	Service Disable
ge8	Not Used	Service Disable
xe1	Not Used	Service Disable
xe2	Not Used	Service Disable

Address

IP ADDRESS	123 . 123 . 123 . 1
NETMASK	255 . 255 . 255 . 1

DHCP

GLOBAL USE	□
PRIMARY DHCP SERVER	192 . 168 . 22 . 1
SECONDARY DHCP SERVER	1 . 1 . 1 . 1
OPTION 82 STATE	Disable
OPTION 82 TYPE	AP-MAC

Access Control List

ACL NAME	-----

Figure 25. Interfaces Window (3)

[Deleting VLAN]

In the Interface initial window, click the <**Delete**> button to delete a selected VLAN. The select VLAN cannot be deleted if it is being used in the system.

3.2.2 Managing Interface Group

To use WLAN and other services, it is necessary to configure an interface into an interface group.

Configuration using CLI

An example of entering into the group configuration mode of ifg_01 interface is shown below.

```
WEC8500# configure terminal
WEC8500/configure# if-group ifg_01
```

Interface Group related commands are as follows:

[Creating or Deleting Interface group]

This command creates an interface group. Use 'no' parameter to delete an interface group.

- if-group [INTERFACE_GROUP_NAME]
- no if-group [INTERFACE_GROUP_NAME]

[Adding or deleting Interface]

This command adds an interface to an interface group being configured. Use 'no' parameter to delete an interface.

- add-if [INTERFACE_GROUP_NAME]
- no add-if [INTERFACE_GROUP_NAME]

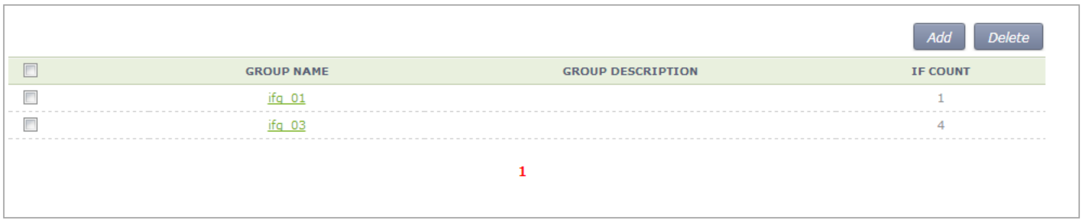
[Retrieving Interface Group Status]

This command retrieves the configuration status of an interface group.

- show if-group

Configuration using Web UI

In the menu bar of <**WEC Main window**>, select <**Configuration**> and then select the <**Controller**> → <**Interfaces Groups**> menu in the sub-menus. Click the <**Add**> or <**Delete**> button to add or delete an interface group.



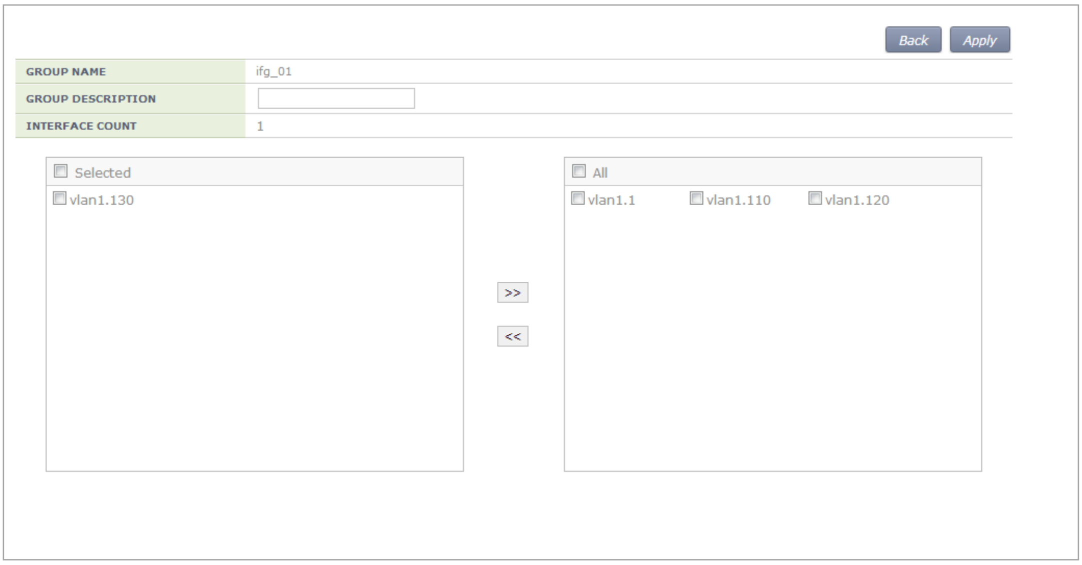
☐	GROUP NAME	GROUP DESCRIPTION	IF COUNT
☐	ifg_01		1
☐	ifg_03		4

Figure 26. Interface Group Window (1)

Follow the below procedure to add an interface group.

1) In the Interface group initial window, click the **<Add>** button.

2) Enter the GROUP NAME and GROUP DESCRIPTION information and then select the VLAN interface.



GROUP NAME	ifg_01
GROUP DESCRIPTION	
INTERFACE COUNT	1

□ Selected

□ vlan1.130

□ All

□ vlan1.1 □ vlan1.110 □ vlan1.120

Figure 27. Interface Group Window (2)

3) Click the **<Apply>** button to apply the configuration.

3.3 VLAN Configuration

3.3.1 VLAN

Configuration using CLI

To configure VLAN, go to the VLAN interface mode by executing the following command.

```
WEC8500# configure terminal
WEC8500/configure# interface vlan
WEC8500/configure/interface vlan#
```

The related command is shown below and the range of VLAN ID is 1-4094.

[vlan bridge]

This command creates VLAN. The ‘no’ parameter is used to delete VLAN.

- vlan [VLAN_ID] bridge 1
- no vlan [VLAN_ID] bridge 1

[switchport access vlan]

This command set the VLAN mode to the access or hybrid mode. The ‘no’ parameter is used to delete the VLAN configuration.

- switchport {access/hybrid} vlan [VLAN_ID]

[switchport mode]

This command configures the mode of switch port. The ‘no’ parameter is used to delete the configuration.

- switchport mode {access/hybrid/trunk}
- no switchport mode

[switchport hybrid allowed vlan]

This command configures the mode of switch port to hybrid. The ‘no’ parameter is used to delete the configuration.

- switchport hybrid allowed vlan: Configures VLAN to hybrid.
- switchport hybrid allowed vlan all: Configures all the allowed VLANs to hybrid.
- switchport hybrid allowed vlan none: Stops VLAN data transmission/reception.
- switchport hybrid allowed vlan add [VLAN_ID]: Adds VLAN to the hybrid mode.
- switchport hybrid allowed vlan remove [VLAN_ID]: Deletes VLAN from the hybrid mode.
- no switchport hybrid vlan: Deletes all the hybrid settings.

[switchport trunk allowed vlan]

This command configures the mode of switch port to trunk. The ‘no’ parameter is used to delete the configuration.

- switchport trunk allowed vlan: Configure VLAN to the trunk mode.
- switchport trunk allowed vlan all: Configure all the VLANs to the trunk mode.
- switchport trunk allowed vlan none: Stops VLAN data transmission/reception.
- switchport trunk allowed vlan add [VLAN_ID]: Adds VLAN to the trunk mode.
- switchport trunk allowed vlan remove [VLAN_ID]: Removes VLAN with the trunk mode.
- no switchport trunk vlan: Removes all the trunk settings.

[show vlan]

This command retrieves VLAN configuration status.

- show vlan [VLAN_ID]: Displays specific VLAN information.
- show vlan all bridge 1: Displays all the VLAN information.
- show vlan brief: Displays all the VLAN information briefly.
- show vlan dynamic bridge 1: Displays dynamic VLAN information.
- show vlan static bridge 1: Displays static VLAN information.

[Typical configuration procedure]

The typical configuration procedure of VLAN is as follows:

```
WEC8500# configure terminal
WEC8500/configure# bridge 1 protocol mstp
WEC8500/configure # vlan database
WEC8500/configure/vlan#vlan {2-4094} bridge 1
WEC8500/configure/vlan# exit
WEC8500/configure# interface vlan1.{2-4094}
```

Configuration using Web UI

In the menu bar of **<WEC Main window>**, select **<Configuration>** and then select the **<Controller>** → **<Interfaces>** menu in the sub-menus.

For more information about configuration procedure, see ‘3.2.1 Interface Management’.

3.3.2 Bridge

To set up bridge related functions, go to configure mode by executing the following command

```
WEC8500# configure terminal
```

The bridge related commands are as follows:

[bridge address]

This command configures a bridge address. The 'no' parameter is used to clear the configuration.

- bridge 1 address [MAC] [forward/discard] [IFNAME]
- no bridge 1 address [MAC] [forward/discard] [IFNAME]

Parameter	Description
MAC	MAC address. Entered in the format of HHHH.HHHH.HHHH.
forward/discard	- forward: Configures forward matching frame. - discard: Configures discard matching frame.
IFNAME	Interface name of a bridge.

[bridge ageing time]

This command configures the age-out time of a bridge. The 'no' parameter is used to clear the configuration.

- bridge-group 1 ageing-time [AGEINGTIME]
- no bridge-group 1 ageing-time

Parameter	Description
AGEINGTIME	age-out time (range: 10-1000000 s)

[bridge protocol]

This command creates a bridge in one of the IEEE 802.1Q Spanning-Tree Protocol (STP), IEEE802.1s multiple STP (MSTP), or IEEE 802.1W Rapid STP (RSTP) protocol.

- bridge 1 protocol [PROTOCOL]
- no bridge 1 protocol

Parameter	Description
PROTOCOL	Protocol to configure (ieee/mstp/rstp) - ieee: STP - mstp: MSTP - rstp: RSTP

[clear mac address-table]

This command deletes the filtering database of a default bridge.

- clear mac address-table [OPTION] [KIND] [WORD]

Parameter	Description
OPTION	Filtering database option (static/multicast) - static: Filtering database item that is configured as static - multicast: Filtering database item that is automatically configured by the multicast protocol
KIND	Filtering database type (address/vlan/interface) - address: Filtering database using a MAC address - vlan: Filtering database using the VLAN information. - interface: Filtering database using the interface information
WORD	Option

[clear mac address-table dynamic]

This command deletes bridge operation among the filtering database of a default bridge.

- clear mac address-table dynamic [KIND] [WORD]

Parameter	Description
KIND	Filtering database type (address/vlan/interface) - address: Filtering database using a MAC address - vlan: Filtering database using the VLAN information. - interface: Filtering database using the interface information
WORD	Option

[clear mac address-table dynamic bridge]

This command deletes the filtering database of bridge operation.

- clear mac address-table dynamic bridge [BRIDGE_NAME]
- clear mac address-table dynamic [address/interface/vlan] [WORD] bridge [NAME]

Parameter	Description
KIND	Filtering database type (address/vlan/interface) - address: Filtering database using a MAC address - vlan: Filtering database using the VLAN information. - interface: Filtering database using the interface information
WORD	Option
BRIDGE_NAME	Bridge name

[show bridge]

This command retrieves bridge information.

- show bridge

[show interface switchport bridge]

This command retrieves the bridge information, i.e. the layer 2 protocol characteristic information of the current VLAN, of a switch port.

- show interface switchport bridge [BRIDGE_NAME]

Parameter	Description
BRIDGE_NAME	Bridge name

[switchport]

This command configures a switch port, i.e. the layer 2 protocol characteristic information of the current VLAN. The ‘no’ parameter is used for default configuration. Go to interface mode and then execute the command.

- switchport
- no switchport

3.3.3 Spanning Tree

Configuration using CLI

To set up spanning tree related functions, go to configure mode by executing the following command.

```
WEC8500# configure terminal
```

The related command is as follows.

[bridge forward-time]

This command configures the forward time of a bridge. The ‘no’ parameter is used for default configuration.

- bridge 1 forward-time [FORWARD_DELAY]
- no bridge 1 forward-time

Parameter	Description
FORWARD_DELAY	Forward time delay (range: 4-30 s, default: 15)

[bridge hello-time]

This command configures the hello time of a bridge. The time required when a bridged LAN is changed to Bridge Protocol Data Units (BPDUs) is called as hello-time. The ‘no’ parameter is used for default configuration.

- bridge 1 hello-time [HELLOTIME]
- no bridge 1 hello-time

Parameter	Description
HELLOTIME	Hello BPDU interval (range: 1-10 s)

[bridge instance priority]

This command configures the bridge priority of MST instance. The ‘no’ parameter is used to delete priority.

- bridge 1 instance [INSTANCE_ID] priority [BRIDGE_PRIORITY]
- no bridge 1 instance [INSTANCE_ID]

Parameter	Description
INSTANCE_ID	Instance ID (range: 1-64)
BRIDGE_PRIORITY	Bridge priority (range: 0-61440)

[bridge max-age]

This command configures the max-age of a bridge. The ‘no’ parameter is used for default configuration.

- bridge 1 max-age [MAXAGE]
- no bridge 1 max-age

Parameter	Description
MAXAGE	Configures a maximum time (range: 6-40 s)

[bridge max-hops]

This command configures the maximum allowed number of hops of a Bridge Protocol Data Unit (BPDU) bridge in the MST area.
The ‘no’ parameter is used for default configuration.

- bridge 1 max-hops [HOP_COUNT]
- no bridge 1 max-hops

Parameter	Description
HOP_COUNT	Maximum allowed number of hops

[bridge multiple-spanning-tree enable]

This command configures a MSTP bridge. The ‘no’ parameter is used to clear the configuration.

- bridge 1 multiple-spanning-tree enable
- no bridge 1 multiple-spanning-tree enable

[bridge rapid-spanning-tree enable]

This command configures a RSTP bridge. The ‘no’ parameter is used to clear the configuration.

- bridge 1 rapid-spanning-tree enable
- no bridge 1 rapid-spanning-tree enable(bridge-forward)

[bridge spanning-tree enable]

This command configures a STP bridge. The ‘no’ parameter is used to clear the configuration.

- bridge 1 spanning-tree enable
- no bridge 1 spanning-tree enable(bridge-forward)

[bridge priority]

This command configures the priority of a bridge. The ‘no’ parameter is used to delete a priority.

- bridge 1 priority [PRIORITY]
- no bridge 1 priority

Parameter	Description
PRIORITY	Bridge priority (range: 0-61440)

[bridge shutdown]

This command clears bridge settings. The ‘no’ parameter is used to restart a bridge.

- bridge shutdown [1-32]
- no bridge shutdown [1-32]

Configuration using Web UI

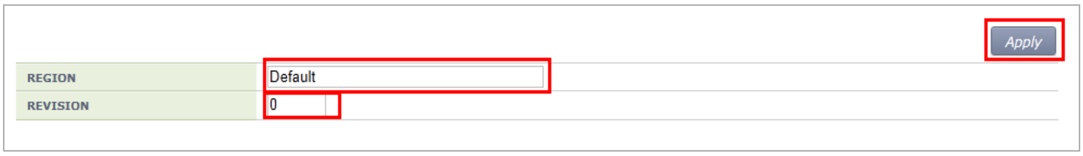
In the menu bar of <**WEC Main window**>, select <**Configuration**> and then select the <**Controller**> → <**Network**> → <**MSTP**> menu in the sub-menus.

The sub-menus of the MSTP menu are as follows:

- Config: Configures the spanning tree.
- Instance: Manages the MSTP VLAN instance.
- Port: Manages the MSTP port.

[Configuring Spanning Tree]

After selecting the <**Config**> menu, enter configuration information and then click the <**Apply**> button.

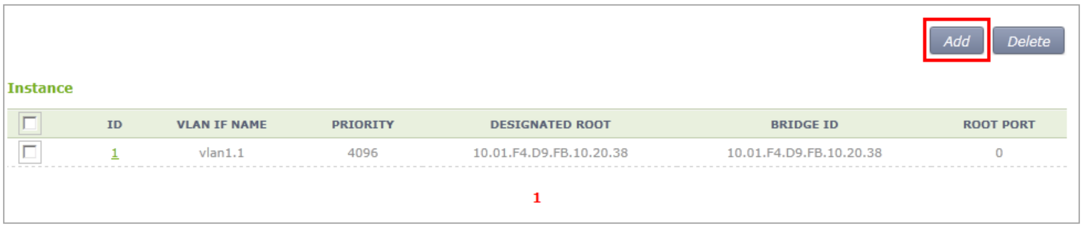


REGION	Default
REVISION	0

Figure 28. Spanning Tree Configuration Window (1)

[Managing the MSTP VLAN instance]

When you select the <**Instance**> menu, the configured MSTP VLAN Instance list is displayed on the window. Click the <**Add**> or <**Delete**> button to add or delete an instance.



Instance

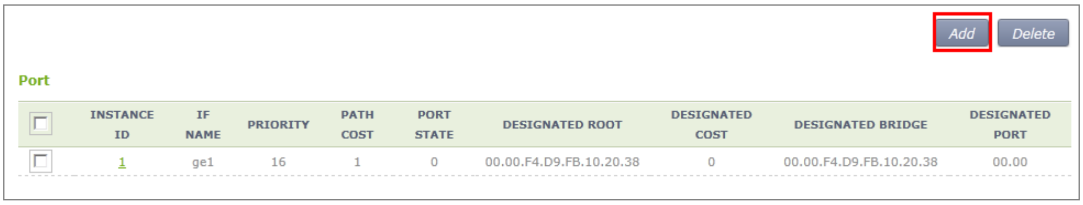
□	ID	VLAN IF NAME	PRIORITY	DESIGNATED ROOT	BRIDGE ID	ROOT PORT
□	1	vlan1.1	4096	10.01.F4.D9.FB.10.20.38	10.01.F4.D9.FB.10.20.38	0

1

Figure 29. Spanning Tree Configuration Window (2)

[Managing MSTP Port]

When you select the <**Port**> menu, the configured MSTP Port list is displayed on the window. Click the <**Add**> or <**Delete**> button to add or delete a port.



Port

□	INSTANCE ID	IF NAME	PRIORITY	PATH COST	PORT STATE	DESIGNATED ROOT	DESIGNATED COST	DESIGNATED BRIDGE	DESIGNATED PORT
□	1	ge1	16	1	0	00.00.F4.D9.FB.10.20.38	0	00.00.F4.D9.FB.10.20.38	00.00

Figure 30. Spanning Tree Configuration Window (3)

3.4 Layer 3 Protocol Configuration

This provides the IP address configuration and static/dynamic routing configuration of an interface. The APC provides the Open Shortest Path First (OSPF) routing protocol.

3.4.1 IP Address Configuration

The procedure for IP address configuration is given below.

1) Go to configure → interface configuration mode of CLI.

```
WEC8500# configure terminal
WEC8500/configure# interface ge2
```

2) Set up an IP address.

```
WEC8500/configure/interface ge2# ip address 100.100.100.1/24
```

3) Enable the interface.

```
WEC8500/configure/interface ge2# no shutdown
```

3.4.2 Static Routing Configuration

Configuration using CLI

1) Go to configure mode of CLI.

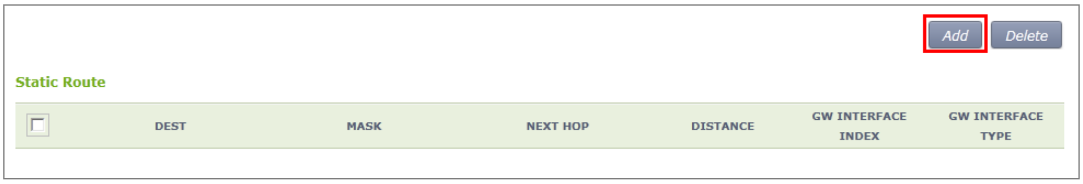
```
WEC8500# configure terminal
```

2) Configure static routing.

```
WEC8500/configure# ip route 10.2.3.0/24 30.30.30.2
```

Configuration using Web UI

In the menu bar of **<WEC Main window>**, select **<Configuration>** and then select the **<Controller>** → **<Network>** → **<Static Route>** menu in the sub-menus.
The configured static route list is displayed on the window. When you click the **<Add>** or **<Delete>** button, you can add or delete a static routing entry.



Static Route

□	DEST	MASK	NEXT HOP	DISTANCE	GW INTERFACE INDEX	GW INTERFACE TYPE

Figure 31. Static Routing Configuration Window

After adding or deleting an entry, check if the information is reflected to the list in the Static Route window. If the added information is not displayed, it means the added routing information is not enabled. If the operational status of an interface that will be used as a routing result is not UP, check the interface status through CLI or Web UI.
Because only enabled routing entries are listed in the Web UI, you cannot remove a disabled routing entry.

3.4.3 IP Multicast Routing Configuration

1) Go to configure mode of CLI.

```
WEC8500# configure terminal
WEC8500/configure#
```

2) Enable or disable multicast-routing.
   - ip multicast-routing
   - no multicast-routing

3) Check multicast-routing using the ‘show running-config network’ command.

3.4.4 PIM Configuration

The procedure for Protocol Independent Multicast (PIM) configuration is given below.

1) Go to configure → interface configuration mode of CLI.

```
WEC8500# configure terminal
WEC8500/configure# interface ge2
```

2) Configure the PIM sparse mode to an interface.

```
WEC8500/configure/interface ge2# ip pim sparse-mode
```

3) Check a configured PIM using the ‘show running-config network’ command.
To check the multicast-routing table, use the ‘show ip mroute’ command.

```
WEC8500# show ip mroute
(90.90.1.242, 224.0.1.1)       Iif: mgmt0     Oifs: pimreg
```

3.4.5 OSPF Configuration

3.4.5.1 General settings

Configuration using CLI

1) Go to configure → ospf configuration mode of CLI.

```
WEC8500# configure terminal
WEC8500/configure# router ospf
WEC8500/configure# router ospf ?
  1 - 10                    OSPF process ID
```

2) Configure the process ID from 1 to 10.

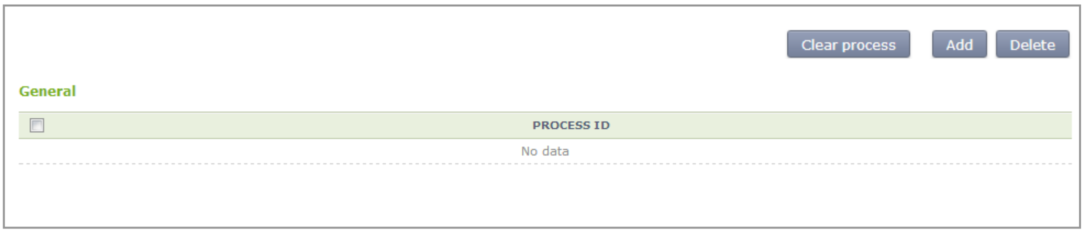
```
WEC8500/configure# router ospf ?
1 - 10                     OSPF process ID
WEC8500/configure# router ospf 2
WEC8500/configure/router/ospf 2#
```

Parameter	Description
OSPF process ID	Configure the process ID from 1 to 10.

Configuration using Web UI

In the menu bar of **<WEC Main window>**, select **<Configuration>** and then select the **<Controller>** → **<Network>** → **<OSPF>** → **<General>** menu in the sub-menus.

The OSPF initial window is shown below.

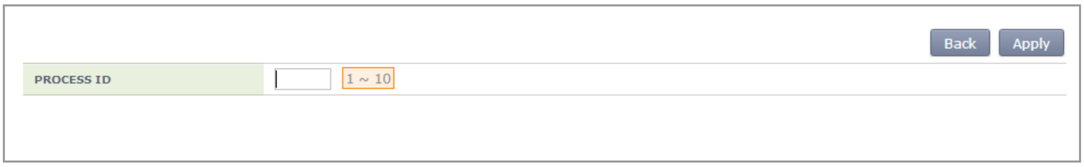


General

☐	PROCESS ID
	No data

Figure 32. OSPF Configuration Window

Click the **<Add>** button and configure the PROCESS ID to 1-10 in the below screen.



PROCESS ID		1 ~ 10

Configuration using CLI

1) Go to configure → ospf configuration mode of CLI.

```
WEC8500# configure terminal
WEC8500/configure# router ospf
WEC8500/configure# router ospf ?
1 - 10                          OSPF process ID
WEC8500/configure# router ospf 2
WEC8500/configure/router/ospf 2#
```

2) The detail configuration items of a process ID are as follows:

```
WEC8500/configure/router/ospf 2# ?

     area                     OSPF area parameters
     auto-cost                Calculate OSPF interface cost according
to bandwidth
     capability               Enable specific OSPF feature
     compatible               OSPF compatibility list
     default-information      Control distribution of default
information
     default-metric           Set metric of redistributed routes
     distance                 Define an administrative distance
     distribute-list          Filter networks in routing updates
     exit                     Exit from router mode
     host                     OSPF stub host entry
     max-concurrent-dd        Maximum number allowed to process DD
concurrently
     maximum-area             Maximum number of ospf area
     neighbor                 Specify a neighbor router
     network                  Enable routing on an IP network
     ospf                     OSPF specific commands
     overflow                 Control overflow
     passive-interface        Suppress routing updates on an interface
     redistribute             Redistribute information from another
routing protocol
     router-id                Router-id for the OSPF process
     summary-address          Configure IP address summaries
     timers                   Adjust routing timers
```

3) Router ID configuration
Enter an IP address to use.

```
WEC8500/configure/router/ospf 2# router-id ?
A.B.C.D                       OSPF router-id in IP address format
WEC8500/configure/router/ospf 2# router-id 10.10.0.1 ?
  <cr>
```

Parameter	Description
OSPF router-id in IP address	Enter an IP address.

4) AUTO COST configuration
Enter an OSPF cost value (1-4294967) to use.

```
WEC8500/configure/router/ospf 2# auto-cost ?
  reference-bandwidth         Use reference bandwidth method to assign
OSPF cost
WEC8500/configure/router/ospf 2# auto-cost reference-bandwidth ?
  1 - 4294967                 The reference bandwidth in terms of
Mbits per second

WEC8500/configure/router/ospf 2# auto-cost reference-bandwidth 200 ?
  <cr>
WEC8500/configure/router/ospf 2# auto-cost reference-bandwidth 200
```

Parameter	Description
reference-bandwidth	Enter a value from 1-4294967.

5) CAPABILITY OPAQUE configuration

Enter the capability opaque.

```
WEC8500/configure/router/ospf 2# capability ?
     opaque                   Opaque LSA
WEC8500/configure/router/ospf 2# capability opaque ?
  <cr>
WEC8500/configure/router/ospf 2# capability opaque
```

Parameter	Description
Capability opaque	Enabled when the CLI is entered.

6) COMPATIBLE RFC configuration

Enter the compatible rfc1583.

```
WEC8500/configure/router/ospf 2# compatible ?
  rfc1583                     Compatible with RFC 1583
WEC8500/configure/router/ospf 2# compatible rfc1583 ?
  <cr>
WEC8500/configure/router/ospf 2# compatible rfc1583
```

Parameter	Description
compatible rfc1583	Enabled when the CLI is entered.

7) DEFAULT METRIC configuration

Enter the DEFAULT METRIC (1-16777214) to use.

```
WEC8500/configure/router/ospf 2# default-metric ?
  1 - 16777214                Default metric
WEC8500/configure/router/ospf 2# default-metric 3 ?
  <cr>
WEC8500/configure/router/ospf 2# default-metric 3
```

Parameter	Description
Default metric	Enter a value from 1-16777214.

8) MAX CONCURRENT DD configuration

Enter the MAX CONCURRENT DD (1-65535) to use.

```
WEC8500/configure/router/ospf 2# max-concurrent-dd ?
  1 - 65535                   Number of DD process
WEC8500/configure/router/ospf 2# max-concurrent-dd 2 ?
  <cr>
WEC8500/configure/router/ospf 2# max-concurrent-dd 2
```

9) MAXIMUM AREA configuration
Enter the DEFAULT METRIC (1-4294967294) to use.

```
WEC8500/configure/router/ospf 2# maximum-area ?
  1 - 4294967294              Area limit
WEC8500/configure/router/ospf 2# maximum-area 3 ?
  <cr>
WEC8500/configure/router/ospf 2# maximum-area 3
```

10) SPF TIMER (MILLISECONDS) configuration
Configure the SPF TIMER (MILLISECONDS) value.

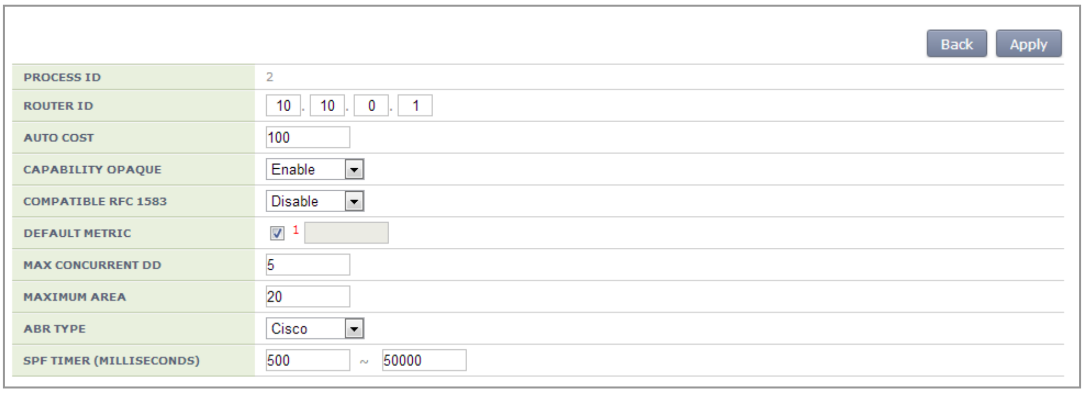
```
WEC8500/configure/router/ospf 2# timers ?
     spf                      OSPF SPF timers
WEC8500/configure/router/ospf 2# timers spf ?
     exp                      Use exponential backoff delays
WEC8500/configure/router/ospf 2# timers spf exp ?
  0 - 2147483647              Minimum Delay between receiving a change
to SPF calculation in
                              milliseconds
WEC8500/configure/router/ospf 2# timers spf exp 3 ?
  0 - 2147483647              Maximum Delay between receiving a change
to SPF calculation in
                              milliseconds
WEC8500/configure/router/ospf 2# timers spf exp 3 100 ?
  <cr>
WEC8500/configure/router/ospf 2# timers spf exp 3 100
```

Configuration using Web UI

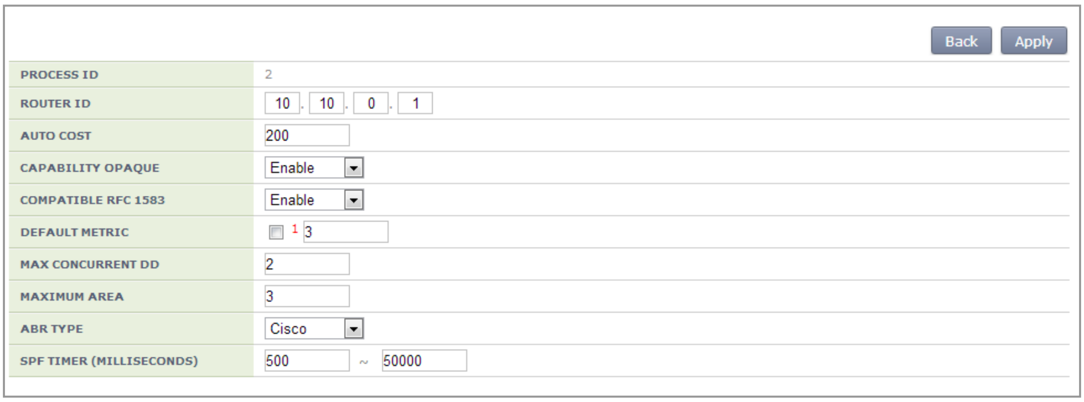
In the menu bar of <**WEC Main window**>, select <**Configuration**> and then select the <**Controller**> → <**Network**> → <**OSPF**> → <**General**> menu in the sub-menus.

Click a PROCESS ID that user wants to configure. The OSPF configuration window is shown below.

Use the value configured in ‘Configuration using CLI’ as a user-defined value in the below screen.



PROCESS ID	2
ROUTER ID	10 . 10 . 0 . 1
AUTO COST	100
CAPABILITY OPAQUE	Enable
COMPATIBLE RFC 1583	Disable
DEFAULT METRIC	☑ 1
MAX CONCURRENT DD	5
MAXIMUM AREA	20
ABR TYPE	Cisco
SPF TIMER (MILLISECONDS)	500 ~ 50000



PROCESS ID	2
ROUTER ID	10 . 10 . 0 . 1
AUTO COST	200
CAPABILITY OPAQUE	Enable
COMPATIBLE RFC 1583	Enable
DEFAULT METRIC	□ 1 3
MAX CONCURRENT DD	2
MAXIMUM AREA	3
ABR TYPE	Cisco
SPF TIMER (MILLISECONDS)	500 ~ 50000

The value configured in ‘Configuration using CLI’ is shown in the below screen.

3.4.5.2 Default Information Configuration of General Settings

Configuration using CLI

1) Detail configuration of OSPF default-information

```
WEC8500/configure/router/ospf 2# default-information ?
  originate                   Distribute a default route
WEC8500/configure/router/ospf 2# default-information originate ?
     always                   Always advertise default route
     metric                   OSPF default metric
     metric-type              OSPF metric type for default routes
     route-map                Route map reference

  <cr>
```

2) Configuration of default-information ALWAYS

```
WEC8500/configure/router/ospf 2# default-information originate ?

     always                   Always advertise default route
     metric                   OSPF default metric
     metric-type              OSPF metric type for default routes
     route-map                Route map reference

  <cr>
WEC8500/configure/router/ospf 2# default-information originate always
?
  <cr>
WEC8500/configure/router/ospf 2# default-information originate always

WEC8500/configure/router/ospf 2#
```

3) Configuration of default-information METRIC
Configure the OSPF metric (0-16777214) value.

```
WEC8500/configure/router/ospf 2# default-information originate metric
?
  0 - 16777214                OSPF metric
WEC8500/configure/router/ospf 2# default-information originate metric
3 ?
  <cr>
WEC8500/configure/router/ospf 2# default-information originate metric
3
WEC8500/configure/router/ospf 2#
```

4) Configuration of default-information METRIC-TYPE
Configure the OSPF metric-type (1/2) value.

```
WEC8500/configure/router/ospf 2# default-information originate metric-
type ?
  1                              Set OSPF External Type 1 metrics
  2                              Set OSPF External Type 2 metrics
WEC8500/configure/router/ospf 2# default-information originate metric-
type 1 ?
  <cr>
```

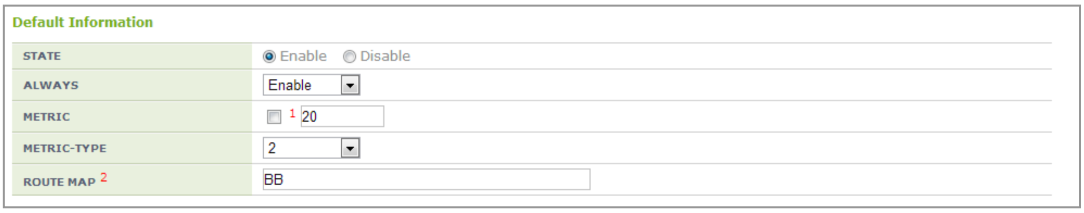
5) Configuration of default-information ROUTE MAP
Enter the name of pointer to route-map entries.

```
WEC8500/configure/router/ospf 2# default-information originate route-
map ?
  <WORD>                         Pointer to route-map entries
WEC8500/configure/router/ospf 2# default-information originate route-
map AA

WEC8500/configure/router/ospf 2#
```

Configuration using Web UI

In the menu bar of <**WEC Main window**>, select <**Configuration**> and then select the <**Controller**> → <**Network**> → <**OSPF**> → <**General**> menu in the sub-menus.

Click a PROCESS ID that user wants to configure. The OSPF configuration window is shown below.
Use the value configured in ‘Configuration using CLI’ as a user-defined value in the below screen.



Default Information

STATE	● Enable ○ Disable
ALWAYS	Enable
METRIC	□ [1] 20
METRIC-TYPE	2
ROUTE MAP [2]	BB

3.4.5.3 Distance Configuration of General Settings

Configuration using CLI

1) Detail configuration of OSPF distance

```
WEC8500/configure/router/ospf 2# distance ?

     admin                         OSPF Administrative distance
     ospf                          OSPF Distance
```

2) Distance admin configuration
Enter the OSPF Admin distance value.

```
WEC8500/configure/router/ospf 2# distance ?

     admin                         OSPF Administrative distance
     ospf                          OSPF Distance

WEC8500/configure/router/ospf 2# distance admin ?
  1 - 255                         OSPF Administrative distance

WEC8500/configure/router/ospf 2# distance admin 100
```

The OSPF Admin distance is displayed as GENERAL in the Web UI.

3) Configuration of EXTERNAL distance ospf
Enter the OSPF EXTERNAL distance value.

```
WEC8500/configure/router/ospf 2# distance ospf ?
  external                     External routes
  inter-area                   Inter-area routes
  intra-area                   Intra-area routes
WEC8500/configure/router/ospf 2# distance ospf external ?
  1 - 255                      <1-255> Distance for external/inter-
area/intra-area routes
WEC8500/configure/router/ospf 2# distance ospf external 50
WEC8500/configure/router/ospf 2#
```

4) Configuration of INTER-AREA distance ospf
Enter the OSPF INTER-AREA distance value.

```
WEC8500/configure/router/ospf 2# distance ospf inter-area ?
  1 - 255                     <1-255> Distance for external/inter-
area/intra-area routes

WEC8500/configure/router/ospf 2# distance ospf inter-area 50 ?
  <cr>
WEC8500/configure/router/ospf 2# distance ospf inter-area 50

WEC8500/configure/router/ospf 2#
```

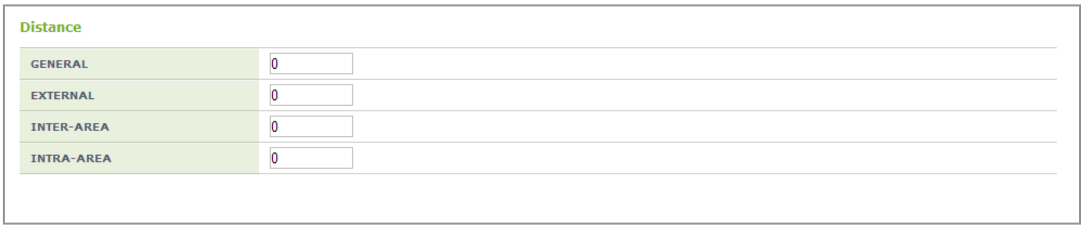
5) Configuration of INTRA-AREA distance ospf
Enter the OSPF INTRA-AREA distance value.

```
WEC8500/configure/router/ospf 2# distance ospf intra-area ?
  1 - 255                     <1-255> Distance for external/inter-
area/intra-area routes

WEC8500/configure/router/ospf 2# distance ospf intra-area 50 ?
  <cr>
WEC8500/configure/router/ospf 2# distance ospf intra-area 50

WEC8500/configure/router/ospf 2#
```

Configuration using Web UI

In the menu bar of **<WEC Main window>**, select **<Configuration>** and then select the **<Controller>** → **<Network>** → **<OSPF>** → **<General>** menu in the sub-menus.

Click a PROCESS ID that user wants to configure. The OSPF configuration window is shown below.
Use the value configured in ‘Configuration using CLI’ as a user-defined value in the below screen.



Distance

GENERAL	0
EXTERNAL	0
INTER-AREA	0
INTRA-AREA	0

3.4.5.4 Overflow Configuration of General Settings

Configuration using CLI

1) Detail configuration of OSPF overflow

```
WEC8500/configure/router/ospf 2# overflow ?

     database                     Database

WEC8500/configure/router/ospf 2# overflow database ?
  external                        External link states
  0 - 4294967294                  Maximum number of LSAs

WEC8500/configure/router/ospf 2# overflow database
```

2) Overflow external configuration
Enter the maximum number of LSAs and time to recover (0 not recover) value.

```
WEC8500/configure/router/ospf 2# overflow ?

     database                     Database

WEC8500/configure/router/ospf 2# overflow database ?
  external                        External link states
  0 - 4294967294                  Maximum number of LSAs

WEC8500/configure/router/ospf 2# overflow database external ?
  0 - 2147483647                  Maximum number of LSAs

WEC8500/configure/router/ospf 2# overflow database external 3 ?
  0 - 65535                       Time to recover (0 not recover)

WEC8500/configure/router/ospf 2# overflow database external 3 10 ?
  <cr>
WEC8500/configure/router/ospf 2# overflow database external 3 10
```

3) Configuration of maximum number of LSAs
Enter the maximum number of LSAs and hard limit value.

```
WEC8500/configure/router/ospf 2# overflow ?

     database                     Database

WEC8500/configure/router/ospf 2# overflow database ?
  external                        External link states
  0 - 4294967294                  Maximum number of LSAs
```

```
WEC8500/configure/router/ospf 2# overflow database 100 ?
  hard                          Hard limit; Instance will be shutdown if
exceed
  soft                          Soft limit; Warning will be given if
exceed
  <cr>
WEC8500/configure/router/ospf 2# overflow database 100 hard ?
  <cr>
WEC8500/configure/router/ospf 2# overflow database 100 hard
```

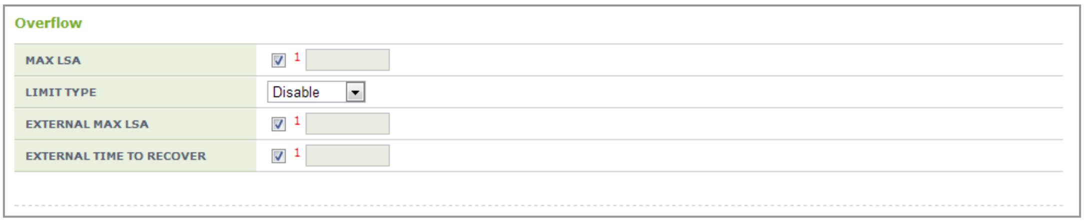
Enter the maximum number of LSAs and soft limit value.

```
WEC8500/configure/router/ospf 2# overflow ?

     database                   Database

WEC8500/configure/router/ospf 2# overflow database ?
  external                      External link states
  0 - 4294967294                Maximum number of LSAs

WEC8500/configure/router/ospf 2# overflow database 100 ?
  hard                          Hard limit; Instance will be shutdown if
exceed
  soft                          Soft limit; Warning will be given if
exceed
  <cr>
WEC8500/configure/router/ospf 2# overflow database 100 soft ?
  <cr>
WEC8500/configure/router/ospf 2# overflow database 100 soft
```

Configuration using Web UI

In the menu bar of <**WEC Main window**>, select <**Configuration**> and then select the <**Controller**> → <**Network**> → <**OSPF**> → <**General**> menu in the sub-menus.

Click a PROCESS ID that user wants to configure. The OSPF configuration window is shown below.
Use the value configured in ‘Configuration using CLI’ as a user-defined value in the below screen.



Overflow

MAX LSA	☑ 1
LIMIT TYPE	Disable ▾
EXTERNAL MAX LSA	☑ 1
EXTERNAL TIME TO RECOVER	☑ 1

3.4.5.5 Network Configuration

Configuration using CLI

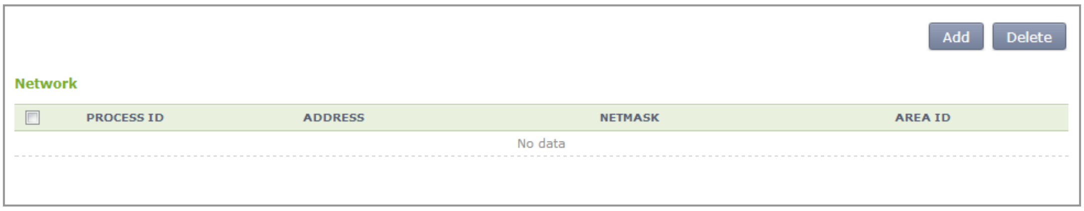
Go to configure → ospf configuration mode of CLI.

```
WEC8500/configure/router/ospf 2# ?

     area                         OSPF area parameters
     auto-cost                    Calculate OSPF interface cost according
to bandwidth
     capability                   Enable specific OSPF feature
     compatible                   OSPF compatibility list
     default-information          Control distribution of default
information
     default-metric               Set metric of redistributed routes
     distance                     Define an administrative distance
     distribute-list              Filter networks in routing updates
     exit                         Exit from router mode
     host                         OSPF stub host entry
     max-concurrent-dd            Maximum number allowed to process DD
concurrently
     maximum-area                 Maximum number of ospf area
     neighbor                     Specify a neighbor router
     network                      Enable routing on an IP network
     ospf                         OSPF specific commands
     overflow                     Control overflow
     passive-interface            Suppress routing updates on an interface
     redistribute                 Redistribute information from another
routing protocol
     router-id                    Router-id for the OSPF process
     summary-address              Configure IP address summaries
     timers                       Adjust routing timers

WEC8500/configure/router/ospf 2# network ?
  A.B.C.D                         Network number
  A.B.C.D/M                       OSPF network prefix
```

Configuration using Web UI

In the menu bar of <WEC Main window>, select <Configuration> and then select the <Controller> → <Network> → <OSPF> → <Network> menu in the sub-menus.

The OSPF initial window is shown below.



Network

□	PROCESS ID	ADDRESS	NETMASK	AREA ID
		No data		

3.4.5.6 Configuration of Network Details

Configuration using CLI

1) Go to configure → ospf configuration mode of CLI.

```
WEC8500# configure terminal
WEC8500/configure# router ospf
WEC8500/configure# router ospf ?
  1 - 10                      OSPF process ID
```

2) Network configuration
   Configure the ADDRESS, NETMASK, and AREA ID of a user-defined network.

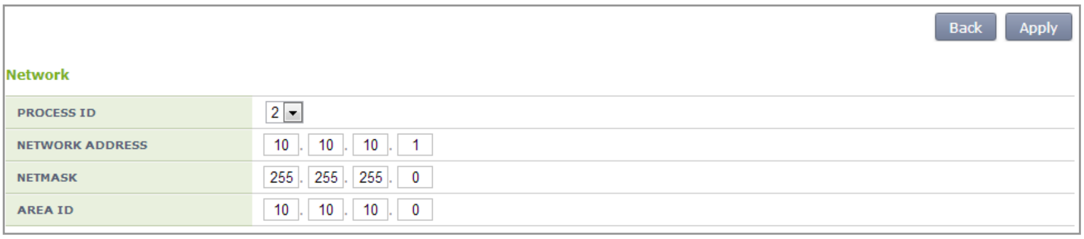
```
WEC8500/configure/router/ospf 2# network ?
  A.B.C.D                     Network number
  A.B.C.D/M                   OSPF network prefix
WEC8500/configure/router/ospf 2# network 100.100.100.1 ?
  A.B.C.D                     OSPF wild card bits(network mask)
WEC8500/configure/router/ospf 2# network 100.100.100.1 255.255.255.0 ?

     area                     Set the OSPF area ID

WEC8500/configure/router/ospf 2# network 100.100.100.1 255.255.255.0 ?

     area                     Set the OSPF area ID

WEC8500/configure/router/ospf 2# network 100.100.100.1 255.255.255.0
area ?
  0 - 4294967295              OSPF area ID as a decimal value

  A.B.C.D                     OSPF area ID in IP address format
WEC8500/configure/router/ospf 2# network 100.100.100.1 255.255.255.0
area 3  ?
  <cr>
WEC8500/configure/router/ospf 2# network 100.100.100.1 255.255.255.0
area 3
```

Parameter	Description
NETWORK ADDRESS	Network number OSPF network prefix
NETMASK	OSPF wild card bits (network mask)
AREA ID	OSPF area ID as a decimal value/ OSPF area ID in IP address format

Configuration using Web UI

In the menu bar of <**WEC Main window**>, select <**Configuration**> and then select the <**Controller**> → <**Network**> → <**OSPF**> → <**Network**> menu in the sub-menus.

Enter the NETWORK ADDRESS, NETMASK, and AREA ID and click the <**Apply**> button.



Network

PROCESS ID	2
NETWORK ADDRESS	10 . 10 . 10 . 1
NETMASK	255 . 255 . 255 . 0
AREA ID	10 . 10 . 10 . 0

3.4.5.7 Redistribute Configuration

Configuration using CLI

Go to configure → ospf configuration mode of CLI.

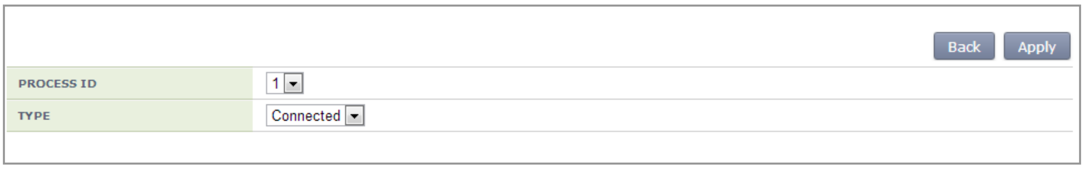
```
WEC8500/configure/router/ospf 2# ?

     area                     OSPF area parameters
     auto-cost                Calculate OSPF interface cost according
to bandwidth
     capability               Enable specific OSPF feature
     compatible               OSPF compatibility list
     default-information      Control distribution of default
information
     default-metric           Set metric of redistributed routes
     distance                 Define an administrative distance
     distribute-list          Filter networks in routing updates
     exit                     Exit from router mode
     host                     OSPF stub host entry
     max-concurrent-dd         Maximum number allowed to process DD
concurrently
     maximum-area             Maximum number of ospf area
     neighbor                 Specify a neighbor router
     network                  Enable routing on an IP network
     ospf                     OSPF specific commands
     overflow                 Control overflow
     passive-interface        Suppress routing updates on an interface
     redistribute             Redistribute information from another
routing protocol
     router-id                Router-id for the OSPF process
     summary-address          Configure IP address summaries
     timers                   Adjust routing timers
WEC8500/configure/router/ospf 2# redistribute ?
  connected                   Connected
  static                      Static routes
  ospf                        Open Shortest Path First (OSPF)
WEC8500/configure/router/ospf 2# redistribute
```

]

Configuration using Web UI

In the menu bar of **<WEC Main window>**, select **<Configuration>** and then select the **<Controller>** → **<Network>** → **<OSPF>** → **<Redistribute>** menu in the sub-menus.

The OSPF Redistribute initial window is shown below.



PROCESS ID: 1

TYPE: Connected

Configuration using CLI

1) Connected configuration
The metric, metric-type, route-map, tag detail setting and default setting can be configured.

```
WEC8500/configure/router/ospf 2# redistribute ?
  connected                        Connected
  static                           Static routes
  ospf                             Open Shortest Path First (OSPF)
WEC8500/configure/router/ospf 2# redistribute connected ?

      metric                       OSPF default metric
      metric-type                  OSPF metric type for default routes
      route-map                    Route map reference
      tag                        Set tag for routes redistributed into
OSPF
```

2) Metric configuration

```
WEC8500/configure/router/ospf 2# redistribute connected ?

      metric                       OSPF default metric
      metric-type                  OSPF metric type for default routes
      route-map                    Route map reference
      tag                        Set tag for routes redistributed into
OSPF
  <cr>
WEC8500/configure/router/ospf 2# redistribute connected metric ?
  1 - 16777214                     OSPF metric

WEC8500/configure/router/ospf 2# redistribute connected metric 3 ?
  <cr>
WEC8500/configure/router/ospf 2# redistribute connected metric 3
```

Parameter	Description
metric	Enter a value from 1-16777214.

3) Metric-type configuration

```
WEC8500/configure/router/ospf 2# redistribute connected metric-type ?
  1                            Set OSPF External Type 1 metrics
  2                            Set OSPF External Type 2 metrics
WEC8500/configure/router/ospf 2# redistribute connected metric-type 1
?
  <cr>
WEC8500/configure/router/ospf 2# redistribute connected metric-type 1
```

Parameter	Description
metric-type	Select 1 or 2.

4) Route-map configuration

```
WEC8500/configure/router/ospf 2# redistribute connected route-map ?
  <WORD>                       Pointer to route-map entries
WEC8500/configure/router/ospf 2# redistribute connected route-map a ?
  <cr>
WEC8500/configure/router/ospf 2# redistribute connected route-map a
```

Parameter	Description
route-map entries	Enter <WORD>.

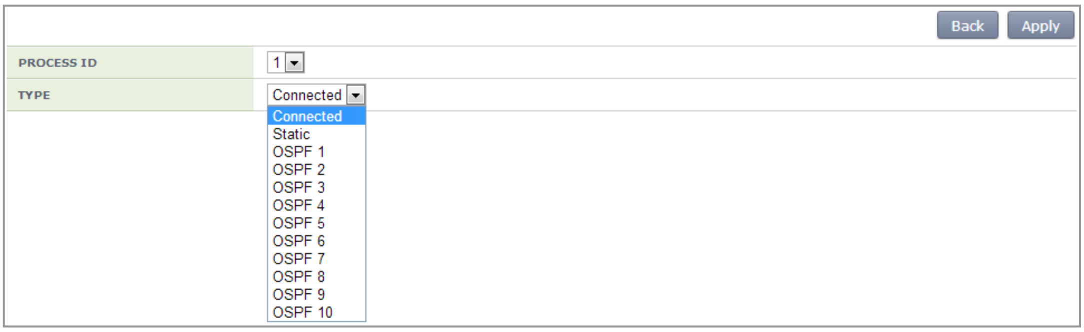
5) Tag configuration

```
WEC8500/configure/router/ospf 2# redistribute connected tag ?
  0 - 4294967295               32-bit tag value

WEC8500/configure/router/ospf 2# redistribute connected tag 3 ?
  <cr>
WEC8500/configure/router/ospf 2# redistribute connected tag 3
```

Parameter	Description
Tag value	Enter a tag value from 0-4294967295.

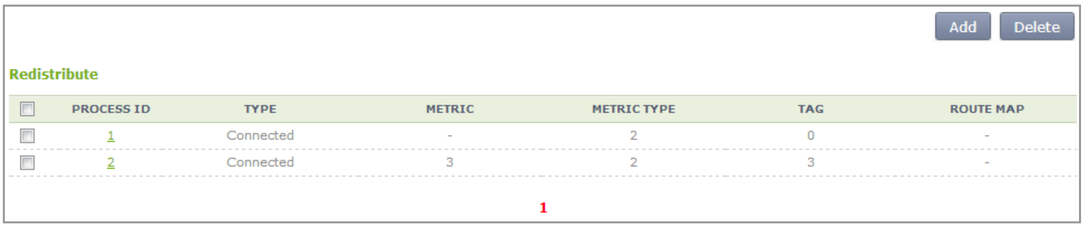
Configuration using Web UI

In the menu bar of <**WEC Main window**>, select <**Configuration**> and then select the <**Controller**> → <**Network**> → <**OSPF**> → <**Redistribute**> menu in the sub-menus.



PROCESS ID	1
TYPE	Connected

After configuring Redistribute default, select a PROCESS ID for detail configuration.

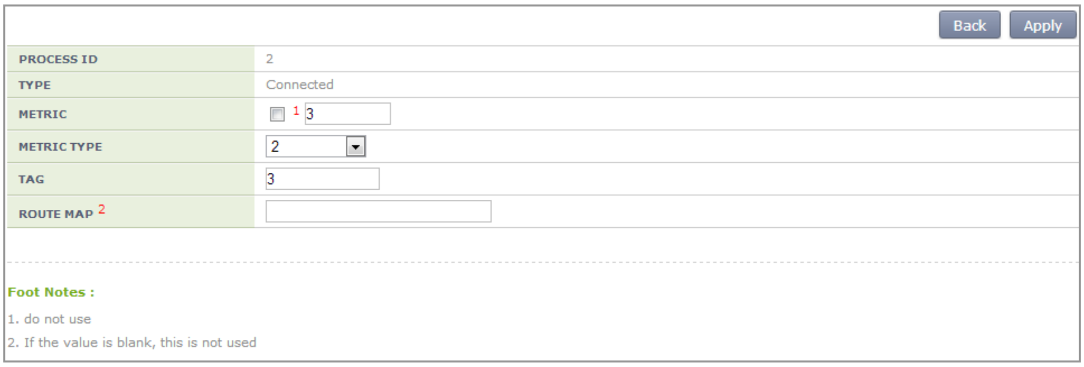


Redistribute

□	PROCESS ID	TYPE	METRIC	METRIC TYPE	TAG	ROUTE MAP
□	1	Connected	-	2	0	-
□	2	Connected	3	2	3	-

Configuring Redistribute details

Configure the details of metric, metric-type, route-map, or tag, etc. which is configured in CLI.



PROCESS ID	2
TYPE	Connected
METRIC	□ [1] 3
METRIC TYPE	2
TAG	3
ROUTE MAP [2]	

Foot Notes :

1. do not use
2. If the value is blank, this is not used

3.4.5.8 AREA Configuration

The Area configuration includes Stub, Not So Stubby Areas (NSSA), Virtual-Link, Range, or Detail.

1) Stub configuration

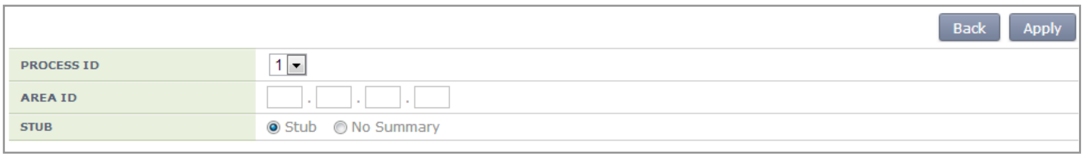
Configuration using CLI

```
WEC8500/configure/router/ospf 2# area 1 stub ?
  no-summary                     Do not inject inter-area routes into
stub
  <cr>
WEC8500/configure/router/ospf 2# area 1 stub no-summary ?
  <cr>
WEC8500/configure/router/ospf 2# area 1 stub no-summary
```

Parameter	Description
no-summary	Select Stub or No Summary.

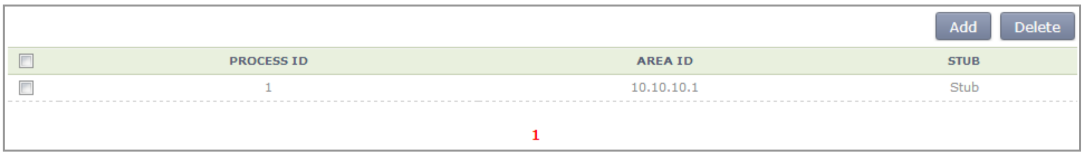
Configuration using Web UI

In the menu bar of **<WEC Main window>**, select **<Configuration>** and then select the **<Controller>** → **<Network>** → **<OSPF>** → **<Area>** → **<Stub>** menu in the sub-menus.



PROCESS ID	1
AREA ID	. . .
STUB	● Stub ○ No Summary

In the Stub add page, configure the details and click the **<Apply>** button. Then, the initial window is changed as shown below.



□	PROCESS ID	AREA ID	STUB
□	1	10.10.10.1	Stub

1

2) NSSA configuration

Configuration using CLI

```
WEC8500/configure/router/ospf 2# area 1 nssa ?

     default-information-originate Originate Type 7 default into NSSA
area
     no-redistribution        No redistribution into this NSSA area
     no-summary               Do not send summary LSA into NSSA
     translator-role          NSSA-ABR Translator role

  <cr>
```

default-information-originate configuration CLI of NSSA

The metric, metric-type, no-redistribution, no-summary, or translator-role details can be configured.

```
WEC8500/configure/router/ospf 1# area 2 nssa default-information-
originate ?

     metric                   OSPF default metric
     metric-type              OSPF metric type for default routes
     no-redistribution        No redistribution into this NSSA area
     no-summary               Do not send summary LSA into NSSA
     translator-role          NSSA-ABR Translator role

  <cr>
```

Metric configuration of NSSA default-information-originate

```
WEC8500/configure/router/ospf 1# area 2 nssa default-information-
originate metric ?
  0 - 16777214                OSPF metric

WEC8500/configure/router/ospf 1# area 2 nssa default-information-
originate metric 3

WEC8500/configure/router/ospf 1#
```

Parameter	Description
OSPF metric	Enter a value from 0-16777214.

Metric-type configuration of NSSA default-information-originate

```
WEC8500/configure/router/ospf 1# area 2 nssa default-information-
originate metric-type ?
  1 - 2                         OSPF Link State type

WEC8500/configure/router/ospf 1# area 2 nssa default-information-
originate metric-type 2

WEC8500/configure/router/ospf 1#
```

Parameter	Description
OSPF metric-type	Select 1 or 2.

Configuring no-redistribution of NSSA default-information-originate

```
WEC8500/configure/router/ospf 1# area 2 nssa default-information-
originate ?
     metric                     OSPF default metric
     metric-type                OSPF metric type for default routes
     no-redistribution          No redistribution into this NSSA area
     no-summary                 Do not send summary LSA into NSSA
     translator-role            NSSA-ABR Translator role
  <cr>
WEC8500/configure/router/ospf 1# area 2 nssa default-information-
originate no-redistribution ?
  <cr>
WEC8500/configure/router/ospf 1# area 2 nssa default-information-
originate no-redistribution
```

Parameter	Description
no-redistribution	Enable/Disable Configuration

Configuring no-summary NSSA default-information-originate

```
WEC8500/configure/router/ospf 1# area 2 nssa default-information-
originate no-summary ?
  <cr>
WEC8500/configure/router/ospf 1# area 2 nssa default-information-
originate no-summary

WEC8500/configure/router/ospf 1#
```

Parameter	Description
no-summary	Enable/Disable Configuration

Configuring translator-role of NSSA default-information-originate

```
WEC8500/configure/router/ospf 1# area 2 nssa default-information-
originate translator-role ?
  always                            Translate always
  candidate                         Candidate for translator (default)
  never                             Do not translate
WEC8500/configure/router/ospf 1# area 2 nssa default-information-
originate translator-role always ?
  no-redistribution                 No redistribution into this NSSA area
  no-summary                        Do not send summary LSA into NSSA
  <cr>
WEC8500/configure/router/ospf 1# area 2 nssa default-information-
originate translator-role candidate ?
  no-redistribution                 No redistribution into this NSSA area
  no-summary                        Do not send summary LSA into NSSA
  <cr>
WEC8500/configure/router/ospf 1# area 2 nssa default-information-
originate translator-role never ?
  no-redistribution                 No redistribution into this NSSA area
  no-summary                        Do not send summary LSA into NSSA
  <cr>
WEC8500/configure/router/ospf 1# area 2 nssa default-information-
originate translator-role never
```

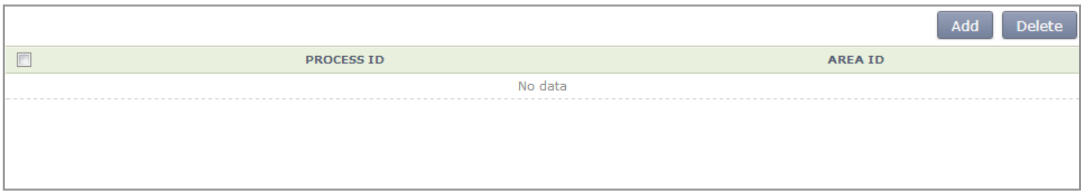
Parameter	Description
always	Translate always
candidate	Candidate for translator (default)
never	Do not translate

After the configuration of each parameter is finished, enable or disable the no-redistribution or no-summary parameter.

Configuration using Web UI

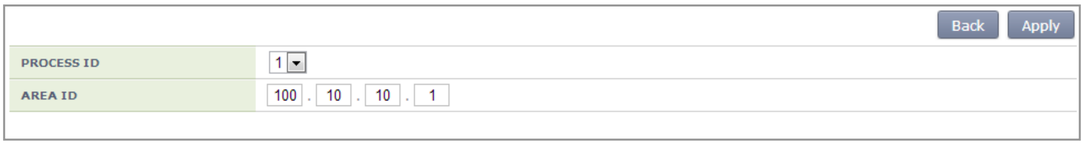
In the menu bar of **<WEC Main window>**, select **<Configuration>** and then select the **<Controller>** → **<Network>** → **<OSPF>** → **<Area>** → **<NSSA>** menu in the sub-menus.

The default window is shown below.



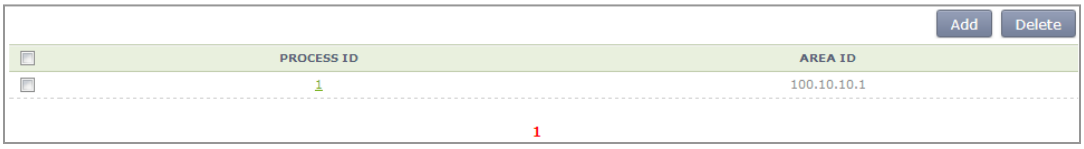
□	PROCESS ID	AREA ID
No data		

The default configuration screen is shown below.



PROCESS ID	1
AREA ID	100 . 10 . 10 . 1

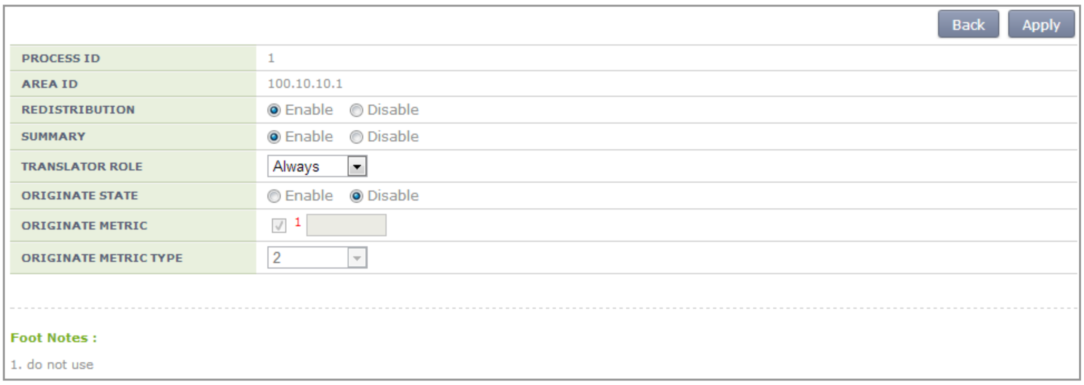
The NSSA window screen is shown as below after detail configuration is completed.



□	PROCESS ID	AREA ID
□	1	100.10.10.1

1

If you select a Process ID after NSSA default configuration, operator can do detail configuration.



PROCESS ID	1
AREA ID	100.10.10.1
REDISTRIBUTION	● Enable ○ Disable
SUMMARY	● Enable ○ Disable
TRANSLATOR ROLE	Always
ORIGINATE STATE	○ Enable ● Disable
ORIGINATE METRIC	☑ 1
ORIGINATE METRIC TYPE	2

Foot Notes :

1. do not use

3) Virtual-Link configuration

Configuration using CLI

```
WEC8500/configure/router/ospf 1# area 2 ?
     authentication            Enable authentication
     default-cost              Set the summary-default cost of a NSSA
or stub area
     filter-list               Filter networks between OSPF areas
     nssa                      Specify a NSSA area
     range                     Summarize routes matching address/mask
(border routers only)
     shortcut                  Configure the area's shortcutting mode
     stub                      Configure OSPF area as stub
     virtual-link              Define a virtual link and its parameters
WEC8500/configure/router/ospf 1# area 2 virtual-link ?
  A.B.C.D                      ID (IP addr) associated with virtual
link neighbor
WEC8500/configure/router/ospf 1# area 2 virtual-link 10.10.10.1 ?
     authentication            Enable authentication
     authentication-key        Set authentication key
     dead-interval             Dead router detection time
     hello-interval            Hello packet interval
     message-digest-key        Set message digest key
     retransmit-interval       LSA retransmit interval
     transmit-delay            LSA transmission delay
  <cr>
```

To configure the Virtual-Link, enter an ID (router ID of OSPF that is connected via Virtual) and configure the detail items. The detail items include authentication, authentication-key, dead-interval, hello-interval, message-digest-key, retransmit-interval, or transmit-delay, etc.

Authentication configuration

Operator can configure authentication and message-digest.

```
WEC8500/configure/router/ospf 2# area 2 virtual-link 10.10.10.1
authentication ?
  message-digest               Use message-digest authentication
  <cr>
WEC8500/configure/router/ospf 2# area 2 virtual-link 10.10.10.1
authentication message-digest ?
  <cr>
WEC8500/configure/router/ospf 2# area 2 virtual-link 10.10.10.1
authentication message-digest
```

Authentication-key configuration

Enter 8-character word to be used as an authentication key. Use the entered 8-character as an authentication key.

```
WEC8500/configure/router/ospf 2# area 2 virtual-link 10.10.10.1
authentication-key ?
  <WORD>                      Authentication key (8 chars)
WEC8500/configure/router/ospf 2# area 2 virtual-link 10.10.10.1
authentication-key aaaaaaaa

WEC8500/configure/router/ospf 2#
```

Dead-interval configuration

The default value of dead-interval is 4 times of hello-interval. Because the default hello-interval is configured to 10 sec., the dead-interval will be 40 seconds if the hello-interval is not configured. In addition, operator can change it to a value between 1 second and 65535 seconds.

```
WEC8500/configure/router/ospf 2# area 2 virtual-link 10.10.10.1 dead-
interval ?
  1 - 65535                   Seconds
WEC8500/configure/router/ospf 2# area 2 virtual-link 10.10.10.1 dead-
interval 50
WEC8500/configure/router/ospf 2#
```

Hello-interval configuration

The default hello-interval is 10 seconds. In addition, operator can change it to a value between 1 second and 65535 seconds.

```
WEC8500/configure/router/ospf 2# area 2 virtual-link 10.10.10.1 hello-
interval ?
  1 - 65535                   Seconds
WEC8500/configure/router/ospf 2# area 2 virtual-link 10.10.10.1 hello-
interval 50
WEC8500/configure/router/ospf 2#
```

Message-digest-key configuration

The message-digest-key configures a key ID between 1 and 255. After key ID configuration, configure the authentication key by using the md5 algorithm. Operator can enter maximum 16 characters.

When you enter an authentication key, the message-digest-key configuration is completed.

```
WEC8500/configure/router/ospf 2# area 2 virtual-link 10.10.10.1
message-digest-key ?
  1 - 255                     Key ID

WEC8500/configure/router/ospf 2# area 2 virtual-link 10.10.10.1
message-digest-key 2 ?
     md5                      Use MD5 algorithm
```

```
WEC8500/configure/router/ospf 2# area 2 virtual-link 10.10.10.1
message-digest-key 2 md5 ?
  <WORD>                          Authentication key (16 chars)
WEC8500/configure/router/ospf 2# area 2 virtual-link 10.10.10.1
message-digest-key 2 md5 b

WEC8500/configure/router/ospf 2#
```

Retransmit-interval configuration

The default retransmit-interval is 5 seconds. In addition, operator can change it to a value between 1 second and 65535 seconds.

```
WEC8500/configure/router/ospf 2# area 2 virtual-link 10.10.10.1
retransmit-interval ?
  1 - 65535                       Seconds (default: 5)

WEC8500/configure/router/ospf 2# area 2 virtual-link 10.10.10.1
retransmit-interval
```

Transmit-delay configuration

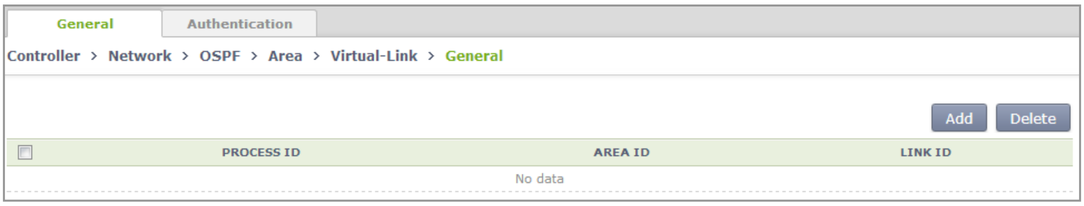
The default transmit-delay is 1 second. In addition, operator can change it to a value between 1 second and 65535 seconds.

```
WEC8500/configure/router/ospf 2# area 2 virtual-link 10.10.10.1
transmit-delay ?
  1 - 65535                       Seconds
WEC8500/configure/router/ospf 2# area 2 virtual-link 10.10.10.1
transmit-delay 5
WEC8500/configure/router/ospf 2#
```

Configuration using Web UI

In the menu bar of **<WEC Main window>**, select **<Configuration>** and then select the **<Controller>** → **<Network>** → **<OSPF>** → **<Area>** → **<Virtual-Link>** menu in the sub-menus.

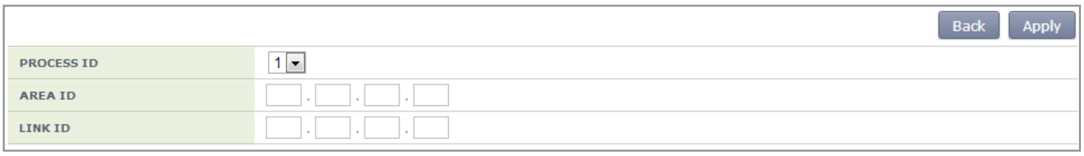
The default window is shown below.



□	PROCESS ID	AREA ID	LINK ID
No data			

Unlike other configurations, there are two tabs at the top; General page and Authentication page.

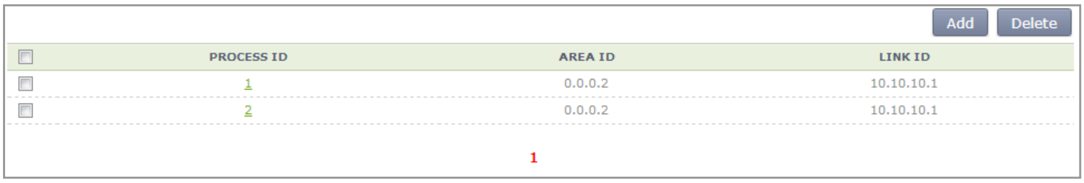
Start configuration in the General page for the basic configuration of Virtual-Link.



PROCESS ID	1
AREA ID	. . .
LINK ID	. . .

In the default configuration page, configure PROCESS ID, AREA ID, or LINK ID.

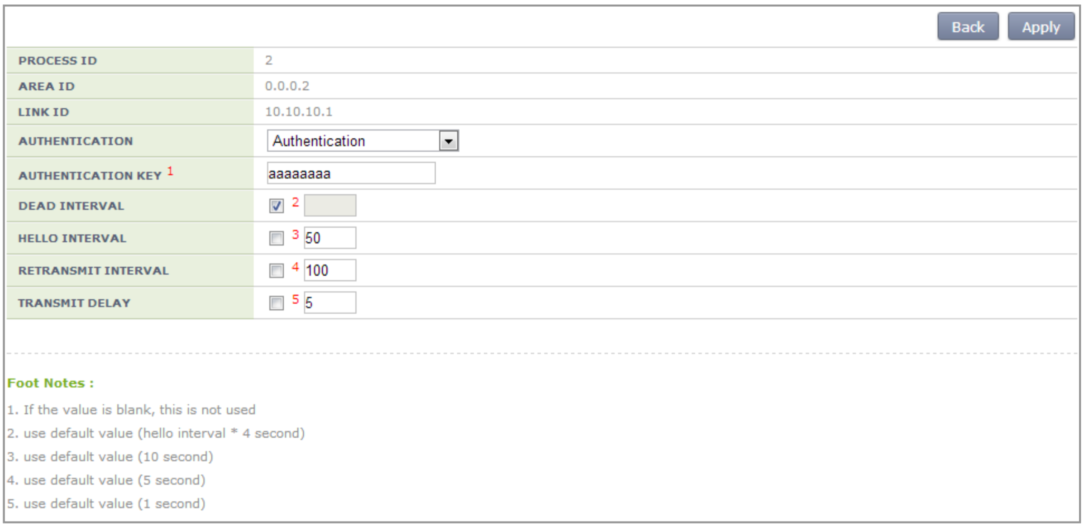
For detail configuration, select a PROCESS ID you want. Operator can do detail configuration for an item you select.



□	PROCESS ID	AREA ID	LINK ID
□	1	0.0.0.2	10.10.10.1
□	2	0.0.0.2	10.10.10.1

1

The detail configuration page is shown below.

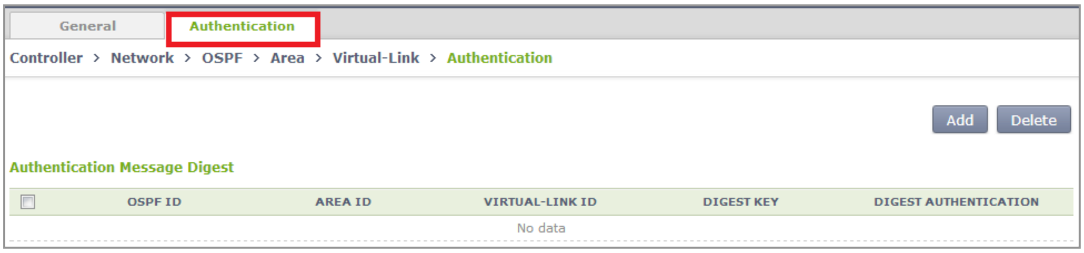


PROCESS ID	2
AREA ID	0.0.0.2
LINK ID	10.10.10.1
AUTHENTICATION	Authentication
AUTHENTICATION KEY [1]	aaaaaaaa
DEAD INTERVAL	☑ [2]
HELLO INTERVAL	□ [3] 50
RETRANSMIT INTERVAL	□ [4] 100
TRANSMIT DELAY	□ [5] 5

Foot Notes :

1. If the value is blank, this is not used
2. use default value (hello interval * 4 second)
3. use default value (10 second)
4. use default value (5 second)
5. use default value (1 second)

The Authentication page of a Virtual-Link is shown below.

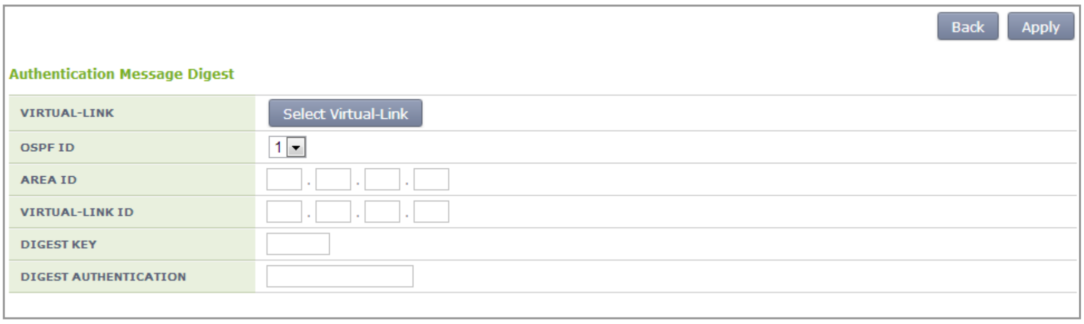


Controller > Network > OSPF > Area > Virtual-Link > Authentication

Authentication Message Digest

□	OSPF ID	AREA ID	VIRTUAL-LINK ID	DIGEST KEY	DIGEST AUTHENTICATION
			No data		

Click the <**Select Virtual-Link**> button.

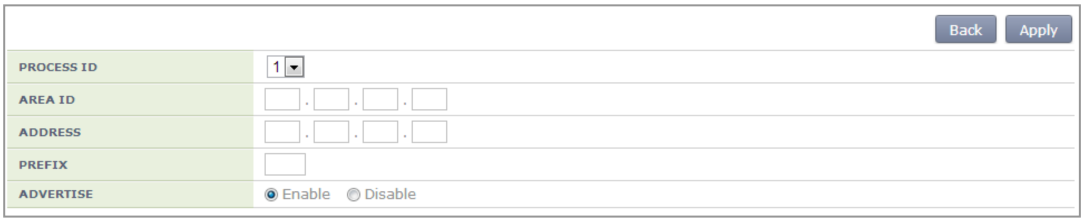


Authentication Message Digest

VIRTUAL-LINK	Select Virtual-Link
OSPF ID	1
AREA ID	. . .
VIRTUAL-LINK ID	. . .
DIGEST KEY	
DIGEST AUTHENTICATION	

Select a PROCESS ID that you have selected in the General page.

And then, configure Digest Key or Digest Authentication.
Just like CLI configuration, select a digest key between 1 and 255 and enter a key whose length is 16-character or less for digest authentication.



PROCESS ID	1
AREA ID	. . .
ADDRESS	. . .
PREFIX	
ADVERTISE	● Enable ○ Disable

4) Range configuration

Configuration using CLI

To configure the Range detail items, start detail configuration after entering an Area range prefix value.

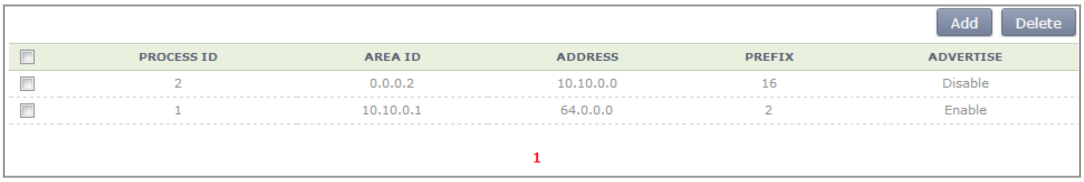
```
WEC8500/configure/router/ospf 2# area 2 range ?
  A.B.C.D/M                    Area range prefix
WEC8500/configure/router/ospf 2# area 2 range 10.10.10.1/16 ?
  advertise                    Advertise this range (default)
  not-advertise                DoNotAdvertise this range
  <cr>
WEC8500/configure/router/ospf 2# area 2 range 10.10.10.1/16
```

The detail items include advertise or no-advertise configuration
Configure whether to advertise to the range or not.

Configuration using Web UI

In the menu bar of **<WEC Main window>**, select **<Configuration>** and then select the **<Controller>** → **<Network>** → **<OSPF>** → **<Area>** → **<Range>** menu in the sub-menus.

The configuration page is as follows:



☐	PROCESS ID	AREA ID	ADDRESS	PREFIX	ADVERTISE
☐	2	0.0.0.2	10.10.0.0	16	Disable
☐	1	10.10.0.1	64.0.0.0	2	Enable

5) Detail configuration

Configuration using CLI

This is additional explanations for Area. Operator can configure authentication, default-cost, or shortcut.

```
WEC8500/configure/router/ospf 2# area 2 ?
     authentication            Enable authentication
     default-cost              Set the summary-default cost of a NSSA
or stub area
     filter-list               Filter networks between OSPF areas
     nssa                      Specify a NSSA area
     range                     Summarize routes matching address/mask
(border routers only)
     shortcut                  Configure the area's shortcutting mode
     stub                      Configure OSPF area as stub
     virtual-link              Define a virtual link and its parameters
```

Authentication configuration

Operator can select whether to use authentication or message-digest function.

```
WEC8500/configure/router/ospf 2# area 2 authentication ?
  message-digest                Use message-digest authentication
  <cr>
WEC8500/configure/router/ospf 2# area 2 authentication message-digest
?
  <cr>
WEC8500/configure/router/ospf 2# area 2 authentication message-digest
```

Default-cost configuration

Configure a value between 0 and 1677215 as a default-cost. However, operator can configure the default-cost value in AREA ID whether a stub or NSSA is configured.
If you try to configure the default-cost in an ID where neither the two items are configured, the following error phrase is displayed.
'% The area is neither stub, nor NSSA'

```
WEC8500/configure/router/ospf 2# area 0.0.0.1 default-cost ?
  0 - 16777215                  Stub's advertised default summary cost
WEC8500/configure/router/ospf 2# area 0.0.0.1 default-cost 3 ?
  <cr>
WEC8500/configure/router/ospf 2# area 0.0.0.1 default-cost 3
```

Shortcut configuration

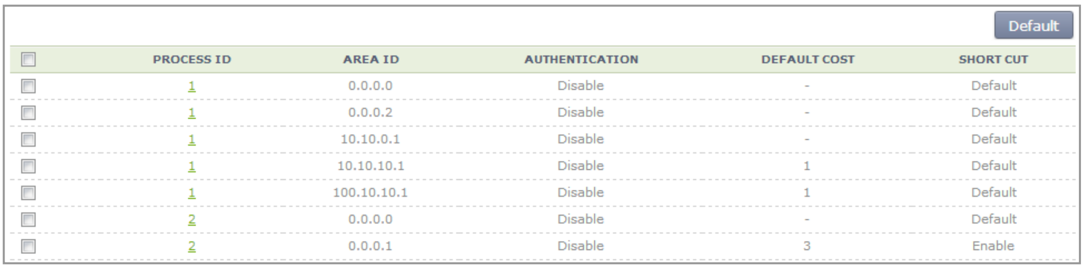
For Shortcut configuration, operator can select one out of 3 selections including default, disable, and enable.

```
WEC8500/configure/router/ospf 2# area 0.0.0.1 shortcut ?
  default                       Set default shortcutting behavior
  disable                       Disable shortcutting through the area
  enable                        Enable shortcutting through the area
WEC8500/configure/router/ospf 2# area 0.0.0.1 shortcut enable

WEC8500/configure/router/ospf 2#
```

Configuration using Web UI

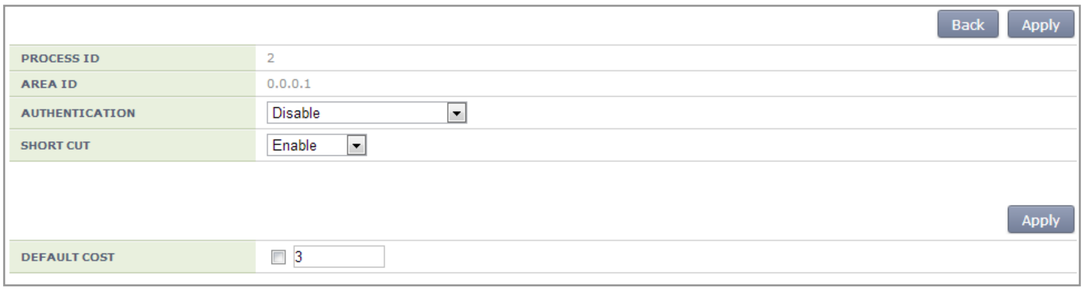
In the menu bar of <**WEC Main window**>, select <**Configuration**> and then select the <**Controller**> → <**Network**> → <**OSPF**> → <**Area**> → <**Detail**> menu in the sub-menus.

The configuration page is as follows:



□	PROCESS ID	AREA ID	AUTHENTICATION	DEFAULT COST	SHORT CUT
□	1	0.0.0.0	Disable	-	Default
□	1	0.0.0.2	Disable	-	Default
□	1	10.10.0.1	Disable	-	Default
□	1	10.10.10.1	Disable	1	Default
□	1	100.10.10.1	Disable	1	Default
□	2	0.0.0.0	Disable	-	Default
□	2	0.0.0.1	Disable	3	Enable

Select a PROCESS ID for detail configuration. As mentioned in the CLI, the Stub or NSSA must be configured to the PROCESS ID in a window where default-cost is selected. If a PROCESS ID without the configuration is completed, the detail configuration can not be performed. Therefore, the below default-cost configuration is available only when the Stub or NSSA is configured to the ID.



PROCESS ID	2
AREA ID	0.0.0.1
AUTHENTICATION	Disable
SHORT CUT	Enable

DEFAULT COST	□ 3

3.4.5.9 Summary Configuration

Configuration using CLI

```
WEC8500/configure/router/ospf 2# summary-address ?
  A.B.C.D/M                         IP summary prefix
WEC8500/configure/router/ospf 2# summary-address 1.1.1.1/16 ?
  not-advertise                     Suppress routes that match the prefix
  tag                               Set tag

  <cr>
WEC8500/configure/router/ospf 2# summary-address 1.1.1.1/16

WEC8500/configure/router/ospf 2#
```

Parameter	Description
summary-address	A.B.C.D/M

Operator can perform detail configuration only when you enter a summary-address. The detail configuration includes advertise or TAG configuration.

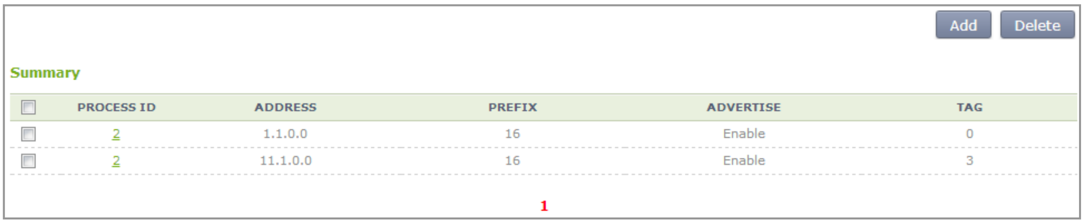
1) Advertise Configuration
   The default is set to Enable. Therefore, if no-advertise is selected in the CLI, the configuration is changed to Disable.
2) Tag
   A tag is a user-defined 32-bit tag value between 0 and 4294967295. A tag also has a default value and it is 0.

```
WEC8500/configure/router/ospf 2# summary-address 11.1.1.1/16

WEC8500/configure/router/ospf 2# summary-address 11.1.1.1/16 tag ?
  0 - 4294967295                    32-bit tag value
WEC8500/configure/router/ospf 2# summary-address 11.1.1.1/16 tag 3
```

Configuration using Web UI

In the menu bar of **<WEC Main window>**, select **<Configuration>** and then select the **<Controller>** → **<Network>** → **<OSPF>** → **<Summary>** menu in the sub-menus.

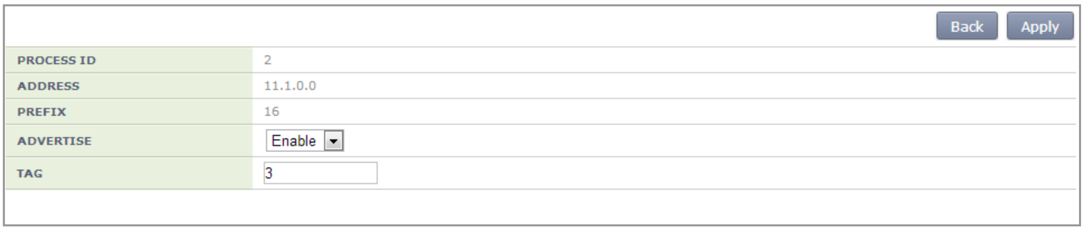
The configuration page is as follows:



Summary

□	PROCESS ID	ADDRESS	PREFIX	ADVERTISE	TAG
□	2	1.1.0.0	16	Enable	0
□	2	11.1.0.0	16	Enable	3

After default configuration, select a PROCESS ID for detail configuration.
The detail configuration includes advertise and TAG configuration mentioned in the CLI.
Unlike CLI, there is no no-advertise. A user can change the default Enable to Disable.



PROCESS ID	2
ADDRESS	11.1.0.0
PREFIX	16
ADVERTISE	Enable
TAG	3

3.4.5.10 Passive Interface Configuration

Configuration using CLI

```
WEC8500/configure/router/ospf 2# passive-interface ?
  <WORD>                           Interface's name
WEC8500/configure/router/ospf 2# passive-interface ge2 ?
  A.B.C.D                          Address of interface
  <cr>
```

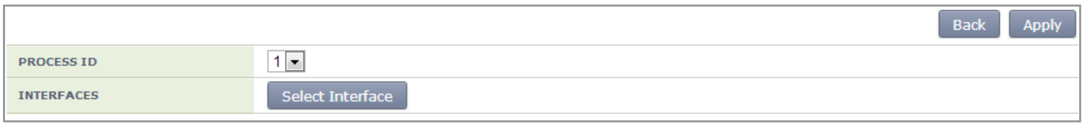
Parameter	Description
Interface Name	Enter the name of an interface to use directly.

A user directly enters an interface name for Passive-interface configuration. Also, a user can enter an address to the interface.

Configuration using Web UI

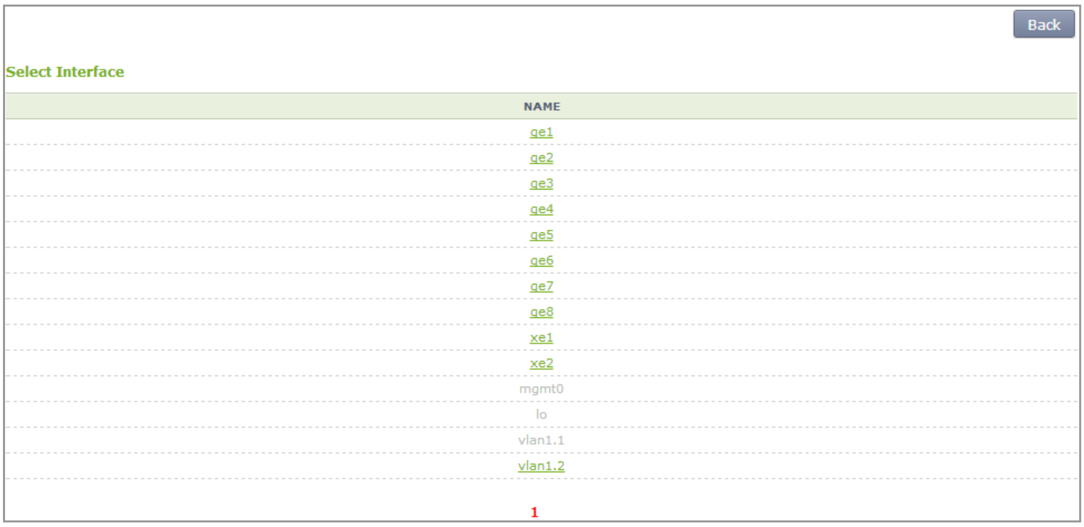
In the menu bar of **<WEC Main window>**, select **<Configuration>** and then select the **<Controller>** → **<Network>** → **<OSPF>** → **<Passive Interface>** menu in the sub-menus.

The configuration page is as follows:



PROCESS ID	1
INTERFACES	Select Interface

After selecting a PROCESS ID that a user will use, select an interface to apply.



NAME
ge1
ge2
ge3
ge4
ge5
ge6
ge7
ge8
xe1
xe2
mgmt0
lo
vlan1.1
vlan1.2

Among the interface items displayed on the screen, configure the interface that a user wants.

3.4.5.11 Interface General Configuration

Configuration using CLI

Unlike other OSPF configurations, the interface general does not enter into the OSPF mode. Perform related configuration at the interface that a user wants. Therefore, the CLI configuration is as follows:

1) Go to configure → interface configuration mode of CLI.

```
WEC8500# configure terminal
WEC8500/configure#
WEC8500/configure# interface ge2
```

2) The items for detail configuration are as follows:

WEC8500/configure/interface ge2# ip ospf ?

```
     address                   Address of interface
     authentication            Enable authentication
     authentication-key        Authentication password (key)
     cost                      Interface cost
     database-filter           Filter OSPF LSA during synchronization
and flooding
     dead-interval             Interval after which a neighbor is
declared dead
     disable                   Disable OSPF
     hello-interval            Time between HELLO packets
     message-digest-key        Message digest authentication password
(key)
     mtu                       OSPF interface MTU
     mtu-ignore                Time between HELLO packets
     network                   Network type
     priority                  Router priority
     retransmit-interval       Time between retransmitting lost link
state advertisements
     transmit-delay            Link state transmit delay
```

DISABLE OSPF configuration

```
WEC8500/configure/interface ge2# ip ospf disable ?
  all                          All functionality
WEC8500/configure/interface ge2# ip ospf disable all ?
  <cr>
WEC8500/configure/interface ge2# ip ospf disable all
```

MTU configuration

The default does not use Maximum Transmission Unit (MTU) configuration.
The range of MTU user configuration is 576-65535.

```
WEC8500/configure/interface ge2# ip ospf mtu ?
  576 - 65535
WEC8500/configure/interface ge2# ip ospf mtu 600
WEC8500/configure/interface ge2#
```

Network Type configuration

The network type includes 4 types, i.e. broadcast, non-broadcast, point-to-point, and point-to-multipoint. The Ethernet is broadcast configuration.

```
WEC8500/configure/interface ge2# ip ospf network ?
  broadcast                    Specify OSPF broadcast multi-access
network
  non-broadcast                Specify OSPF NBMA network
  point-to-point              Specify OSPF point-to-point network
  point-to-multipoint         Specify OSPF point-to-multipoint network
WEC8500/configure/interface ge2# ip ospf network
```

Authentication configuration

This is CLI that selects whether to use user authentication.

```
WEC8500/configure/interface ge2# ip ospf authentication ?
  message-digest              Use message-digest authentication
  null                        Use null authentication
  <cr>
WEC8500/configure/interface ge2# ip ospf authentication message-digest
?
  <cr>
WEC8500/configure/interface ge2# ip ospf authentication null ?
  <cr>
WEC8500/configure/interface ge2# ip ospf authentication null
```

OSPF Cost configuration

Enter a cost value between 1 and 65535.

```
WEC8500/configure/interface ge2# ip ospf cost ?
  1 - 65535                   Cost
WEC8500/configure/interface ge2# ip ospf cost 2 ?
  <cr>
```

DATABASE-FILTER configuration

```
WEC8500/configure/interface ge2# ip ospf database-filter ?
  all                         Filter all LSA
WEC8500/configure/interface ge2# ip ospf database-filter all ?
  out                         Outgoing LSA
WEC8500/configure/interface ge2# ip ospf database-filter all out ?
  <cr>
WEC8500/configure/interface ge2# ip ospf database-filter all out
```

Dead-interval configuration

The default value of dead-interval is 4 times of hello-interval. Because the default hello-interval is configured to 10 sec., the dead-interval will be 40 seconds if the hello-interval is not configured. In addition, operator can change it to a value between 1 second and 65535 seconds.

```
WEC8500/configure/interface ge2# ip ospf dead-interval ?
  1 - 65535                   Seconds
```

```
WEC8500/configure/interface ge2# ip ospf dead-interval 30 ?
  <cr>
WEC8500/configure/interface ge2# ip ospf dead-interval 30
```

Hello-interval configuration

The default hello-interval is 10 seconds. In addition, operator can change it to a value between 1 second and 65535 seconds.

```
WEC8500/configure/interface ge2# ip ospf hello-interval ?
  1 - 65535                   Seconds
WEC8500/configure/interface ge2# ip ospf hello-interval 50 ?
  <cr>
WEC8500/configure/interface ge2# ip ospf hello-interval 50
WEC8500/configure/interface ge2#
```

Retransmit-interval configuration

The default retransmit-interval is 5 seconds. In addition, operator can change it to a value between 1 second and 65535 seconds.

```
WEC8500/configure/interface ge2# ip ospf retransmit-interval ?
  1 - 65535                   Seconds (default: 5)
WEC8500/configure/interface ge2# ip ospf retransmit-interval 100 ?
  <cr>
WEC8500/configure/interface ge2# ip ospf retransmit-interval 100
WEC8500/configure/interface ge2#
```

TRANSMIT DELAY configuration

The default transmit-delay is 1 second. In addition, operator can change it to a value between 1 second and 65535 seconds.

```
WEC8500/configure/interface ge2# ip ospf transmit-delay ?
  1 - 65535                   Seconds
WEC8500/configure/interface ge2# ip ospf transmit-delay 400
WEC8500/configure/interface ge2#
```

MTU IGNORE configuration

The default configuration is Disable. If you configure CLI, it is changed to Enable.

```
WEC8500/configure/interface ge2# ip ospf mtu-ignore ?
  <cr>
WEC8500/configure/interface ge2# ip ospf mtu-ignore
WEC8500/configure/interface ge2#
```

PRIORITY configuration

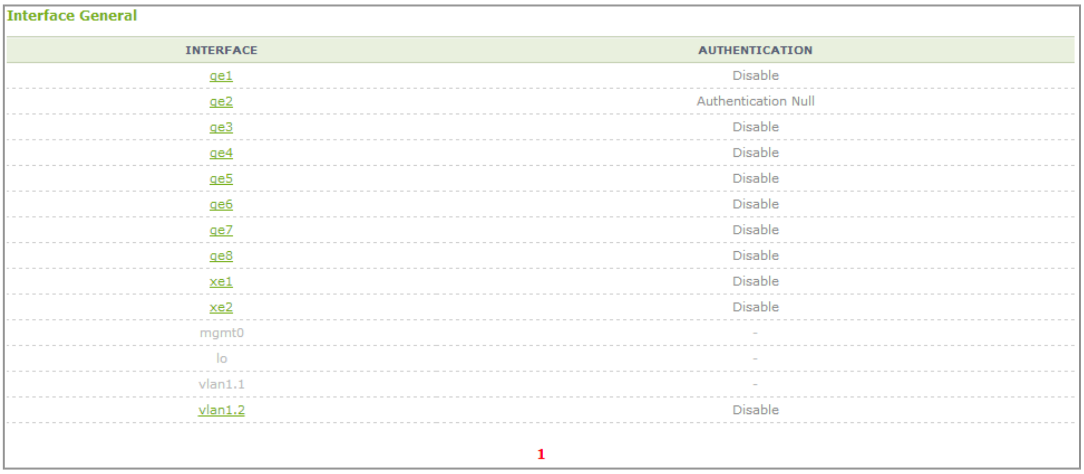
The default OSPF Priority value is 1. A user can configure the priority between 1 and 255.

```
WEC8500/configure/interface ge2# ip ospf priority ?
  0 - 255                          Priority
WEC8500/configure/interface ge2# ip ospf priority 2
```

Configuration using Web UI

In the menu bar of **<WEC Main window>**, select **<Configuration>** and then select the **<Controller>** → **<Network>** → **<OSPF>** → **<Interface General>** menu in the sub-menus.

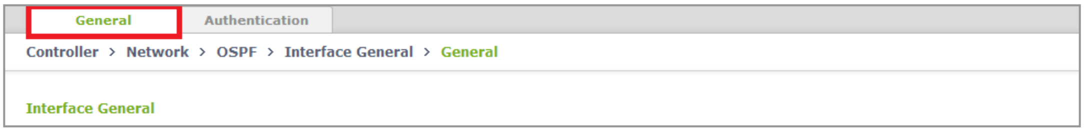
The configuration page is as follows:
As shown in the below figure, the currently enabled interface items are displayed.
When you select an interface for detail configuration, operator can go to the detail item configuration page.
The Interface General item is also divided into General configuration and Authentication window as a tab.



Interface General

INTERFACE	AUTHENTICATION
ge1	Disable
ge2	Authentication Null
ge3	Disable
ge4	Disable
ge5	Disable
ge6	Disable
ge7	Disable
ge8	Disable
xe1	Disable
xe2	Disable
mgmt0	-
lo	-
vlan1.1	-
vlan1.2	Disable

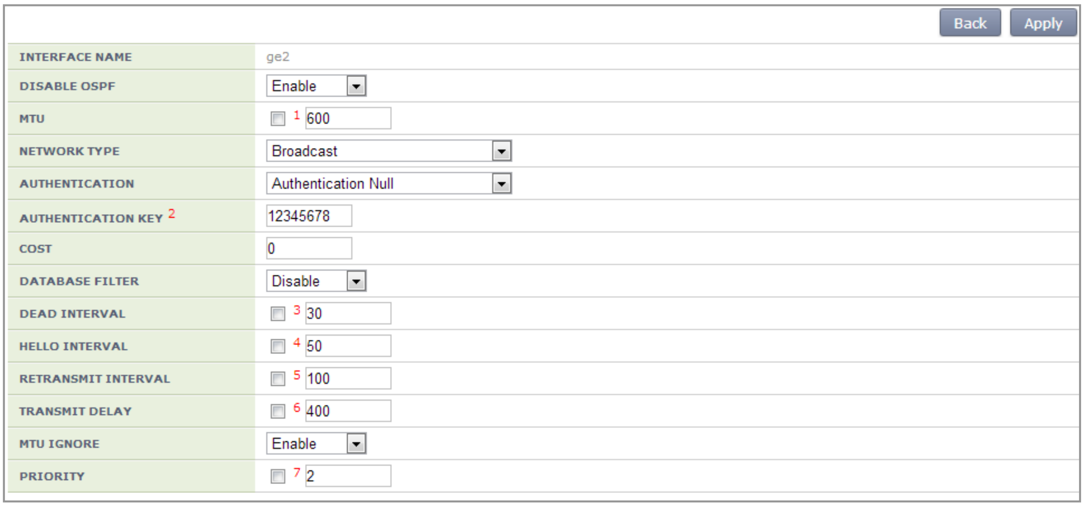
1



The General configuration screen is as follows:

The detail item configuration page is as follows:

When you select the name of an enabled interface, the below detail item configuration page is displayed.



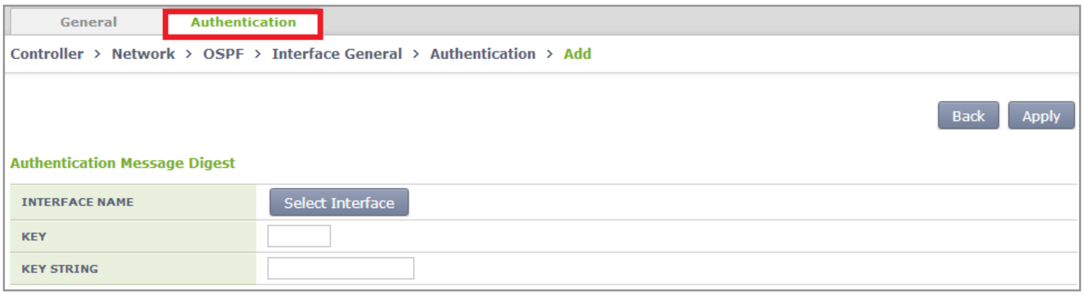
INTERFACE NAME	ge2
DISABLE OSPF	Enable
MTU	□ [1] 600
NETWORK TYPE	Broadcast
AUTHENTICATION	Authentication Null
AUTHENTICATION KEY [2]	12345678
COST	0
DATABASE FILTER	Disable
DEAD INTERVAL	□ [3] 30
HELLO INTERVAL	□ [4] 50
RETRANSMIT INTERVAL	□ [5] 100
TRANSMIT DELAY	□ [6] 400
MTU IGNORE	Enable
PRIORITY	□ [7] 2

After entering a value that a user wants for the item configured in the above CLI, click the <**Apply**> button.

Authentication configuration

Just as General configuration, click the Authentication configuration in the tab.

Then, the page for authentication related detail configuration is displayed as shown below. Select an interface that a user wants to configure, and enter the key string (1-255) of the configuration.

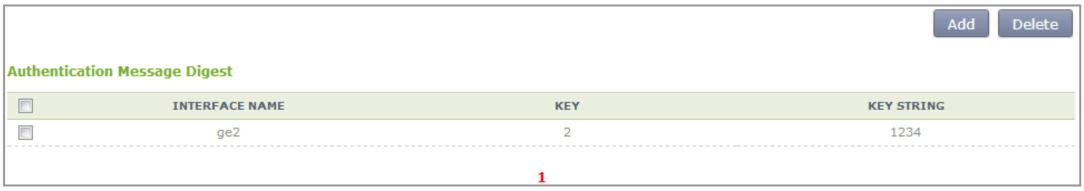


Controller > Network > OSPF > Interface General > Authentication > Add

Authentication Message Digest

INTERFACE NAME	Select Interface
KEY	
KEY STRING	

The verification page after configuration is as follows:



Authentication Message Digest

□	INTERFACE NAME	KEY	KEY STRING
□	ge2	2	1234

3.4.6 VRRP Configuration

The Virtual Router Redundancy Protocol (VRRP) is an Internet protocol that provides the backup router operation method in a LAN. If a fault occurs with a router that transmits a packet from a host in a LAN, decide a virtual IP address in a DHCP manually or by default by using a virtual router fault recovery protocol and share it among routers. Once a primary router and a backup router are decided, the backup router becomes a primary router when a fault occurs with the primary router.

Configuration using CLI

To configure the VRRP related function, go to configure → router mode of CLI, enter a router ID and interface name to go to the VRRP configuration mode.

```
WEC8500# configure terminal
WEC8500/configure# router
WEC8500/configure# router vrrp
WEC8500/configure# router vrrp 1 vlan1.10
WEC8500/configure/router/vrrp#
```

The following commands are provided.

[advertisement-interval]

This command configures the advertisement interval of VRRP in second. A user can configure the interval from 1 to 10.

- advertisement-interval [INTERVAL]

Parameter	Description
INTERVAL	Advertisement interval (range: 1-10 s)

[circuit-failover]

Enter an interface to configure and its priority.

- circuit-failover [WORD] [PRIORITY]

Parameter	Description
WORD	Interface name
PRIORITY	Priority setup (range: 1-100)

[enable/disable]

This command enables or disables the VRRP session.

- enable
- disable

[preempt-delay]

This command configures the preempt delay time.

- preempt-delay [DELAY_TIME]

Parameter	Description
DELAY_TIME	Preempt delay time (range: 0-3600 s)

[preempt-mode]

This command configures whether to use the preempt mode.

- preempt-mode [MODE]

Parameter	Description
MODE	- true: Use the preempt mode - false: Stop using the preempt mode.

[priority]

This command configures a priority.

- priority [PRIORITY]

Parameter	Description
PRIORITY	Priority setup (range: 1-255)

[virtual-ip]

This command configures an IP address to use in the VRRP and configure the IP address as master or backup.

- virtual-ip [A.B.C.D]
- virtual-ip [A.B.C.D] [MODE]

Parameter	Description
A.B.C.D	IP address
MODE	IP configuration mode (backup/master) - backup: Backup router configuration. - master: Master configuration.

[show vrrp]

This command retrieves VRRP configuration.

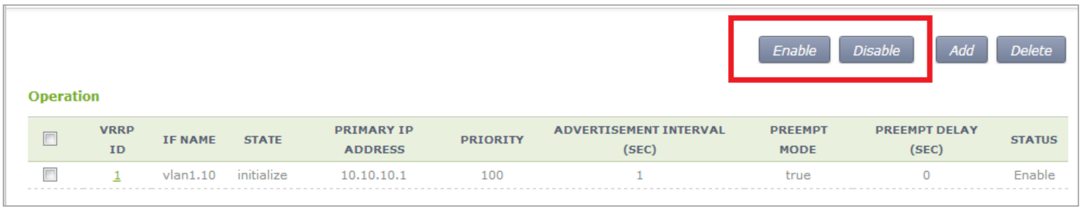
- show vrrp

Configuration using Web UI

In the menu bar of <**WEC Main window**>, select <**Configuration**> and then select the <**Controller**> → <**Network**> → <**VRRP**> menu in the sub-menus.
The VRRP menu provides two sub menus, i.e. Operation and Circuit Failover.

[Operation]

When you click the <**Enable**>/<**Disable**> button, you can Enable or disable VRRP.
In addition, when you click the <**Add**> or <**Delete**> button, you can add or delete VRRP configuration.



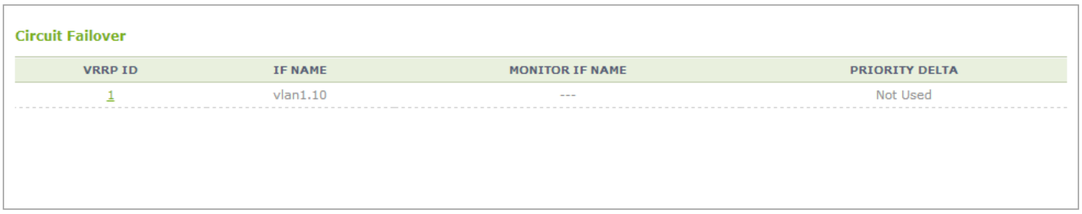
Operation

□	VRRP ID	IF NAME	STATE	PRIMARY IP ADDRESS	PRIORITY	ADVERTISEMENT INTERVAL (SEC)	PREEMPT MODE	PREEMPT DELAY (SEC)	STATUS
□	1	vlan1.10	initialize	10.10.10.1	100	1	true	0	Enable

Figure 33. VRRP-Operation Window

[Circuit Failover]

When you click the Circuit Failover menu, the VRRP list is displayed on the window.

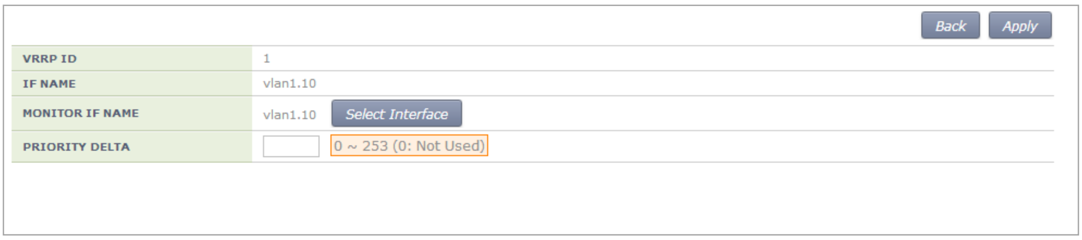


Circuit Failover

VRRP ID	IF NAME	MONITOR IF NAME	PRIORITY DELTA
1	vlan1.10	---	Not Used

Figure 34. VRRP-Circuit Failover Window (1)

To perform detail configuration, select one of VRRP items.
After selecting a configuration you want select the <**Apply**> button to apply the configuration.



VRRP ID	1
IF NAME	vlan1.10
MONITOR IF NAME	vlan1.10
PRIORITY DELTA	0 ~ 253 (0: Not Used)

Figure 35. VRRP-Circuit Failover Window (2)

3.4.7 Configuring IPWATCHD

The IP WATCH Deamon (IPWATCHD) provides the function of detecting active or passive IP collision. Regardless of IP collision attacker or victim, the information including source ip/mac is transmitted as an evm fault event when the IP collision occurs. At the collision time, the Gratuitous Address Resolution Protocol (GARP) reply is transmitted 3 times to the unicast at every 1 second.

It supports the rate-limit function to deal with an intended ARP attack. Although ARP is entered from a host that is not in the same subnet, it generates GARP by recognizing it as a target if the host has the same APC IP.

Configuration using CLI

To configure the IPWATCHD function, enter into the configure mode of CLI.

Configure a TIMEOUT value (that a user wants) to detect an IP address collision.

Operator can enter a value between 10 and 300 seconds.

```
WEC8500# configure terminal
WEC8500/configure#
WEC8500/configure# ipwatch ?
  defend-interval                Ipwatch defend-interval configuration
WEC8500/configure# ipwatch defend-interval ?
  10 - 300                       Ipwatch defend-interval value(seconds)
WEC8500/configure# ipwatch defend-interval 30
```

Parameter	Description
VALUE	Enter a defend-interval (10-300 sec).

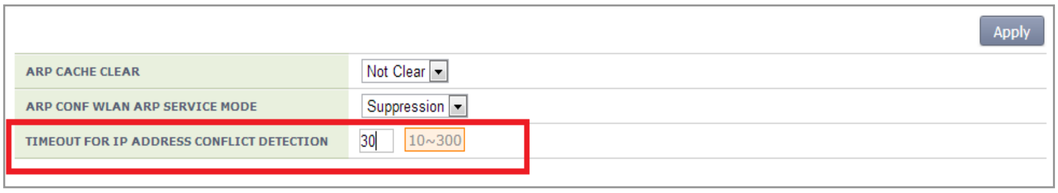
The default TIMEOUT value for IP address collision detection is 30 seconds.

When the time is configured, the IPWATCHD daemon is restarted and a log and GARP is generated if there is an IP collision.

Configuration using Web UI

In the menu bar of **<WEC Main window>**, select **<Configuration>** and then select the **<Controller>** → **<Network>** → **<ARP>** menu in the sub-menus.

After entering a time value (10-300 seconds) that a user wants in the TIMEOUT FOR IP ADDRESS CONFLICT DETECTION window, click the **<Apply>** button. Then, the configuration is applied.



ARP CACHE CLEAR	Not Clear
ARP CONF WLAN ARP SERVICE MODE	Suppression
TIMEOUT FOR IP ADDRESS CONFLICT DETECTION	30 10~300

The default value before user configuration is 30 as shown in the below figure.

Figure 36. IPWATCHD Configuration Window

3.5 QoS

The Access Control List (ACL) allows or blocks a specific network traffic based on an operator's configuration. The APC provides QoS using ACL.

3.5.1 ACL Configuration

3.5.1.1 Access List Configuration

You can create or delete an access list for ACL configuration. To delete an access list, an operator can enter the name of an access list directly or enter a command by copying a value retrieved from the 'show running-config network'. But, if the access list is being used in the WLAN ACL or Admin ACL, etc., you cannot delete it. Therefore, check if it is being used in the WLAN ACL or Admin ACL first of all.

Configuration using CLI

1) Go to fqm mode where you can configure the configure → rule of CLI.

```
APC# configure terminal
APC/configure# fqm-mode
```

2) Create an access list by entering the 'access-list' command. The 'no' parameter is used to delete an access list.
   - access-list [ip/ipv6/mac] [ACL_NAME] [deny/permit/time-profile] seq [seq_NUM] [1/*/ahp/eigrp/esp/gre/icmp/igmp/igrp/ip/nos/ospf/pcp/pim/17/6/tcp/udp/1-255] [any/A.B.C.D A.B.C.D] eq [eq_VALUE] [any/A.B.C.D A.B.C.D] eq [eq_VALUE] [[[dscp [*|[0-63]]|precedence [*|[0-7])]]]|]

   An example of entering a command is shown below.
   - Creating Access list 'acl1':

```
APC# configure terminal
APC/configure# fqm-mode
APC/configure# access-list ip acl1 permit seq 1 icmp any any
```

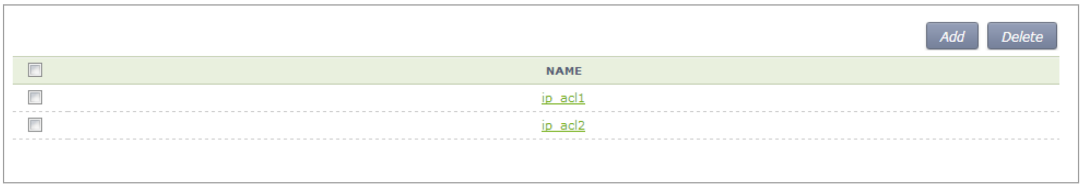
   - Deleting Access list 'acl1':

```
APC# configure terminal
APC/configure# fqm-mode
APC/configure# no access-list ip acl1 permit seq 1 icmp any any
```

3) Check a created access list using the 'show running-config network' command.

Configuration using Web UI

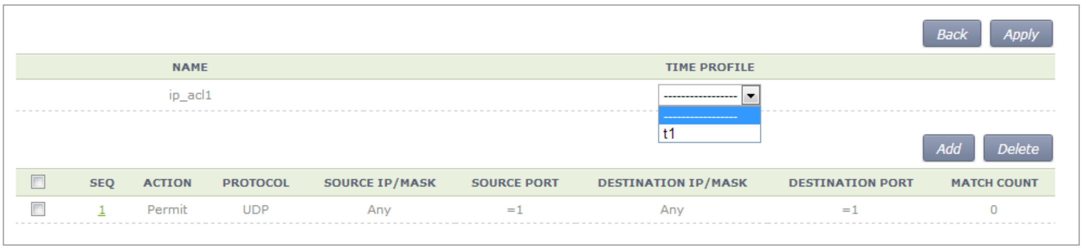
In the menu bar of <**WEC Main window**>, select <**Configuration**> and then select the <**Security**> → <**Access Control Lists**> → <**IP ACL**> menu in the sub-menus.
The initial window of ACL rule configuration is shown below. When you click the <**Add**> or <**Delete**> button, you can add or delete ACL rule.



☐	NAME
☐	ip_acl1
☐	ip_acl2

Figure 37. ACL Configuration Window

To change the configuration of ACL rule, click ACL NAME to change. You can change the configuration using the <**Add**> or <**Delete**> button. In addition, if there is a time profile in an ACL name, the IP ALC window is changed as shown below. After selecting a time profile, click the <**Apply**> button to apply the time profile to the ACL.



NAME	TIME PROFILE
ip_acl1	----------------

☐	SEQ	ACTION	PROTOCOL	SOURCE IP/MASK	SOURCE PORT	DESTINATION IP/MASK	DESTINATION PORT	MATCH COUNT
☐	1	Permit	UDP	Any	=1	Any	=1	0

Figure 38. Window where a Time Profile is Applied to ACL

3.5.1.2 ACL Rule Configuration

Configuration using CLI

1) Go to interface configuration mode where you will apply the configure → ACL rule of CLI.

```
APC# configure terminal
APC/configure# interface [name]
APC/configure/interface [name]#
```

2) Configure ACL to an interface.
   - ip access-group [MODE] [DIRECTION] [ACL_NAME]

Parameter	Description
MODE	Configuration mode (fw/fqm)

Parameter	Description
DIRECTION	Application direction configuration (in/out)
ACL_NAME	ACL name to configure

An example of entering a command that configures 'acl1' to the 'ge2' interface is shown below.

```
APC# configure terminal
APC/configure# interface ge2
APC/configure/interface ge2#ip access-group fqm in acl1
```

3) To check the configuration information, use the 'show running-config network' command.

Configuration using Web UI

In the menu bar of <**WEC Main window**>, select <**Configuration**> and then select the <**Security**> → <**Access Control Lists**> → <**Access Group (Interface)**> menu in the sub-menus.

The initial window of WLAN ACL configuration is shown below. When you click the <**Add**> or <**Delete**> button, you can add or delete ACL rule.

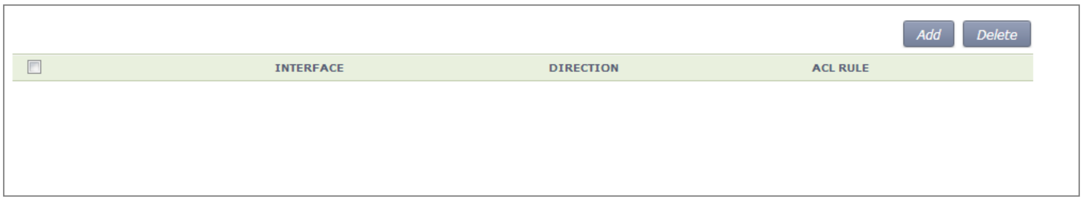
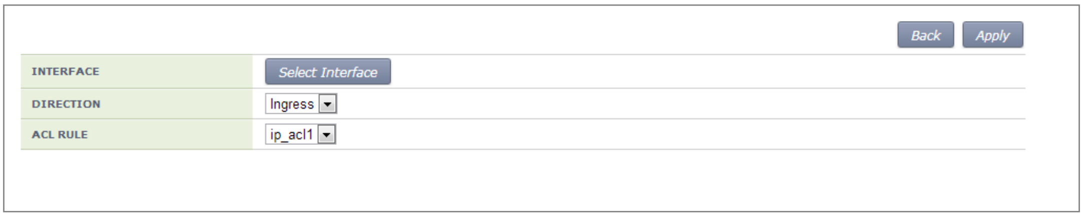


Figure 39. ACL Interface Configuration Window (1)

To perform detail configuration, select an interface in the list.



INTERFACE	Select Interface
DIRECTION	Ingress
ACL RULE	ip_acl1

Figure 40. ACL Interface Configuration Window (2)

The types of interfaces you can configure are retrieved. In the INTERFACE, select an interface. For DIRECTION, select Ingress or Egress. For ACL NAME, select an item (name) that is configured in the ACL List configuration.

To apply the changed configuration, click the <**Apply**> button.

3.5.1.3 WLAN ACL Configuration

1) Go to the fqm mode to configure the configure → ACL rule of CLI.

```
APC# configure terminal
APC/configure# fqm-mode
```

2) Configure WLAN ACL by entering the ‘ip access-group wireless’ command.
   - ip access-group wireless [ACL_NAME]

Parameter	Description
ACL_NAME	ACL name to configure

3) To check the configuration information, use the ‘show running-config network’ command.

3.5.1.4 Admin ACL Configuring

Configuration using CLI

1) Go to the fqm mode to configure → ACL rule of CLI.

```
APC# configure terminal
APC/configure# fqm-mode
```

2) Configure Admin ACL by entering the ‘ip access-group wireless’ command.
   - ip access-group system [ACL_NAME]

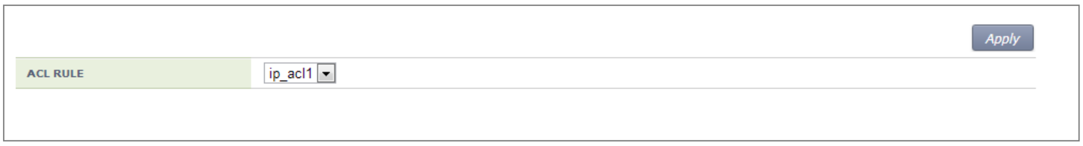
Parameter	Description
ACL_NAME	ACL name to configure

3) To check the configuration information, use the ‘show running-config network’ command.

Configuration using Web UI

In the menu bar of <**WEC Main window**>, select <**Configuration**> and then select the <**Security**> → <**Access Control Lists**> → <**Access Group (System)**> menu in the sub-menus.

The initial window of Access Group is shown below. After selecting a configuration, click the <**Apply**> button to configure Admin ACL.



ACL RULE: ip_acl1

Figure 41. Admin ACL Configuration Window

3.5.2 Class-map Configuration

1) Go to the fqm mode to configure the configure → ACL rule of CLI.

```
APC# configure terminal
APC/configure# fqm-mode
```

2) Go to Class-map mode.
   - class-map c1

3) Select match-all or match-any.
   - match-type [MODE]

Parameter	Description
MODE	Match mode configuration (match-all/match-any)

4) Perform detail configuration according to match criteria.

Match Criteria	Description
access-group	match access-group [ACCESS_GROUP_NAME]
class	match class [CLASS_NAME]
COS	match cos [COS_VALUE/any]
destination IP range	match dst ip range [A.B.C.D] [A.B.C.D]
IP	match ip dscp [DSCP_VALUE/any] match ip precedence [IP_PRECEDENCE_VALUE/any] match ip tos [TOS_VALUE/any]
protocol	match protocol [PROTOCOL_VALE/any]
source IP range	match src ip range [A.B.C.D] [A.B.C.D]

5) Exit the Class-map mode.
   - exit

6) To check the configuration information, use the ‘show running-config network’ command.

3.5.3 Policy-map Configuration

1) Go to the fqm mode to configure the configure → ACL rule of CLI.

```
APC# configure terminal
APC/configure# fqm-mode
```

2) Go to policy-map mode. To delete a policy map, enter ‘no’ parameter in front of the command.
   - policy-map [POLICY_MAP_NAME]
   - no policy-map [POLICY_MAP_NAME]

3) By using the class name configured in the class-map, go to the input mode.
   - class [CLASSMAP_NAME]

4) Configure a policy-map using the following command.

   [Bandwidth to a class of traffic]
   - bandwidth percentage [PERCENTAGE_VALUE]

   [Configure set action]
   - mark cos [COS_VALUE]
   - mark ip dscp [DSCP_VALUE]
   - mark ip precedence [PRECEDENCE_VALUE]
   - mark priority [PRIORITY_VALUE]

   [Configure police action]
   - police trtcm cir [1-1000] cbs [125000-125000000] pir [1-1000] pbs [125000-125000000] conform-action(drop|(dscp [0-63]|ip [0-7])|transmit) exceed-action(drop|(dscp [0-63]|ip [0-7])|transmit) violate-action(drop|(dscp [0-63]|ip [0-7])|transmit)(color-aware|color-blind|)

   [Peak rate to a class of traffic]
   - queue-limit [QUEUE_NUM]

   [Peak rate to a class of traffic]
   - shape-peak [PEAK_RATE]

5) Exit the policy-map mode.
   - exit

6) To check the configuration information, use the ‘show running-config network’ command.

3.5.4 Service Policy Configuration

Apply the policy configured in the policy-map to an interface.

1) Go to configure → interface configuring mode to apply the service policy of CLI.

```
APC# configure terminal
APC/configure# interface ge2
APC/configure/interface ge2#
```

2) Apply the policy configured in the policy-map to an interface. The ‘no’ parameter is used to delete the policy.
   - service-policy [DIRECTION] [POLICY_NAME]
   - no service-policy [DIRECTION] [POLICY_NAME]

Parameter	Description
DIRECTION	Application direction configuration (in/out)
POLICY_NAME	Policy to apply

An example of entering a command is shown below.

```
APC/configure/interface ge2# service-policy in p1
APC/configure/interface ge2# no service-policy in p1
```

3) To check the configuration information, use the ‘show running-config network’ command.

3.5.5 Time Profile

The procedure of configuring a time profile and applying it to ACL is described.

3.5.5.1 Time Profile Configuration

Configuration using CLI

1) Go to configure of CLI→ fqm mode.

```
APC# configure terminal
APC/configure# fqm-mode
```

2) Configure a time profile. The 'no' parameter is used to delete a time profile.
    - time-profile [PROFILE_NAME]
      day-start (any|YY[-MM[-DD[THH[:MM[:SS]]]]])
      day-stop (any|YY[-MM[-DD[THH[:MM[:SS]]]]])
      time-start (any|HH:MM[:SS])
      time-stop (any|HH:[MM:SS])
      monthdays (any|[0-31])
      weekdays (any|VARIABLE))
    - no time-profile [PROFILE_NAME]

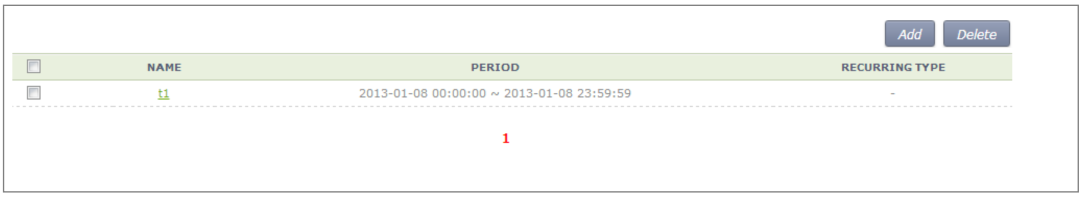
Parameter	Description
PROFILE_NAME	Name of a time profile to configure

3) To check the configured time profile, use the 'show running-config network' command.

Configuration using Web UI

In the menu bar of <**WEC Main window**>, select <**Configuration**> and then select the <**Security**> → <**Access Control Lists**> → <**Time Profile**> menu in the sub-menus.

The configured time profile list is displayed on the window. When you click the <**Add**> or <**Delete**> button, you can add or delete a time profile.

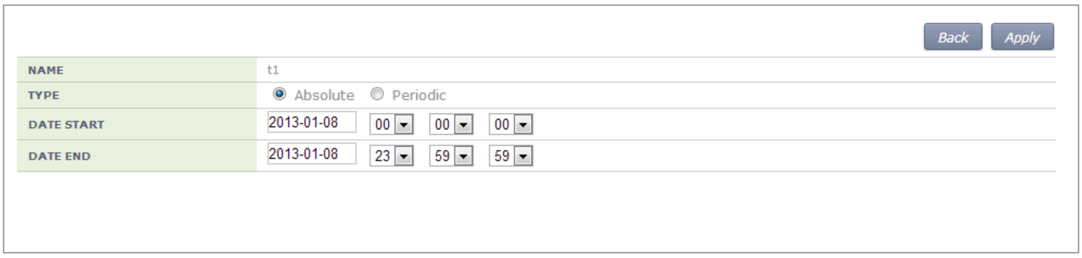


□	NAME	PERIOD	RECURRING TYPE
□	t1	2013-01-08 00:00:00 ~ 2013-01-08 23:59:59	-

1

Figure 42. Time Profile Configuration Window (1)

Select an item in the list and perform detail configuration.



NAME	t1
TYPE	● Absolute ○ Periodic
DATE START	2013-01-08 00 00 00
DATE END	2013-01-08 23 59 59

Figure 43. Time Profile Configuration Window (2)

After finishing configuration in the window, click the <**Apply**> button to apply it to the system.

3.5.5.2 Applying to ACL

Configuration using CLI

1) Go to the fqm mode to configure the configure → ACL rule of CLI.

```
APC# configure terminal
APC/configure# fqm-mode
```

2) Apply a time-profile to ACL. The ‘no’ parameter is used to delete a time profile.
   - access-list ip [ACL_NAME] time-profile [PROFILE_NAME]
   - no access-list ip [ACL_NAME] time-profile [PROFILE_NAME]

Parameter	Description
ACL_NAME	ACL name to configure
PROFILE_NAME	Name of a time profile to configure

An example of applying ‘t1’ to ‘acl’ is shown below.

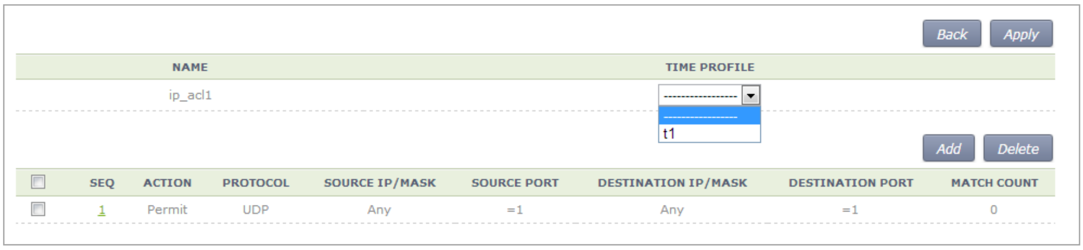
```
APC# configure terminal
APC/configure# fqm-mode
access-list ip acl1 time-profile t1
```

3) To check the configuration information, use the ‘show running-config network’ command.

Configuration using Web UI

In the menu bar of <**WEC Main window**>, select <**Configuration**> and then select the <**Security**> → <**Access Control Lists**> → <**IP ACL**> menu in the sub-menus.

To change the configuration of ACL rule, click ACLNAME to change. You can change the configuration using the <**Add**> or <**Delete**> button. In addition, if there is a time profile in an ACL name, the IP ACL window is changed as shown below. After selecting a time profile, click the <**Apply**> button to apply the time profile to the ACL.



NAME	TIME PROFILE
ip_acl1	------------------ t1

□	SEQ	ACTION	PROTOCOL	SOURCE IP/MASK	SOURCE PORT	DESTINATION IP/MASK	DESTINATION PORT	MATCH COUNT
□	1	Permit	UDP	Any	=1	Any	=1	0

Figure 44. Applying to ACL

3.5.5.3 ACL (Time-Profile) Rule Configuration

Configuration using CLI

1) Go to configure → interface configuration mode of CLI.

```
APC# configure terminal
APC/configure# interface ge2
```

2) Configure ACL to the interface. The ‘no’ parameter is used to delete ACL.
   - ip access-group [MODE] [DIRECTION] [ACL_NAME]
   - no ip access-group [fw/fqm] [DIRECTION] [ACL_NAME]

Parameter	Description
MODE	Configuration mode (fw/fqm) For ACL rule configuration, select ‘fqm’ (The ‘fw’ is used for firewall configuration.)
DIRECTION	Application direction configuration (in/out)
ACL_NAME	ACL name to configure

3) To check the configuration information, use the ‘show running-config network’ command.

Configuration using Web UI

In the menu bar of <**WEC Main window**>, select <**Configuration**> and then select the <**Security**> → <**Access Control Lists**> → <**Access Group (Interface)**> menu in the sub-menus.

Perform configuration by referring to ‘ACL Rule Configuration’.

3.5.6 OS-AWARE

OS-AWARE is a function to use the option value of the DHCP Discover/Request transmitted from a station to check the type of the operating system used by the station.

The procedures to set OS-AWARE and apply the OS-AWARE settings to ACL are described below.

3.5.6.1 OS-AWARE Configuration

Configuration using CLI

1) Go to configure → os-aware mode of CLI.

```
APC# configure terminal
APC/configure# os-aware
APC/configure/os-aware # ?

     delete                         Os-aware delete operation
     exit                           Exit from os-aware mode
     os-aware                       Os-aware add operation
     update                         Os-aware update
```

2) Set the OS-AWARE. Use the ‘delete’ parameter to delete the OS-AWARE.
- os-aware [OS_AWARE NAME] dhcp-option [OPTION_NUM] dhcp-option [OPTION_NUM] eq[VALUE] os-type [OS_TYPE NAME]
- delete os-aware [OS_AWARE NAME]
- update os-aware [OS_AWARE NAME] dhcp-option [OPTION_NUM] dhcp-option [OPTION_NUM] eq [VALUE] os-type [OS_TYPE NAME]

Parameter	Description
OS_AWARE NAME	os-aware name to configure
SEQUENCE_NUM	Fingerprint pattern match sequence(1~255)
OPTION_NUM	dhcp option value (1~255)
VALUE	Fingerprint value(HEX)
OS_TYPE NAME	os-type name to configure(Unknown, android, ios, windows, mac)

os-aware ‘window7’ creation:

```
APC# configure terminal
APC/configure# os-aware
APC/configure/os-aware # os-aware window7 seq 5 dhcp-option 1 eq AA
os-type windows
```

os-aware ‘window7’ modification:

```
APC# configure terminal
APC/configure# os-aware
APC/configure/os-aware # os-aware window7 seq 8 dhcp-option 2 eq FF
os-type windows
```

os-aware ‘window7’ deletion:

```
APC# configure terminal
APC/configure# os-aware
APC/configure/os-aware # no os-aware window7
```

3) Check the settings by using the ‘show OS-AWARE-all’ or ‘show OS-AWARE-[OS_AWARE NAME]’ commands.
‘show OS-AWARE-all’ retrieves all OS-AWARE information and ‘show OS-AWARE-[OS_AWARE NAME]’ only retrieves user defined information out of all OS-AWARE information.

```
======================================================================
=========================
PLD_INDEX   OS_NAME  TYPE   REFCNT    OPTION   LENGTH   FINGERPRINT
OS_TYPE
======================================================================
=========================
    1       window7   0     0         5        2        1234 windows
```

3.5.6.2 Applying to ACL

Configuration using CLI

1) Go to configure → fqm mode to set the ACL rule of CLI.

```
APC# configure terminal
APC/configure# fqm-mode
```

2) Apply the OS-AWARE to ACL. Use the ‘no’ parameter to delete the OS-AWARE
   - access-list [ip/ipv6/mac] [ACL_NAME] [deny/permit/time-profile] seq [seq_NUM] [1/*/ahp/eigrp/esp/gre/icmp/igmp/igrp/ip/nos/ospf/pcp/pim/17/6/tcp/udp/1-255] [any/A.B.C.D A.B.C.D] eq [eq_VALUE] [any/A.B.C.D A.B.C.D] eq [eq_VALUE] os-aware[OS_AWARE NAME] [[[dscp [*|[0-63]]|precedence [*|[0-7])]]]|]
   - no access-list [ip/ipv6/mac] [ACL_NAME] [deny/permit/time-profile] seq [seq_NUM] [1/*/ahp/eigrp/esp/gre/icmp/igmp/igrp/ip/nos/ospf/pcp/pim/17/6/tcp/udp/1-255] [any/A.B.C.D A.B.C.D] eq [eq_VALUE] [any/A.B.C.D A.B.C.D] eq [eq_VALUE] os-aware[OS_AWARE NAME] [[[dscp [*|[0-63]]|precedence [*|[0-7])]]]|]

Parameter	Description
OS_AWARE NAME	os-aware name to configure

An example of applying ‘window7’ to ‘acl’ is as follows.

```
APC# configure terminal
APC/configure# fqm-mode
access-list ip acl1 permit seq 1 icmp any any os-aware window7
```

3) To check the configuration information, use the ‘show running-config network’ command.

3.6 Multicast to Unicast

Execute the ‘show multi2uni-list’ command to check the list of wireless terminals that use the multicast to unicast function.

3.7 IP Multicast Configuration

3.7.1 IP Multicast Routing Configuration

Configuration using CLI

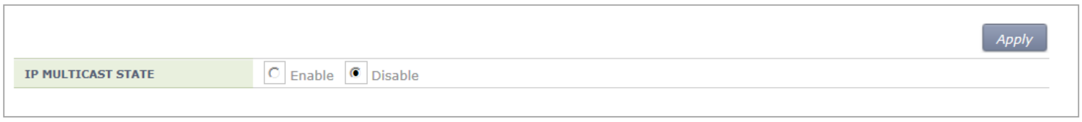
1) Go to configure mode of CLI.

```
WEC8500# configure terminal
```

2) Enable or disable the routing function for IP multicast.
   - ip multicast-routing: Enable
   - no ip multicast-routing: Disable

Configuration using Web UI

In the menu bar of **<WEC Main window>**, select **<Configuration>** and then select the **<Controller>** → **<Multicast>** → **<IP Multicast>** menu in the sub-menus.
After selecting Enable/Disable in the IP Multicast window, click the <**Apply**> button to apply the configuration.



IP MULTICAST STATE ○ Enable ● Disable

Figure 45. IP Multicast Configuration Window

3.7.2 PIM Configuration

As a multicast layer3 transmission protocol, the PIM has two modes, i.e. Dense mode and Sparse mode. The WEC8500 supports only PIM Sparse mode and the PIM Sparse mode can be configured for each interface.

Configuration using CLI

1) Go to configure of CLI → mode where you want to perform configuration.

```
WEC8500# configure terminal
WEC8500/configure# interface ge2
```

2) Perform PIM configuration.
   - ip pim sparse-mode: Enable
   - no ip pim sparse-mode: Disable

Configuration using Web UI

In the menu bar of <**WEC Main window**>, select <**Configuration**> and then select the <**Controller**> → <**Multicast**> → <**PIM-SM**> menu in the sub-menus. When you click the <**Add**> or <**Delete**> button, you can add or delete PIM-SM configuration.

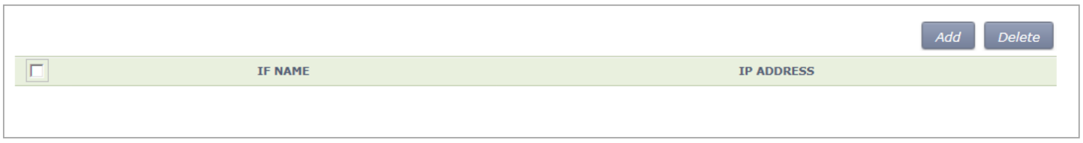


Figure 46. PIM-SM Configuration Window (1)

Follow the below procedure to add a PIM.

1) In the PIM-SM initial window, click the <**Add**> button.

2) Click the <**Select Interface**> button.

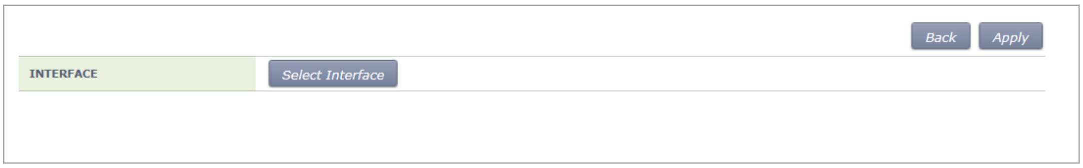
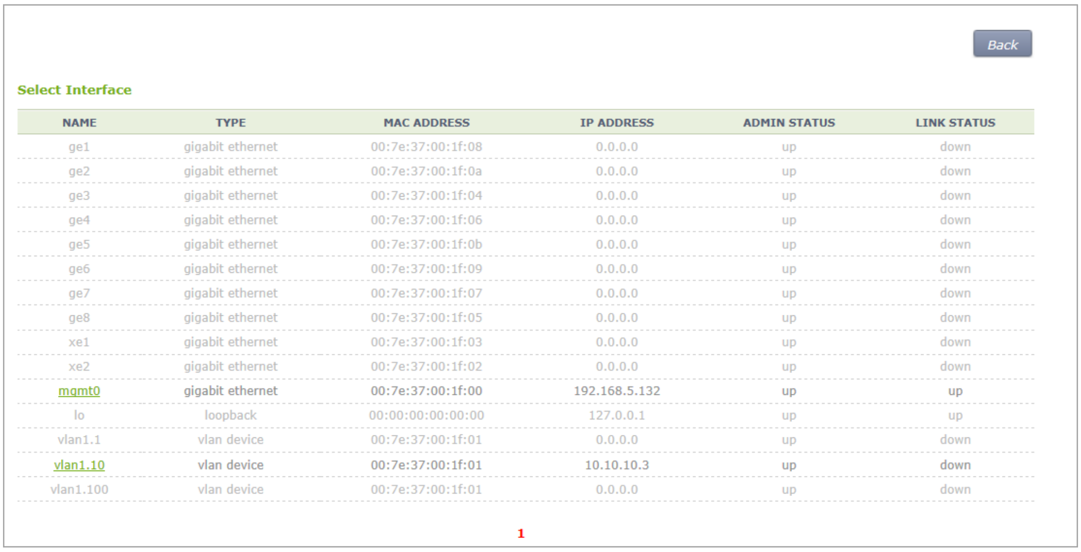


Figure 47. PIM-SM Configuration Window (2)

3) Select an interface to add.

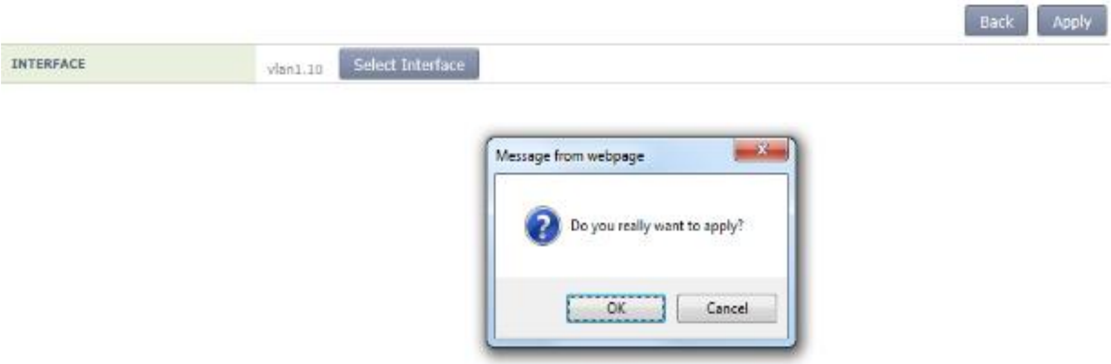


Select Interface

NAME	TYPE	MAC ADDRESS	IP ADDRESS	ADMIN STATUS	LINK STATUS
ge1	gigabit ethernet	00:7e:37:00:1f:08	0.0.0.0	up	down
ge2	gigabit ethernet	00:7e:37:00:1f:0a	0.0.0.0	up	down
ge3	gigabit ethernet	00:7e:37:00:1f:04	0.0.0.0	up	down
ge4	gigabit ethernet	00:7e:37:00:1f:06	0.0.0.0	up	down
ge5	gigabit ethernet	00:7e:37:00:1f:0b	0.0.0.0	up	down
ge6	gigabit ethernet	00:7e:37:00:1f:09	0.0.0.0	up	down
ge7	gigabit ethernet	00:7e:37:00:1f:07	0.0.0.0	up	down
ge8	gigabit ethernet	00:7e:37:00:1f:05	0.0.0.0	up	down
xe1	gigabit ethernet	00:7e:37:00:1f:03	0.0.0.0	up	down
xe2	gigabit ethernet	00:7e:37:00:1f:02	0.0.0.0	up	down
mgmt0	gigabit ethernet	00:7e:37:00:1f:00	192.168.5.132	up	up
lo	loopback	00:00:00:00:00:00	127.0.0.1	up	up
vlan1.1	vlan device	00:7e:37:00:1f:01	0.0.0.0	up	down
vlan1.10	vlan device	00:7e:37:00:1f:01	10.10.10.3	up	down
vlan1.100	vlan device	00:7e:37:00:1f:01	0.0.0.0	up	down

Figure 48. PIM-SM Configuration Window (3)

4) The selected interface is displayed on the window. Click the <**Apply**> button to apply the configuration.



INTERFACE vlan1.10

Do you really want to apply?

Figure 49. PIM-SM Configuration Window (4)

3.8 IGMP Snooping

Configuration using CLI

Use the ‘ip igmp snooping’ command to enable or disable Internet Group Management Protocol (IGMP) Snooping.

- ip igmp snooping
- no ip igmp snooping

When this command is executed in the Configure mode, the IGMP Snooping of a bridge is enabled or disabled. If it is executed in the interface mode, the IGMP Snooping of an interface is enabled or disabled.

Configuring the IGMP Snooping of a bridge:

```
WEC8500# configure terminal
WEC8500/configure# ip igmp snooping
```

Configuring the IGMP Snooping of a VLAN interface:

```
WEC8500# configure terminal
WEC8500/configure# interface vlan1.10
WEC8500/configure/interface vlan1.10# ip igmp snooping
```

In addition, a specific function of the IGMP Snooping functions of a VLAN interface can be enabled or disabled as shown in the below command.

[ip igmp snooping fast-leave]

This command enables or disables the Fast-Leave function. (Default: Enable status)

- ip igmp snooping fast-leave
- no ip igmp snooping fast-leave

[ip igmp snooping querier]

This command enables or disables the Querier function. (Default: Enable status)

- ip igmp snooping querier
- no ip igmp snooping querier

[ip igmp snooping report-suppression]

This command enables or disables the Report-suppression function. (Default: Enable status)

- ip igmp snooping report-suppression
- no ip igmp snooping report-suppression

[ip igmp snooping mroute]

This command enables or disables the Mroute function.

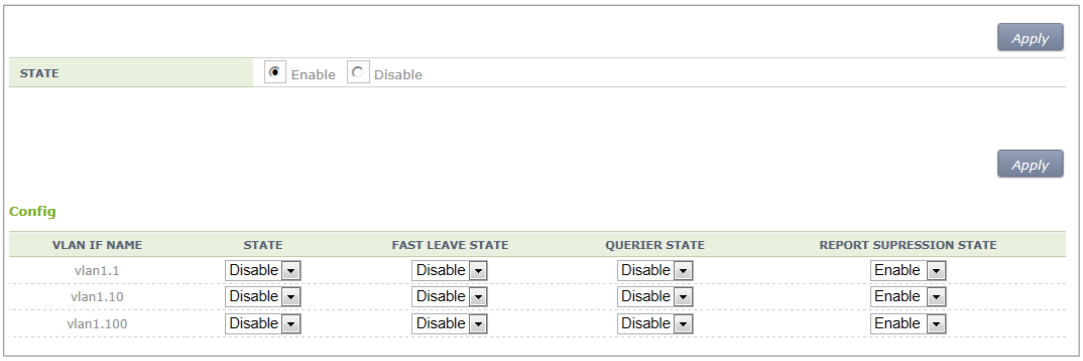
- ip igmp snooping mroute [INTERFACE]
- no ip igmp snooping mroute [INTERFACE]

Configuration using Web UI

In the menu bar of <**WEC Main window**>, select <**Configuration**> and then select the <**Controller**> → <**Multicast**> → <**IGMP Snooping**> menu in the sub-menus.

[Config]

Enables or disables the IGMP Snooping function or configures related functions.
To perform configuration for STATE, FAST LEAVE, QUERIER STATE, or REPORT SUPRESSION STATE, select Enable or Disable and click the <**Apply**> button.



STATE ● Enable ○ Disable

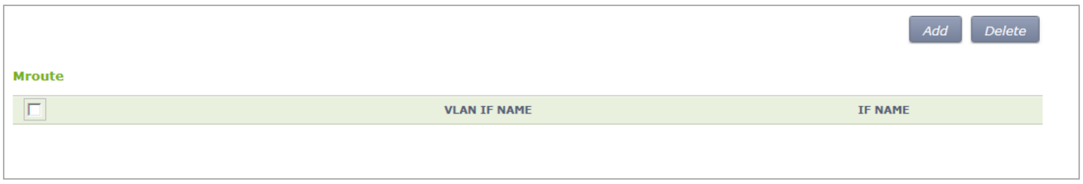
Config

VLAN IF NAME	STATE	FAST LEAVE STATE	QUERIER STATE	REPORT SUPRESSION STATE
vlan1.1	Disable	Disable	Disable	Enable
vlan1.10	Disable	Disable	Disable	Enable
vlan1.100	Disable	Disable	Disable	Enable

Figure 50. IGMP Snooping Config Window

[Mroute]

The PIM-SM initial window is shown below. When you click the <**Add**> or <**Delete**> button, you can add or delete PIM-SM configuration.



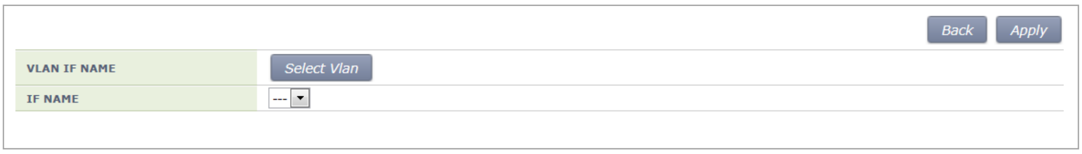
Mroute

□	VLAN IF NAME	IF NAME

Figure 51. IGMP Snooping Mroute Creation Window (1)

1) In the PIM-SM initial window, click the <**Add**> button.

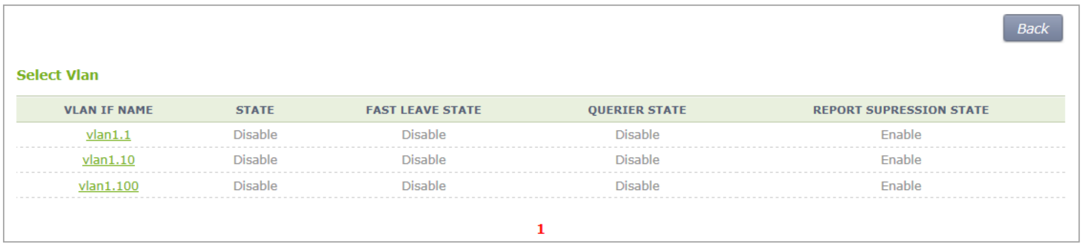
2) Click the <**Select Vlan**> button.



VLAN IF NAME	
IF NAME	---

Figure 52. IGMP Snooping Mroute Creation Window (2)

3) Select a VLAN interface that will be added to the Mroute.

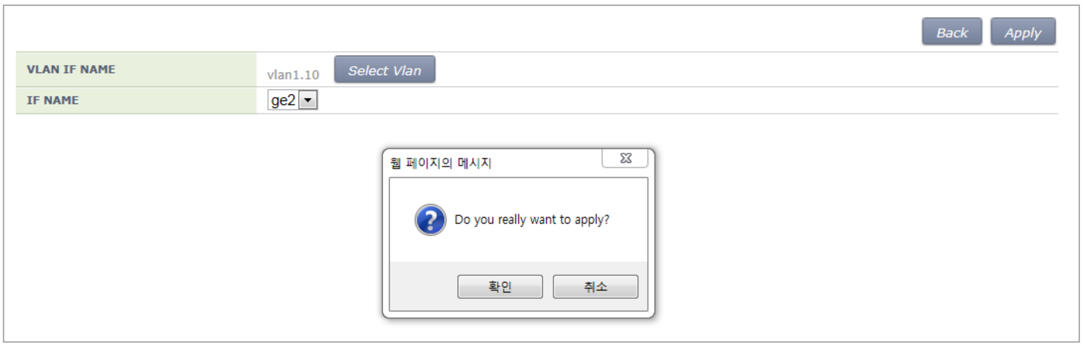


Select Vlan

VLAN IF NAME	STATE	FAST LEAVE STATE	QUERIER STATE	REPORT SUPRESSION STATE
vlan1.1	Disable	Disable	Disable	Enable
vlan1.10	Disable	Disable	Disable	Enable
vlan1.100	Disable	Disable	Disable	Enable

Figure 53. IGMP Snooping Mroute Creation Window (3)

4) The selected interface is displayed on the window. Click the <**Apply**> button to apply the configuration.



VLAN IF NAME	vlan1.10
IF NAME	ge2

웹 페이지의 메시지

Do you really want to apply?

Figure 54. IGMP Snooping Mroute Creation Window (4)

CHAPTER 4. AP Connection Management

This chapter describes the various configuration methods to manage the connection between the APC and AP.

4.1 APC Management

4.1.1 Managing APC List

To enable the APC system to provide the cluster or redundancy service, several APC systems must be installed at a site and each APC must have the information of other APC systems.

Therefore, the APC system provides the function of managing the list of APCs that will provide the cluster or redundancy function. And the APCs added to the APC list are used during cluster or redundancy configuration.

One APC system that will be saved in the APC list consists of an APC name and Medium Access Control (MAC) information. For the MAC address of another APC system, enter the MAC address retrieved from the Monitor → Summary → Inventory → MAC Address menu of system WEC screen.

By default, its own system information is added to the APC list. For the APC, operator can only change its name, but cannot delete it forcibly or change its MAC address.

The maximum number of APC systems that can be registered per model is as follows:

APC Model	The maximum number of APC systems that can be registered
WEC8500	12
WEC8050	2

Configuration using CLI

The procedures for configuration are as follows.

1) Go to configure mode of CLI.

```
WEC8500# configure terminal
WEC8500/configure# apc
WEC8500/configure/apc/apc-list#
```

2) Go to the apc-list item of CLI.

```
WEC8500/configure# apc
WEC8500/configure/apc/apc-list#
```

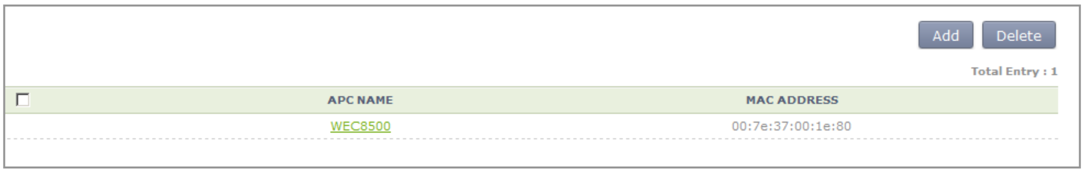
3) Add, delete or change APC.
   - add-apc [APC_NAME] [MAC_ADDRESS]
   - del-apc [APC_NAME]
   - change-apc [CURRENT_APC_NAME] [NEW_APC_NAME]
   - change-mac [APC_NAME] [MAC_ADDRESS]

Parameter	Description
APC_NAME	APC name
CURRENT_APC_NAME	Current APC name (before change)
NEW_APC_NAME	APC name after change
IP_ADDRESS	APC MAC address (xx:xx:xx:xx:xx:xx) In the APC system, enter the system mac address output parameter value of 'show system info' command.)

4) To check the configured APC list, execute the 'show apc-list' command.

Configuration using Web UI

In the menu bar of <**WEC Main window**>, select <**Configuration**> and then select the <**Controller**> → <**APC Lists**> menu in the sub-menus. Operator can add a new APC by clicking the <**Add**> button in the figure.



Total Entry : 1

□	APC NAME	MAC ADDRESS
	WEC8500	00:7e:37:00:1e:80

Figure 55. APC List Management Window

4.1.2 Management Interface Configuration

The APC can communicate with a W-EP wireless LAN AP using management interface. This is one of the information that must be configured first of all for wireless LAN service.

Configuration using CLI

To configure management interface, execute the command as follows:

1) Go to configure mode of CLI.

```
WEC8500# configure terminal
WEC8500/configure#
```

2) Configure a management interface.
   - apc ap-mgmt-if [IP_ADDRESS]

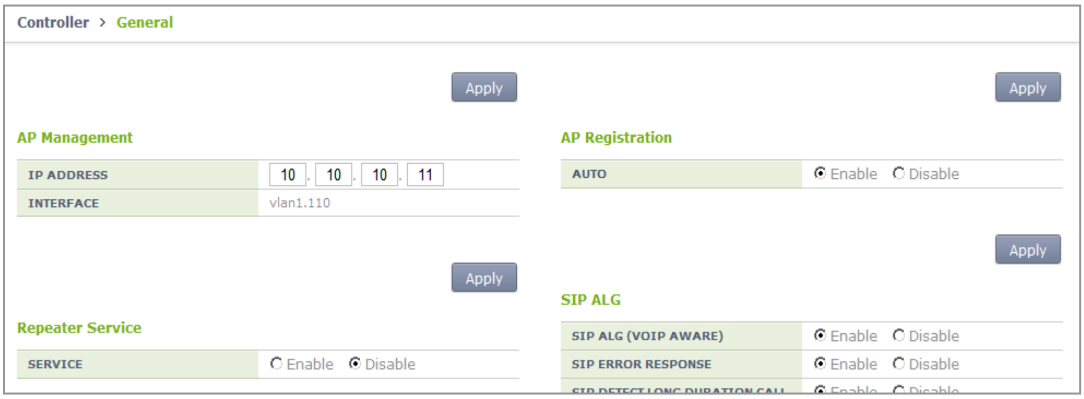
Parameter	Description
IP_ADDRESS	IP address of APC that is used for communication with a W-EP wireless LAN AP

3) To check the configured IP information, use the 'show apc summary' command.

Configuration using Web UI

In the menu bar of **<WEC Main window>**, select **<Configuration>** and then select the **<Controller>** → **<General>** menu in the sub-menus.

After entering a configuration in the AP Management of the window, click the **<Apply>** button.



AP Management

IP ADDRESS	10 . 10 . 10 . 11
INTERFACE	vlan1.110

Repeater Service

SERVICE	○ Enable ● Disable

AP Registration

AUTO	● Enable ○ Disable

SIP ALG

SIP ALG (VOIP AWARE)	● Enable ○ Disable
SIP ERROR RESPONSE	● Enable ○ Disable
SIP DETECT LONG DURATION CALL	● Enable ○ Disable

Figure 56. Management interface configuration

4.1.3 CAPWAP Configuration

A secured tunnel is created between APC and W-EP wireless LAN AP using Control And Provisioning Wireless Access Point (CAPWAP), i.e. a standard protocol, and data is transmitted through the tunnel. An encrypted data is used for both wire and wireless sections, high security is provided.

The CAPWAP channel consists of control channel and data channel depending on the type of packet being transmitted/received. The control channel handles provisioning and configuration/control messages and the data channel transmits the data traffic exchanged with a wireless terminal through CAPWAP tunneling. Because the control channel transmits the wireless LAN configuration information, there should be no data loss. Therefore, the re-transmission function is basically provided. In addition, the Datagram Transmission Layer Security (DTLS) is mandatorily used for the security of transmitted data. Meanwhile, as user data traffic is transmitted through the data channel, a faster response is preferred instead of packet transmission reliability. Therefore, the re-transmission function is not provided and the DTLS function is also optional.

For CAPWAP configuration, execute the following commands.

1) Go to configure → apc→ capwap of CLI.

```
WEC8500# configure terminal
WEC8500/configure# apc
WEC8500/configure/apc/capwap#
WEC8500# configure terminal
WEC8500/configure# apc
WEC8500/configure/apc/capwap#
```

2) Configure the CAPWAP function using the following commands.
   - add-multicast-if [VLAN_ID]: Configure a VLAN ID for multicast interface.
   - auto-discovery: Configures the function of automatically detecting and registering an AP.
   - auto-discovery-ap-group [AP_GROUP_ID]: Configures an AP group that will be working when an AP is automatically registered.
   - change-state-pending-timer [TIMER]: Configures the maximum waiting time until the APC receives the Change State Event Request message from an AP after transmitting the Configuration Status Response message to the AP (RFC 5415).
   - ctr-src-port [port]: Changes the CAPWAP Control port (RFC5415).
   - date-check-timer [TIMER]: Configures the maximum waiting time until the APC receives Data Channel Keep-alive (default: 30 seconds)
   - discovery-by-broadcast: Configures whether to allow connection to CAPWAP broadcast.

- discovery-by-multicast: Configures whether to allow connection to CAPWAP multicast. (The 'add-multicast-if' must be configured before configuring whether to allow multicast connection.)
- discovery-del-timer: If the Join message is not received after receiving a Discovery message, this configures the timeout to discard the previously received Discovery messages.
- dtls-session-delete [TIMER]: Configures the waiting time to disconnect DTLS when releasing the connection between an AP and CAPWAP.
- retransmit-interval [INTERVAL]: Configures the re-transmission interval of CAPWAP control packet retransmission.
- max-retransmit [COUNT]: Configures maximum number of retransmission when there is no answer for CAPWAP control packet transmission.
- wait-dtls-timer [TIMER]: Configures the maximum time until the AP waits without receiving the DTLS handshake message from the APC (RFC 5415) (default: 60 seconds)
- wait-join-timer [TIMER]: Configures the maximum time until the APC receives the Join message after finishing DTLS handshake (RFC 5415) (default: 60 seconds)
- window-size [size]: Configures the maximum number of packets that can be transmitted without response during CAPWAP control packet transmission.

An example of entering a command is shown below.

```
WEC8500/configure/apc/capwap# date-check-timer 30
```

3) To check the configured CAPWAP information, use the 'show apc capwap summary' command.

4.1.4 AP Registration (Auto Discovery) Configuration

The APC provides the AP auto-discovery function that automatically registers APs in the same network without having to configure any settings in advance. To configure the function, execute the following commands.

Configuration using CLI

1) Go to configure → apc → capwap of CLI.

```
WEC8500# configure terminal
WEC8500/configure# apc
WEC8500/configure/apc # capwap
WEC8500/configure/apc/capwap #
```

2) Configure the automatic registration function.
   - auto-discovery

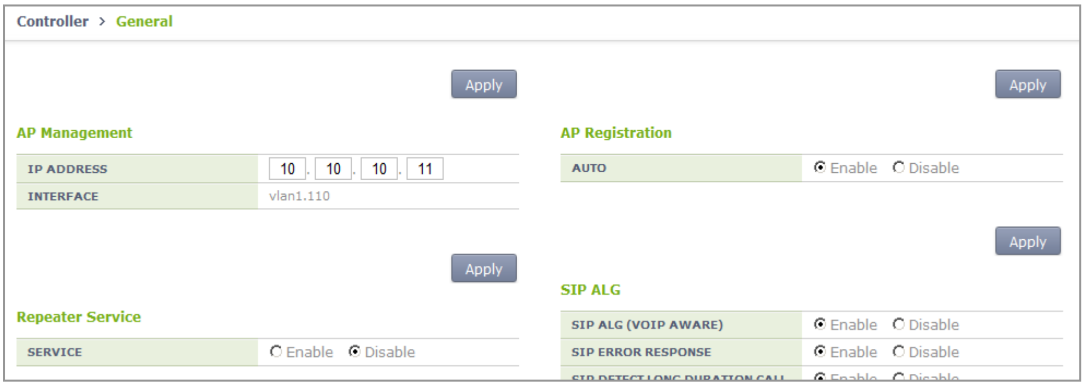
3) Configure an AP group that will be working after AP automatic registration.
   - auto-discovery-ap-group [AP_GROUP_ID]

Parameter	Description
AP_GROUP_ID	ap-group that will be working after AP automatic registration

4) To check the configured information, use the ‘show apc capwap summary’ command.

Configuration using Web UI

In the menu bar of <**WEC Main window**>, select <**Configuration**> and then select the <**Controller**> → <**General**> menu from the sub-menus.
After entering a configuration in the AP Registration of the window, click the <**Apply**> button.



AP Management

IP ADDRESS	10 . 10 . 10 . 11
INTERFACE	vlan1.110

AP Registration

AUTO	● Enable ○ Disable

Repeater Service

SERVICE	○ Enable ● Disable

SIP ALG

SIP ALG (VOIP AWARE)	● Enable ○ Disable
SIP ERROR RESPONSE	● Enable ○ Disable
SIP DETECT LONG DURATION CALL	● Enable ○ Disable

Figure 57. AP Registration Method Setup Window

4.1.5 Managing AP File Transmission

It provides the configuration and transmission management function for the tech support file of the AP.

4.1.5.1 Tech Support Information File

1) Go to configure → APC mode of CLI.

```
WEC8500# configure terminal
WEC8500/configure# apc
WEC8500/configure/apc#
```

2) Configure a file transmission method to collect the AP Tech support information.
   - tech-support [MODE]

Parameter	Description
MODE	Selects file transmission method (ftp/sftp/http). - tftp is not supported.

3) If AP debug information collection is failed, configure maximum number of retries.
   - tech-support max-retry [COUNT]

Parameter	Description
COUNT	Number of retries.

4) To check the configuration information, use the ‘show ap tech-support’ command.

4.1.6 APC Redundancy Configuration

An operator can add a backup APC to an AP to make the backup APC provide the service even when an APC fault occurs.

The maximum number of backup APCs that can be registered to one AP per model is as follows:

APC Model	The maximum number of APC systems that can be registered
WEC8500	3 (Primary Server, Secondary Server, Tertiary Server)
WEC8050	2 (Primary Server, Secondary Server)

If a fault occurs to the primary APC while an AP is connected to the primary APC, the AP is connected to the secondary APC. If a fault also occurs to the secondary APC, the AP is connected to the tertiary APC. For reference, the WEC8050 model does not support a tertiary APC.

Operator can also configure fallback to return to the original APC from the backup APC during the service. If the fallback operation is configured, the AP periodically performs health check to check whether the primary APC can be connected. When the connection is required, it can immediately perform fallback according to the fallback option or can perform fallback on a specified time. The reason why configuring fallback time zone is to minimize the service interruption due to fallback by making it happens when the load is low.

In an APC, operator can configure the primary and backup APCs of an AP in the following steps.

1) Register APCs to the APC list.
   In the 'APC List Management', how to add the APC list is described.
2) Add the APCs in the APC list to redundancy.
   If necessary, configure the fallback function.
   And then, operator can configure the APCs added to redundancy as the primary, secondary, or tertiary server of an AP.
3) Configure a primary, secondary, and tertiary server per AP. To make an AP operate in redundancy configuration, configure the Discovery Type of the AP as 'APC Referal'. Use the Multi-Set function of WEC to configure several APs at the same time.

Configuration using CLI

1) By referring to the 'AP List Management', add the APC list that will be used as a backup APC.
2) After entering into the configure → redundancy mode, add or delete the APCs in the APC list. If necessary, configure the fallback function.

```
WEC8500# configure terminal
WEC8500/configure# redundancy
WEC8500/configure/redundancy#
```

- add-apc [APC_NAME] [IP_ADDRESS] [PORT]
- del-apc [APC_NAME]
- fallback-enable now
- fallback-enable at-time [FALLBACK START-END TIME]
- fallback-interval [INTERVAL]

Parameter	Description
APC_NAME	Name of an APC to be added or deleted to/from redundancy The APC must be an APC registered in the APC list.
IP_ADDRESS	IP address of an APC to add This address is an IP required by an AP to connect to the APC. Therefore, you must enter the AP Management IP address of the APC.

Parameter	Description
PORT	CAPWAP PORT number of the APC to add This port number is required by an AP to connect to the APC. If no port number is entered, it is set to 5246, the default port number of CAPWAP protocol. It is recommended not to use a different port number if it is specially required.
FALLBACK START-END TIME	Enter the time zone where an AP connected to the backup (secondary or tertiary) APC can do fallback. The input format is as follows: - Format: hh:mm-hh:mm - Example: 2:00-5:00 ← Fallback is available between 2pm and 5pm.
INTERVAL	Configures the interval that an AP connected to the backup (secondary or tertiary) APC attempts fallback (second). If a specific time is not entered, the default is 120 seconds. The minimum is 60 seconds and the maximum is 1800 seconds.

3) Enter into the configure → AP configuration mode of CLI and configure a primary, secondary, and tertiary server. To make an AP operate in redundancy configuration, configure the Discovery of the AP as 'apc-referal'.

```
WEC8500# configure terminal
WEC8500/configure# ap ap_1
WEC8500/configure/ap ap_1#
```

- discovery apc-referal
- primary-apc [APC_NAME]
- secondary-apc [APC_NAME]
- tertiary-apc [APC_NAME]

Parameter	Description
APC_NAME	Enter the name of an APC registered to redundancy. - Primary apc: The first APC that the AP attempts to connect. It is usually configured with the currently connected APC. - Secondary-apc, tertiary-apc: APC that the AP attempts to connect when there is no response from the primary-apc.
DISCOVERY_TYPE	Discovery Type - ap-followed: Discovery type is set by AP. - apc-referal: Discovery type is set by APC using the backup APC lists. To apply the priority of APC to which the AP will be connected, operator needs to select the apc-referal. - DHCP: Discovery type is interoperating with the DHCP server. To use this mode, IP ADDRESS POLICY of the AP must be set to DHCP. - Auto: Discovery type is automatically changed by the AP for automatic connection to the APC.

4) To check the configured apc list, execute the ‘show apc summary’ command.

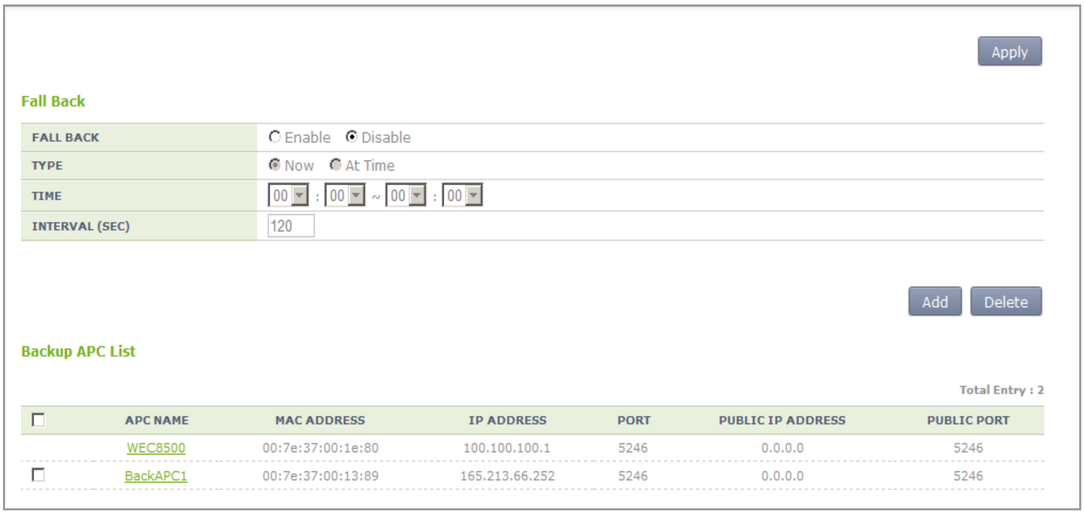
5) To check the redundancy information, execute the ‘show redundancy summary’ command.

6) To check the configured AP profile, execute the ‘show ap detail [AP_PROFILE_ NAME]’ command.

Configuration using Web UI

By referring to the ‘APC List Management’, add the APC list that will be used as a backup APC.

1) In the menu bar of <**WEC Main window**>, select <**Configuration**> and then select the <**Controller**> → <**Redundancy**> menu in the sub-menus. Operator can add or delete the APC list that will be used for redundancy. If necessary, operator can configure the fallback function.



Fall Back

FALL BACK	○ Enable ● Disable
TYPE	● Now ○ At Time
TIME	00 : 00 ~ 00 : 00
INTERVAL (SEC)	120

Backup APC List

Total Entry : 2

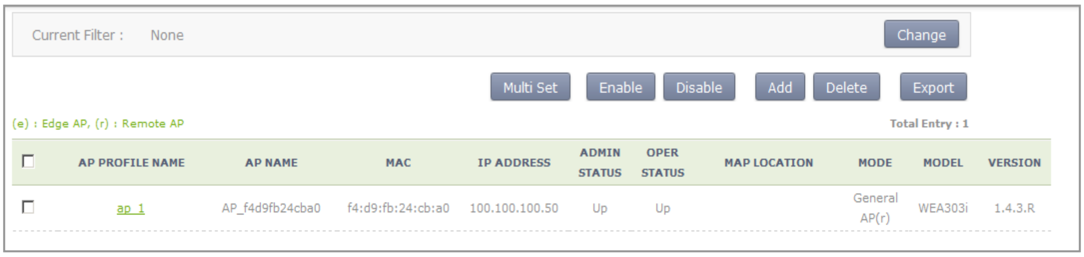
□	APC NAME	MAC ADDRESS	IP ADDRESS	PORT	PUBLIC IP ADDRESS	PUBLIC PORT
	WEC8500	00:7e:37:00:1e:80	100.100.100.1	5246	0.0.0.0	5246
□	BackAPC1	00:7e:37:00:13:89	165.213.66.252	5246	0.0.0.0	5246

Figure 58. Redundancy Configuration Window

Parameter	Description
APC NAME	Name of an APC to be added or deleted to/from redundancy The APC must be an APC registered in the APC list.
MAC ADDRESS	Because this is a MAC address configured during registration to the APC list, an operator does not have to enter this at the redundancy configuration stage.
IP_ADDRESS	IP address of an APC to add This address is an IP required by an AP to connect to the APC. Therefore, you must enter the AP Management IP address of the APC.
PORT	CAPWAP PORT number of the APC to add

Parameter	Description
	If no port number is entered, it is set to 5246, the default port number of CAPWAP protocol. It is recommended not to use a different port number if it is specially required.
PUBLIC_IP_ADDRESS	PUBLIC IP address of the APC to add This address is an IP required by an AP to connect to the APC. If the APC is in the NAT environment, you must enter an official IP configured in the NAT instead of the private IP of APC.
PUBLIC_PORT	PUBLIC CAPWAP PORT number of the APC to add This port number is required by an AP to connect to the APC. If the APC is under the NAT environment, you must enter the port number configured in the NAT instead of the actual CAPWAP port number of APC.
FALLBACK START-END TIME	Enter the time zone where an AP connected to the backup (secondary or tertiary) APC can do fallback. The input format is as follows: Format: hh:mm-hh:mm Example: 2:00-5:00 ← Fallback is available between 2pm and 5pm.
INTERVAL	Configures the interval that an AP connected to the backup (secondary or tertiary) APC attempts fallback (second). If a specific time is not entered, the default is 120 seconds. The minimum is 60 seconds and the maximum is 1800 seconds.

2) In the menu bar of <**WEC Main window**>, select <**Configuration**> and then select the <**Access Points**> menu in the sub-menus. Click the name of AP Profile to which the redundancy function will be applied. After configuring the DISCOVERY TYPE of AP to 'APC Referal', select the PRIMARY CONTROLLER NAME, SECONDARY CONTROLLER NAME, and TERTIARY CONTROLLER NAME. For the WEC8500 model, the TERTIARY CONTROLLER NAME is not shown in the menu.



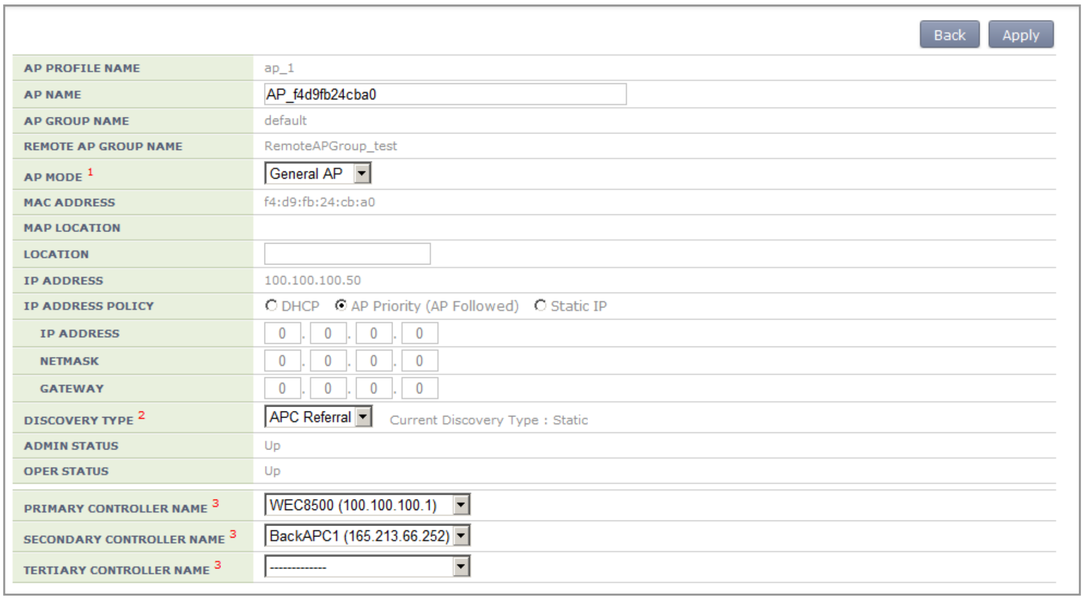
Current Filter : None

(e) : Edge AP, (r) : Remote AP

Total Entry : 1

□	AP PROFILE NAME	AP NAME	MAC	IP ADDRESS	ADMIN STATUS	OPER STATUS	MAP LOCATION	MODE	MODEL	VERSION
□	ap_1	AP_f4d9fb24cba0	f4:d9:fb:24:cb:a0	100.100.100.50	Up	Up		General AP(r)	WEA303i	1.4.3.R

Figure 59. AP retrieving window



AP PROFILE NAME	ap_1
AP NAME	AP_f4d9fb24cba0
AP GROUP NAME	default
REMOTE AP GROUP NAME	RemoteAPGroup_test
AP MODE [1]	General AP
MAC ADDRESS	f4:d9:fb:24:cb:a0
MAP LOCATION	
LOCATION	
IP ADDRESS	100.100.100.50
IP ADDRESS POLICY	○ DHCP ● AP Priority (AP Followed) ○ Static IP
IP ADDRESS	0 . 0 . 0 . 0
NETMASK	0 . 0 . 0 . 0
GATEWAY	0 . 0 . 0 . 0
DISCOVERY TYPE [2]	APC Referral Current Discovery Type : Static
ADMIN STATUS	Up
OPER STATUS	Up
PRIMARY CONTROLLER NAME [3]	WEC8500 (100.100.100.1)
SECONDARY CONTROLLER NAME [3]	BackAPC1 (165.213.66.252)
TERTIARY CONTROLLER NAME [3]	------------

Figure 60. AP redundancy Configuration Window

Parameter	Description
APC_NAME	Enter the name of an APC registered to redundancy. - Primary apc: The first APC that the AP attempts to connect. It is usually configured with the currently connected APC. - Secondary-apc, tertiary-apc: APC that the AP attempts to connect when there is no response from the primary-apc.
DISCOVERY_TYPE	Discovery Type - ap-followed: Discovery type is set by AP. - apc-referal: Discovery type is set by APC using the backup APC lists. To apply the priority of APC to which the AP will be connected, operator needs to select the apc-referal. - Auto: Discovery type is automatically changed by the AP for automatic connection to the APC. - DHCP: Discovery type is interoperating with the DHCP server. To use this mode, IP ADDRESS POLICY of the AP must be set to DHCP.

4.2 AP Management

4.2.1 AP Group Configuration

The APC manages the services provided to the AP by group. An operator can add or delete several APs to/from a group. It is also possible to add/remove WLANs to/from an AP group so that the same WLAN services can be provided for each group.

When the APC is installed for the first time, a ‘default’ group is created. When the AP information is created first time, the AP is automatically added to the ‘default’ group.
If the ‘auto-discovery’ mode is enabled in the APC, an AP connected to the APC is automatically added to the ‘default’ group. For reference, operator can specify a specific AP group where an AP will be added during auto-discovery configuration.

An operator can manage the services per group by creating a new AP group and can move or a specific AP to another group or delete it in the original group. The APs deleted in a group are automatically moved to the ‘default’ group.

When a new AP group is created, it is possible to configure AP information for each group. If the Overwrite option is enabled for each setting, the respective setting is applied to all APs within the group.

Generally, up to 16 WLANs can be added to an AP group. However, if a root AP is contained in an AP group, only up to 15 WLANs can be added to the group.

If the AP group information is changed, i.e. if an AP moves to another group, the AP uses the WLAN of a new group. Therefore, some existing WLANs in the AP are deleted and some new WLANs can be added. The detail example is shown below.
(Example) Default group: Includes wlan1, wlan2, wlan3, and wlan4.
New group: Includes wlan4, wlan5, and wlan6.
When the AP_1 moves from the default group to a new group
The APC asks the AP_1 to delete the wlan1, wlan2, and wlan3.
The APC asks the AP_1 to add the wlan5 and wlan6.

Configuration using CLI

To manage an AP group, execute the command as follows.

1) Go to configure mode of CLI.

```
WEC8500# configure terminal
WEC8500/configure#
```

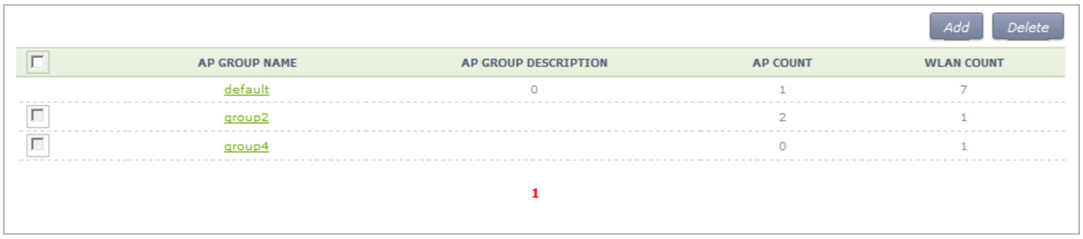
2) Create or delete an AP group. Use ‘no’ parameter in front of the command to delete an AP group.
   - ap-group [AP_GROUP_NAME]
   - no ap-group [AP_GROUP_NAME]

3) Add or delete an AP to or from the AP group. Use ‘no’ parameter in front of the command to delete an AP from the AP group. But, for a default AP group, you cannot delete an AP from the group. If you delete an AP from other AP groups other than the default group, the deleted AP is included into the default AP group.
   - add-ap [AP_NAME]
   - no add-ap [AP_NAME]

4) Use the ‘show ap-group summary’ command to check the AP group information.

Configuration using Web UI

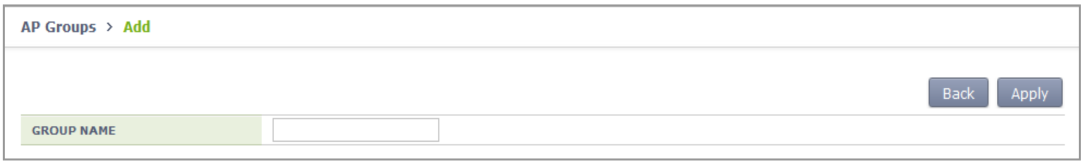
In the menu bar of <**WEC Main window**>, select <**Configuration**> and then select the <**AP Groups**> menu in the sub-menus. It provides the group configuration of the AP. Click the <**Add**> or <**Delete**> button to add or delete a group.



□	AP GROUP NAME	AP GROUP DESCRIPTION	AP COUNT	WLAN COUNT
	default	0	1	7
□	group2		2	1
□	group4		0	1

1

Figure 61. AP groups configuration Window



GROUP NAME	

Figure 62. AP Group Addition Window

General AP Group Settings

To aid management of APs in groups, the APC allows configuration of settings which can be applied commonly to each group. The following functions are provided:

Parameter	Description
Description	This configures the description of the AP group.
AP Mode	This configures the operation mode of the AP. The operator can select General AP, Root AP, or Repeater AP.
Location	This configures the installation location information of the AP.
IP Mode	This configures the IP configuration mode of the AP. The operator can select DHCP or AP Priority.
AP Status	This configures the up/down status of the AP.
Redundancy	If the APCs are configured for redundancy, this configures the discovery type and Primary/Secondary/Tertiary Controller settings of the AP.

The APC provides the overwrite option for each AP group setting. If the Overwrite option is enabled for each setting, the respective setting is applied to all APs within the group. For example, if the Overwrite option is enabled for AP Mode and AP Mode is set to General, all the APs within the group will run as General APs.

Configuration using CLI

To configure redundancy settings for the AP group, perform the following commands:

1) Go to configure mode of CLI.

```
WEC8500# configure terminal
WEC8500/configure#
```

2) Enter the AP Group configuration mode.
   - ap-group [AP_GROUP_NAME]

3) Enter the profile configuration mode for the AP group.
   - Profile

4) Configure the following AP group profiles:
   - description
   - overwrite-ap-mode
   - no overwrite-ap-mode
   - ap-mode
   - overwrite-location
   - no overwrite-location
   - location

- overwrite-ip-mode
- no overwrite-ip-mode
- ip-mode
- overwrite-state
- no overwrite-state
- shutdown
- no shutdown
- no overwrite-redundancy
- discovery
- primary-apc
- no primary-apc
- secondary-apc
- no secondary-apc
- tertiary-apc
- no tertiary-apc

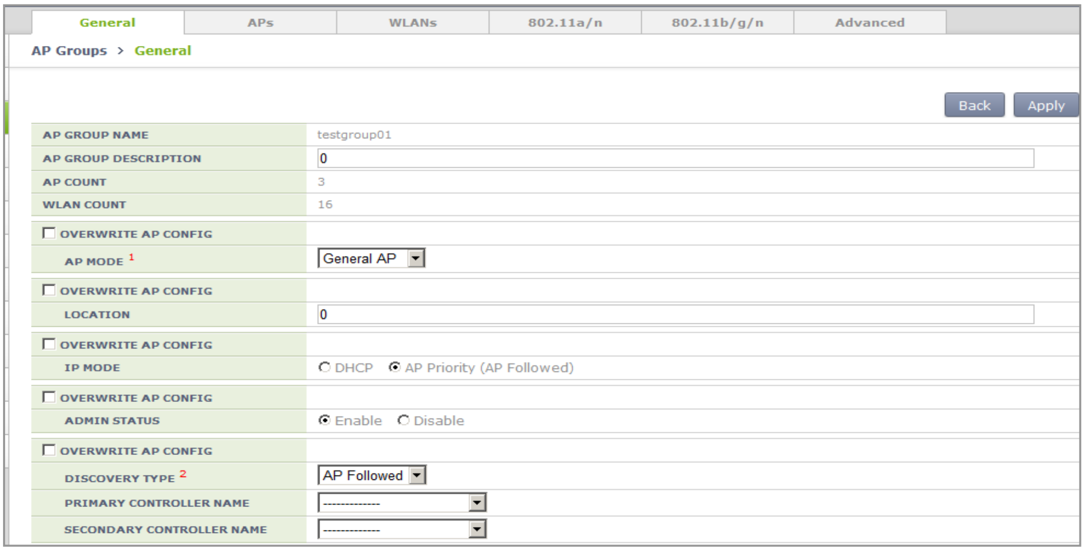
Parameter	Description
DESCRIPTION	This contains a brief description of the AP group.
OVERWRITE-AP-MODE	If overwrite-ap-mode is enabled, the AP mode information set for the group is applied to all APs within the group.
AP-MODE	This is the AP operation mode. The following modes are available: - generalAp: General operation mode. Default value. - rootAp: AP mode where a repeater AP can be connected. - repeasterAp: AP mode that is connected to a wireless area and the APC through the root AP.
OVERWRITE-LOCATION	If overwrite-location is enabled, the location information set for the group is applied to all APs within the group.
LOCATION	This is the location information of the AP.
OVERWRITE-IP-MODE	If overwrite-ip is enabled, the IP mode information set for the group is applied to all APs within the group.
IP-MODE	This is the mode of receiving an IP address by the AP. The following modes are available: - dhcp: The AP receives IP address allocation using DHCP. - ap: The AP uses a manually configured IP address.
OVERWRITE-STATE	If overwrite-state is enabled, the AP state information set for the group is applied to all APs within the group.
shutdown	This sets the AP state to UP or DOWN.
OVERWRITE-REDUNDANCY	If overwrite-redundancy is enabled, the redundancy setting (primary-apc, secondary-apc, tertiary-apc) of the AP group is applied to all APs within the group.
DISCOVERY	If the APCs are configured for redundancy, this configures the method used for APs to connect to the APC. The following modes are available: - ap-followed: The discovery type and discovery list configured for the

Parameter	Description
	AP are used. - apc-referral: The APC list configured for the APC is used as the discovery list. - DHCP: The APC list information relayed by DHCP option 138 (IPv4) or option 52 (IPv6) is used as the discovery list. - auto: Discovery type is automatically changed by the AP for automatic connection to the APC.
PRIMARY-APC	This is the name of the primary APC server. The AP attempts to connect to this APC first.
SECONDARY-APC	This is the name of the secondary APC server. If the AP is unable to connect to the primary APC, the AP attempts to connect to this APC on its second connection attempt.
TERTIARY-APC	This is the name of the tertiary APC server. If the AP is unable to connect to the secondary APC, the AP attempts to connect to this APC on its third connection attempt. The WEC8050 model does not support Tertiary-APC.

5) Use the ‘show ap-group detail [AP_GROUP_NAME]’ command to check the AP group information.

Configuration using Web UI

In the menu bar of **<WEC Main Window>,** select **<Configuration>,** select <AP Groups> in the submenu, and then select an AP group to configure. In the ‘General’ tab of the AP group, configure the necessary settings. If the OVERWRITE AP CONFIG checkbox is selected, the respective setting is applied to all APs within the group.



AP GROUP NAME	testgroup01
AP GROUP DESCRIPTION	0
AP COUNT	3
WLAN COUNT	16
□ OVERWRITE AP CONFIG	
AP MODE [1]	General AP
□ OVERWRITE AP CONFIG	
LOCATION	0
□ OVERWRITE AP CONFIG	
IP MODE	○ DHCP ● AP Priority (AP Followed)
□ OVERWRITE AP CONFIG	
ADMIN STATUS	● Enable ○ Disable
□ OVERWRITE AP CONFIG	
DISCOVERY TYPE [2]	AP Followed
PRIMARY CONTROLLER NAME	--------------
SECONDARY CONTROLLER NAME	--------------

Figure 63. General Configuration Window for AP Group

4.2.1.1 Adding/Removing APs

To aid management of APs in groups, the APC allows addition/removal of APs to/from AP groups.

Configuration using CLI

1) Go to configure mode of CLI.

```
WEC8500# configure terminal
WEC8500/configure#
```

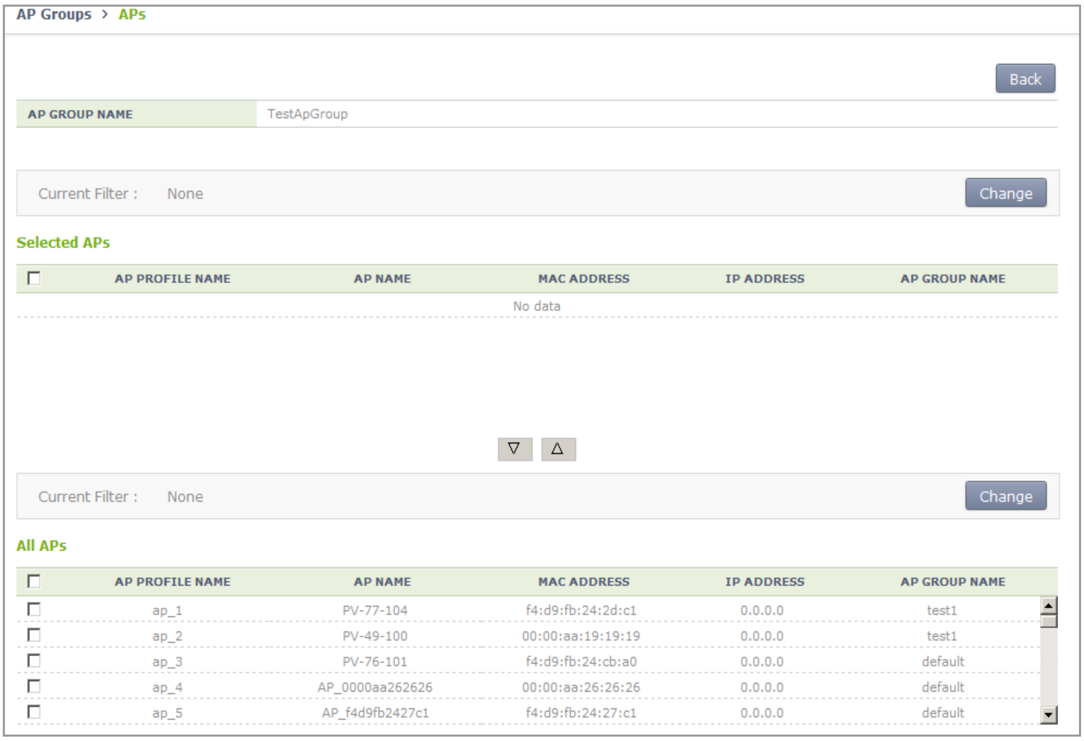
2) Create an AP group or enter the AP group configuration mode.
   - ap-group [AP_GROUP_NAME]

3) Add/remove an AP to/from the AP group. Use ‘no’ parameter in front of the command to delete an AP from the AP group. However, you cannot delete an AP from a default AP group. If you delete an AP from groups other than the default group, the deleted AP is then included in the default AP group.
   - add-ap [AP_NAME]
   - no add-ap [AP_NAME]

4) Use the ‘show ap-group summary’ command to check the AP group information.

Configuration using Web UI

In the menu bar of **<WEC Main Window>**, select **<Configuration>**, select **<AP Groups>** in the submenu, and then select an AP group to configure. Under the ‘APs’ tab of the AP group, APs can be added or removed.



AP GROUP NAME	TestApGroup

Current Filter : None [Change]

Selected APs

□	AP PROFILE NAME	AP NAME	MAC ADDRESS	IP ADDRESS	AP GROUP NAME
			No data		

Current Filter : None [Change]

All APs

□	AP PROFILE NAME	AP NAME	MAC ADDRESS	IP ADDRESS	AP GROUP NAME
□	ap_1	PV-77-104	f4:d9:fb:24:2d:c1	0.0.0.0	test1
□	ap_2	PV-49-100	00:00:aa:19:19:19	0.0.0.0	test1
□	ap_3	PV-76-101	f4:d9:fb:24:cb:a0	0.0.0.0	default
□	ap_4	AP_0000aa262626	00:00:aa:26:26:26	0.0.0.0	default
□	ap_5	AP_f4d9fb2427c1	f4:d9:fb:24:27:c1	0.0.0.0	default

Figure 64. AP Add/Remove Window for AP Group

4.2.1.2 Adding/Removing WLANs

To allows the same WLAN services to be provided to the APs allocated to each group, the APC allows addition/removal of WLANs to/from each AP group.

Configuration using CLI

1) Go to configure mode of CLI.

```
WEC8500# configure terminal
WEC8500/configure#
```

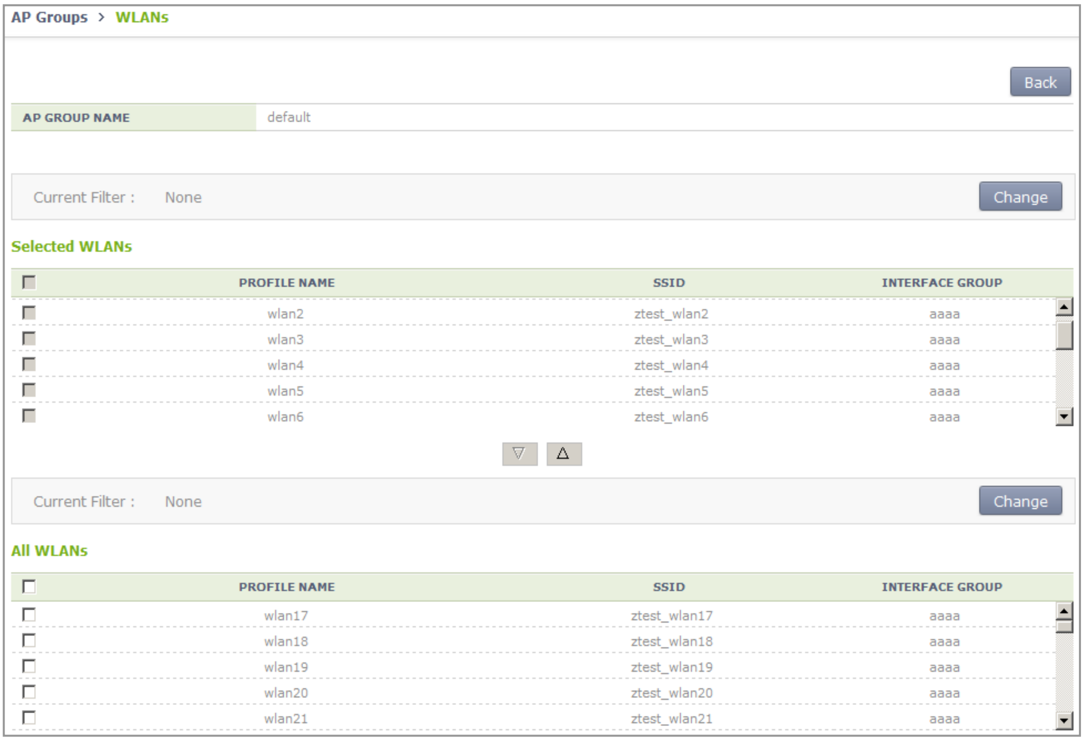
2) Create an AP group or enter the AP group configuration mode.
   - ap-group [AP_GROUP_NAME]

3) Add/remove an WLAN to/from the AP group. Use ‘no’ parameter in front of the command to delete an WLAN from the AP group.
   - add-wlan [WLAN_ID]
   - no add-wlan [WLAN_ID]

4) Use the ‘show ap-group summary’ command to check the AP group information.

Configuration using Web UI

In the menu bar of <**WEC Main Window**>, select <**Configuration**>, select <**AP Groups**> in the submenu, and then select an AP group to configure. Under the ‘WLANs’ tab of the AP group, WLANs can be added or removed.



AP GROUP NAME: default

Current Filter : None

Selected WLANs

□	PROFILE NAME	SSID	INTERFACE GROUP
□	wlan2	ztest_wlan2	aaaa
□	wlan3	ztest_wlan3	aaaa
□	wlan4	ztest_wlan4	aaaa
□	wlan5	ztest_wlan5	aaaa
□	wlan6	ztest_wlan6	aaaa

Current Filter : None

All WLANs

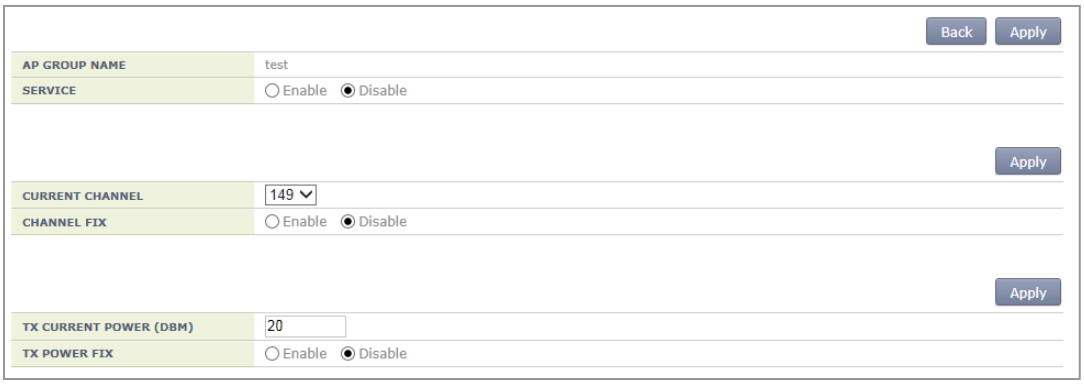
□	PROFILE NAME	SSID	INTERFACE GROUP
□	wlan17	ztest_wlan17	aaaa
□	wlan18	ztest_wlan18	aaaa
□	wlan19	ztest_wlan19	aaaa
□	wlan20	ztest_wlan20	aaaa
□	wlan21	ztest_wlan21	aaaa

Figure 65. WLAN Add/Remove Window for AP Group

4.2.1.3 802.11a/n Configuration

Configuration using Web UI

In the menu bar of <**WEC Main Window**>, select <**Configuration**>, select <**AP Groups**> in the submenu, and then select an AP group to configure. Settings can be configured under the ‘802.11a/n’ tab of the AP group.



AP GROUP NAME	test
SERVICE	○ Enable ● Disable

CURRENT CHANNEL	149
CHANNEL FIX	○ Enable ● Disable

TX CURRENT POWER (DBM)	20
TX POWER FIX	○ Enable ● Disable

Figure 66. 802.11a/n Window for AP Group

The configuration items are as follows:

[Service Configuration of AP Group]

- SERVICE: Enable or disable the radio service.

[Channel Configuration]

- CURRENT CHANNEL: Channel configuration (range: 36-165)
- CHANNEL FIX: The configured channel is configured as fixed and it is not affected by automatic adjustment functions such as RRM. When the <**Monitor**> → <**Access Points**> → <**Radio**> → <**802.11a/n/ac**> menu is selected, the channel value is shown as * (optional).

[TX Power Setting]

- TX CURRENT POWER: TX power (range: 3-23)
- TX POWER FIX: The configured TX power is configured as fixed and it is not affected by automatic adjustment functions such as RRM. When the <**Monitor**> → <**Access Points**> → <**Radio**> → <**802.11a/n/ac**> menu is selected, the TxPower value is shown as * (optional).

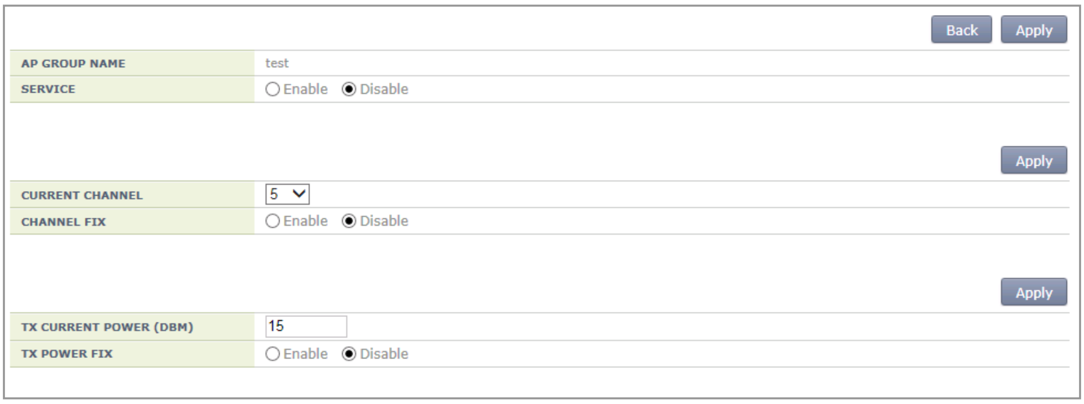
NOTE

To check the configured channel and TX power information, go to **<Monitor>** → **<Access Points>** → **<Radio>** → **<802.11a/n/ac>**.

4.2.1.4 802.11b/g/n Configuration

Configuration using Web UI

In the menu bar of <**WEC Main Window**>, select <**Configuration**>, select <**AP Groups**> in the submenu, and then select an AP group to configure. Settings can be configured under the '802.11b/g/n' tab of the AP group.



AP GROUP NAME	test
SERVICE	○ Enable ● Disable
CURRENT CHANNEL	5
CHANNEL FIX	○ Enable ● Disable
TX CURRENT POWER (DBM)	15
TX POWER FIX	○ Enable ● Disable

Figure 67. 802.11b/g/n Window for AP Group

The configuration items are as follows:

[Service Configuration of AP Group]

- SERVICE: Enable or disable the radio service.

[Channel Configuration]

- CURRENT CHANNEL: Channel configuration (range: 1-14)
- CHANNEL FIX: The configured channel is configured as fixed and it is not affected by automatic adjustment functions such as RRM. When the <**Monitor**> → <**Access Points**> → <**Radio**> → <**802.11b/g/n**> menu is selected, the channel value is shown as * (optional).

[TX Power Setting]

- TX CURRENT POWER: TX power (range: 3-23)
- TX POWER FIX: The configured TX power is configured as fixed and it is not affected by automatic adjustment functions such as RRM. When the <**Monitor**> → <**Access Points**> → <**Radio**> → <**802.11b/g/n**> menu is selected, the TxPower value is shown as * (optional).

NOTE

To check the configured channel and TX power information, go to **<Monitor>** → **<Access Points>** → **<Radio>** → **<802.11b/g/n>**.

4.2.1.5 Advanced Configuration

In order to provide the same services to the APs allocated to each group, the APC allows configuration of advanced settings for each AP group.

Configuring AP Group Profile with CLI

1) Go to configure mode of CLI.

```
WEC8500# configure terminal
WEC8500/configure#
```

2) Create an AP group or enter the AP group configuration mode.
   - ap-group [AP_GROUP_NAME]

3) Enter the profile configuration mode for the AP group.
   - profile

4) Configure the following AP group profiles:
   - overwrite-apc-ap-timer
   - no overwrite-apc-ap-timer
   - echo-interval
   - discovery-interval
   - report-interval
   - statistics-timer
   - retransmit-interval
   - echo-retransmit-interval
   - max-echo-retransmit
   - overwrite-telnet-ssh
   - no overwrite-telnet-ssh
   - telnet-enable
   - no telnet-enable
   - ssh-enable
   - no ssh-enable
   - overwrite-console
   - no overwrite-console
   - console-enable
   - no console-enable
   - overwrite-dtls
   - no overwrite-dtls
   - dtls-policy
   - overwrite-led-control
   - no overwrite-led-control
   - led-config

- overwrite-vlan
- no overwrite-vlan
- vlan-support
- no vlan-support
- native-vlanId
- no native-vlanId

Parameter	Description
DESCRIPTION	This contains a brief description of the AP group.
OVERWRITE-APC-AP-TIMER	If overwrite-apc-ap-timer is enabled, the APC-AP timer setting of the group is applied to all APs within the group.
ECHO-INTERvAL	Configures the time when an echo request message is transmitted to the APC where an AP joins (unit: seconds).
DISCOVERY-INTERVAL	Configures a waiting time until the CAPWAP discovery response message is received (unit: seconds).
REPORT-INTERVAL	Configures the time interval for transmitting the description error from AP to the APC (unit: seconds).
STATISTICS-TIMER	Configures the time interval for transmitting the statistical information provided by the CAPWAP (unit: seconds).
RETRANSMIT-INTERVAL	The APC waits for this length of time before retransmitting an echo request message when there is no response. The APC sets double the length of echo-interval as the echo timeout time. If no echo message is received from the AP for as long as double the length of the echo-interval, the APC judges that the AP is down (unit: seconds).
MAX-ECHO-RETRANSMIT	The APC waits for this length of time before retransmitting an echo request message when there is no response. The APC sets double the length of echo-interval as the echo timeout time. If no echo message is received from the AP for as long as double the length of the echo-interval, the APC judges that the AP is down (unit: seconds).
OVERWRITE-TELNET-SSH	If overwrite-telnet-ssh is enabled, the telnet and SSH settings for the AP group are applied to all APs within the group.
TELNET-ENABLE	This enables the telnet server and configures telnet port of the AP.
SSH-ENABLE	This enables the SSH server and configures SSH port of the AP.
OVERWRITE-CONSOLE	If overwrite-console is enabled, the telnet and SSH settings of the AP group are applied to all APs within the group.
CONSOLE-ENABLE	This configures whether to allow console access to the AP.
OVERWRITE-DTLS	If overwrite-dtls is enabled, the DTLS settings of the AP group are applied to all APs within the group.
DTLS-POLICY	Configures the DTLS Policy of an AP.
OVERWRITE-LED-CONTROL	If overwrite-led-control is enabled, the LED settings of the AP

Parameter	Description
	group are applied to all APs within the group.
LED-CONFIG	This configures whether to turn the LED on/off.
OVERWRITE-VLAN	If overwrite-vlan is enabled, the VLAN settings of the AP group are applied to all APs within the group.
VLAN-SUPPORT	This configures whether to enable the native VLAN of the AP.
NATIVE-VLANID	This configures the native VLAN value of the AP.

5) Use the ‘show ap-group detail [AP_GROUP_NAME]’ command to check the AP group information.

Configuring AirMove Service of AP Group with CLI

1) Go to configure mode of CLI.

```
WEC8500# configure terminal
WEC8500/configure#
```

2) Create an AP group or enter the AP group configuration mode.
   - ap-group [AP_GROUP_NAME]

3) Enter the profile configuration mode for the AP group.
   - profile

4) Configure the AirMove service of the AP group.
   - enable: Enables/disables the AirMove service.
   - target-ap: This option is used for selecting APs which will be applied with the changes made to the group settings. If 'all' is selected, changes are applied to all APs and config priority of the APs also change to group. If 'keep-ap-config' is selected, only the APs whose config priority is set to group have the airmove value of the group applied to them.

```
WEC8500# configure terminal
WEC8500/configure# ap-group default
GroupName : default
WEC8500/configure/ap-group default# airmove
WEC8500/configure/ap-group default/airmove# ?
     decision-delta         Set delta value for handover decision
     enable                 Airmove enable
     exit                   Exit from airmove mode
     number-of-channel      Set the number of channel required during
one time scanning
     number-of-proreq       Set the number of probe request required
during one time scanning
```

```
     scan-time-channel      Set time required for one channel scanning
     scan-time-interleave   Set interval time required for new scanning
start
     scan-time-service      Set time required for STA service during
STA’s scanning
     scan-trigger-level     Set a trigger level for STA's scanning
start
     target-ap              Set config target ap
     <cr>
WEC8500/configure/ap-group default/airmove# enable ?
  <cr>
WEC8500/configure/ap-group default/airmove# decision-delta ?
  1 - 100                   Enter the value [dBm]

WEC8500/configure/ap-group default/airmove# number-of-channel ?
  1 - 20                    Enter the number
WEC8500/configure/ap-group default/airmove# number-of-proreq ?
  1 - 10                      Enter the number

WEC8500/configure/ap-group default/airmove# scan-time-channel ?
  0 - 100                   Enter the time [ms]

WEC8500/configure/ap-group default/airmove# scan-time-interleave ?
  1000 - 10000              Enter the time [ms]

WEC8500/configure/ap-group default/airmove# scan-time-service ?
  1 - 1000                  Enter the time [ms]

WEC8500/configure/ap-group default/airmove# scan-trigger-level ?
  -128 - 0                  Enter the trigger level [dBm]

WEC8500/configure/ap-group default/airmove# target-ap ?
  all                       All
  keep-ap-config            Keep ap config
WEC8500/configure/ap-group default/airmove# end
```

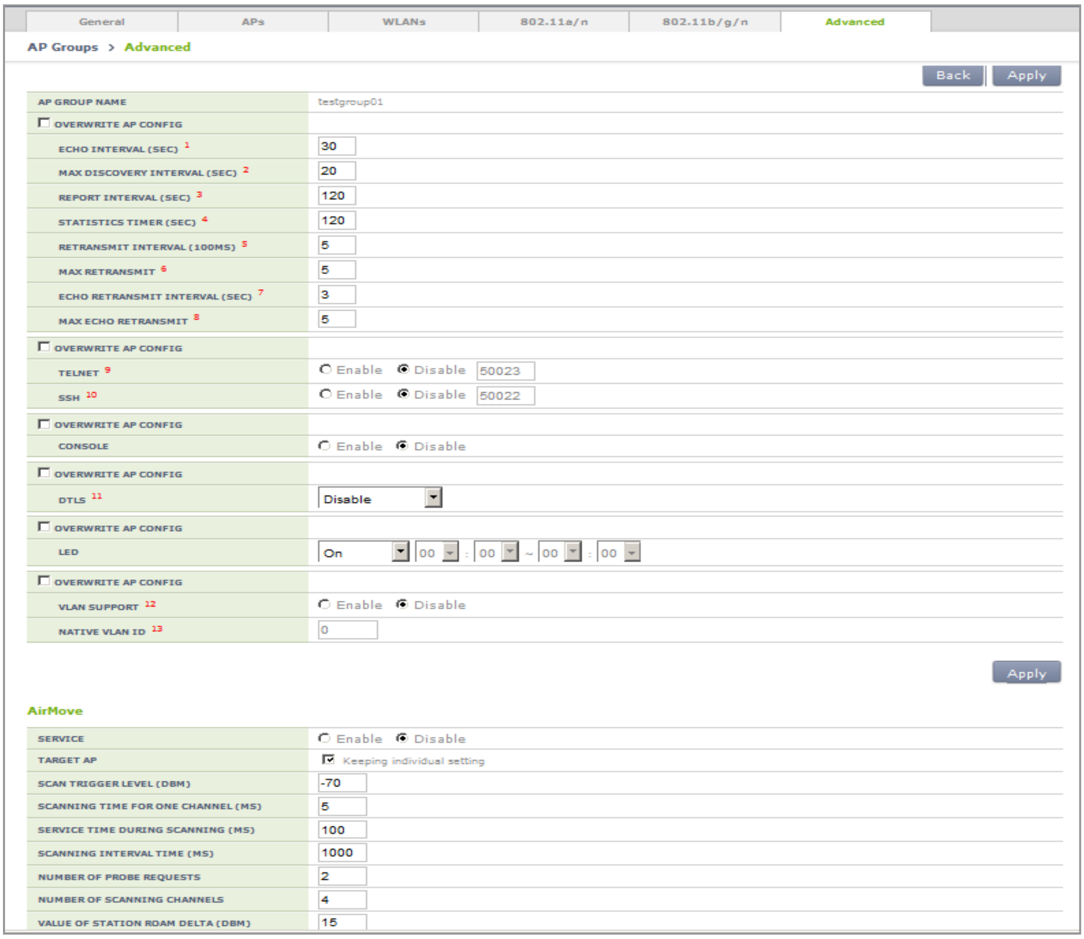
4) Use the ‘show airmove group [ap_group_name]’ command to check the AP group information.

```
WEC8500# show airmove group default

Airmove Group Configurations
----------------------------
   Airmove State                      Disable
   Target AP                          Keep Ap Config
   Scan trigger level                 -70 dBm
   Scanning time for one channel      5 ms
```

```
    Service time during scanning       100 ms
    Scanning interval time             1000 ms
    Number of probe requests           2
    Number of scanning channels        4
    Value of station roam delta        15
WEC8500#
```

Configuration using Web UI

In the menu bar of **<WEC Main Window>**, select **<Configuration>**, select **<AP Groups>** in the submenu, and then select an AP group to configure. Advanced settings and AirMove settings of the AP group can be changed under the ‘Advanced’ tab of AP Group.



AP GROUP NAME	testgroup01
□ OVERWRITE AP CONFIG	
ECHO INTERVAL (SEC) [1]	30
MAX DISCOVERY INTERVAL (SEC) [2]	20
REPORT INTERVAL (SEC) [3]	120
STATISTICS TIMER (SEC) [4]	120
RETRANSMIT INTERVAL (100MS) [5]	5
MAX RETRANSMIT [6]	5
ECHO RETRANSMIT INTERVAL (SEC) [7]	3
MAX ECHO RETRANSMIT [8]	5
□ OVERWRITE AP CONFIG	
TELNET [9]	○ Enable ● Disable 50023
SSH [10]	○ Enable ● Disable 50022
□ OVERWRITE AP CONFIG	
CONSOLE	○ Enable ● Disable
□ OVERWRITE AP CONFIG	
DTLS [11]	Disable
□ OVERWRITE AP CONFIG	
LED	On 00 : 00 ~ 00 : 00
□ OVERWRITE AP CONFIG	
VLAN SUPPORT [12]	○ Enable ● Disable
NATIVE VLAN ID [13]	0

AirMove

SERVICE	○ Enable ● Disable
TARGET AP	☑ Keeping individual setting
SCAN TRIGGER LEVEL (DBM)	-70
SCANNING TIME FOR ONE CHANNEL (MS)	5
SERVICE TIME DURING SCANNING (MS)	100
SCANNING INTERVAL TIME (MS)	1000
NUMBER OF PROBE REQUESTS	2
NUMBER OF SCANNING CHANNELS	4
VALUE OF STATION ROAM DELTA (DBM)	15

Figure 68. Advanced Configuration Window for AP Group

4.2.2 Configuring Remote AP Group

If the APs are located in an area where the APC is not located, those APs must be classified into a separate group for service. The APC can manage the APs in another area by grouping them into a remote AP group.

In the Remote AP group menu, operator can configure the below information and the APs in the Remote AP group are operating based on the same configuration.

- Remote AP Addition/Removal
  - APs can be added to/removed from a remote AP group.
- Local Authentication
  - Radius Server
    The Radius server which authenticates stations accessing the remote AP can be configured.
  - Remote AP User List
    Users (stations) to be managed by the remote AP can be added/removed.

If an AP is added to or deleted from a remote AP group, the AP is rebooted and reconnected to the APC. If an AP moves between remote AP groups, the AP is not rebooted.

If an AP is added to a remote AP group, the WLAN and default configuration of AP is not changed from the policy configured in the AP group.

4.2.2.1 Addition/Removal Setting

Configuration using CLI

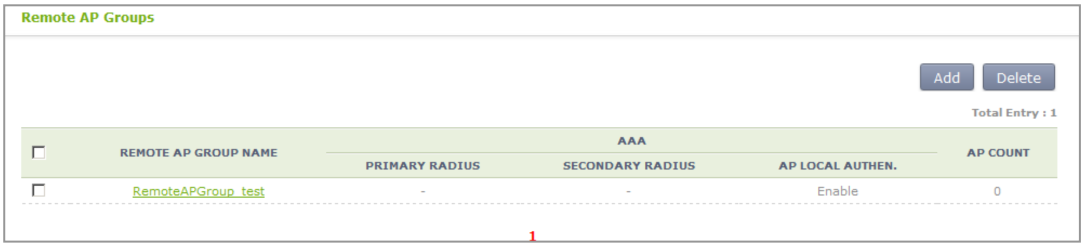
1) Go to configure mode of CLI.

```
WEC8500# configure terminal
WEC8500/configure#
```

2) Create or delete a remote AP group. To delete a remote AP group, enter ‘no’ parameter in front of the command
   - remote-ap-group [REMOTE_AP_GROUP_NAME]
   - no remote-ap-group [REMOTE_AP_GROUP_NAME]

Configuration using Web UI

In the menu bar of **<WEC Main Window>**, select **<Configuration>** and then select the **<Remote AP Groups>** menu in the sub-menus. Click the **<Add>** or **<Delete>** button to add or delete a group.



□	REMOTE AP GROUP NAME	AAA			AP COUNT
		PRIMARY RADIUS	SECONDARY RADIUS	AP LOCAL AUTHEN.	
□	RemoteAPGroup_test	-	-	Enable	0

Figure 69. Remote AP Group Add/Remove Window

4.2.2.2 AP Addition/Removal Configuration for Remote AP Group

To aid management of remote APs in groups, the APC allows addition/removal of APs to/from AP groups.

Configuration using CLI

1) Go to configure mode of CLI.

```
WEC8500# configure terminal
WEC8500/configure#
```

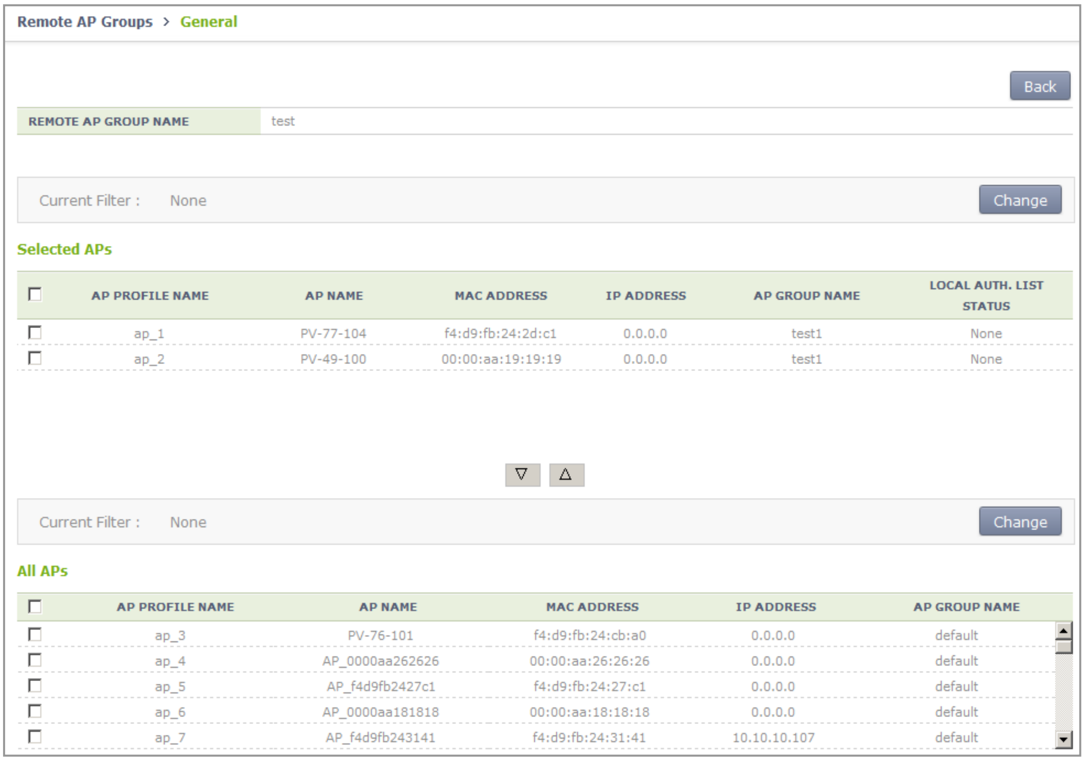
2) Create or delete a remote AP group. To delete a remote AP group, enter ‘no’ parameter in front of the command
   - remote-ap-group [REMOTE_AP_GROUP_NAME]
   - no remote-ap-group [REMOTE_AP_GROUP_NAME]

3) Add or delete an AP to or from a remote AP group. To delete an AP from the remote AP group, enter ‘no’ parameter in front of the command. The Region value of an AP added to a remote AP group is automatically changed to Remote and it is automatically re-connected to the APC. If an AP is deleted from a remote AP group, the Region value is changed to Local and the AP is re-connected to the APC.
   - add-ap [AP_NAME]
   - no add-ap [AP_NAME]

4) Use the ‘show remote-ap-group summary’ command to check the AP group information.

Configuration using Web UI

In the menu bar of **<WEC Main Window>**, select **<Configuration>**, select **<Remote AP Groups>** in the submenu, and then select a remote AP group to configure. Under the ‘General’ tab of the remote AP group, APs can be added or removed.



REMOTE AP GROUP NAME	test

Current Filter : None

Selected APs

□	AP PROFILE NAME	AP NAME	MAC ADDRESS	IP ADDRESS	AP GROUP NAME	LOCAL AUTH. LIST STATUS
□	ap_1	PV-77-104	f4:d9:fb:24:2d:c1	0.0.0.0	test1	None
□	ap_2	PV-49-100	00:00:aa:19:19:19	0.0.0.0	test1	None

Current Filter : None

All APs

□	AP PROFILE NAME	AP NAME	MAC ADDRESS	IP ADDRESS	AP GROUP NAME
□	ap_3	PV-76-101	f4:d9:fb:24:cb:a0	0.0.0.0	default
□	ap_4	AP_0000aa262626	00:00:aa:26:26:26	0.0.0.0	default
□	ap_5	AP_f4d9fb2427c1	f4:d9:fb:24:27:c1	0.0.0.0	default
□	ap_6	AP_0000aa181818	00:00:aa:18:18:18	0.0.0.0	default
□	ap_7	AP_f4d9fb243141	f4:d9:fb:24:31:41	10.10.10.107	default

Figure 70. AP Add/Remove Window for Remote AP Group

4.2.2.3 Local Authentication Configuration for Remote AP Group

Users (stations) accessing the remote AP and the Radius server which authenticates such users can be configured.

Configuration using CLI

Perform the following commands to configure local authentication settings of the remote AP group:

1) Go to configure mode of CLI.

```
WEC8500# configure terminal
WEC8500/configure#
```

2) Create or delete a remote AP group. To delete a remote AP group, enter ‘no’ parameter in front of the command
   - remote-ap-group [REMOTE_AP_GROUP_NAME]

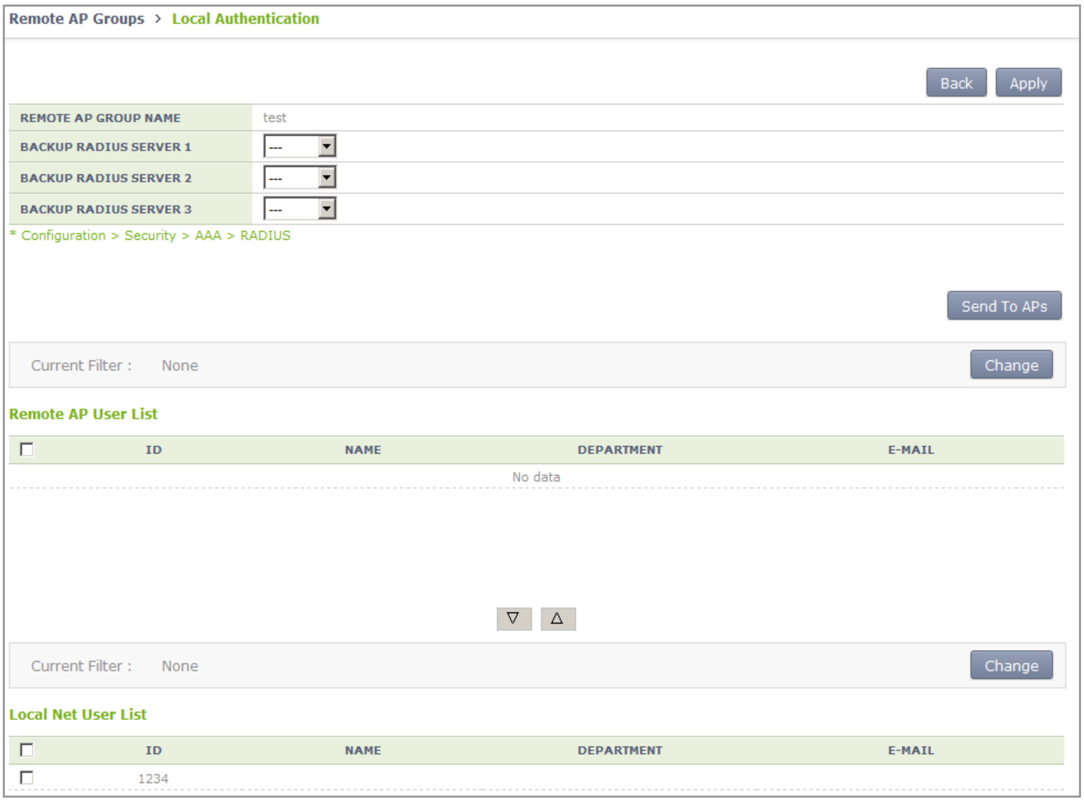
- no remote-ap-group [REMOTE_AP_GROUP_NAME]

3) Configure Primary Radius Server 1, Primary Radius Server 2, and Primary Radius Server 3. The RADIUS server information must be created in the radius of the security item in advance. To delete the configured RADIUS server information, enter ‘no’ parameter in front of the command.
   - primary-radius [RADIUS_SERVER_INDEX]
   - no primary-radius [RADIUS_SERVER_INDEX]
   - secondary-radius [RADIUS_SERVER_INDEX]
   - no secondary-radius [RADIUS_SERVER_INDEX]
   - tertiary-radius [RADIUS_SERVER_INDEX]
   - no tertiary-radius [RADIUS_SERVER_INDEX]

4) Use the ‘show remote-ap-group detail [REMOTE AP GROUP NAME]’ command to check the remote AP group information.

Configuration using Web UI

In the menu bar of **<WEC Main window>**, select **<Configuration>** and then select the **<Remote AP Groups>** menu in the sub-menus. After selecting the name of a remote AP group, you can configure the Radius server or add/remove users under the ‘Local Authentication’ tab.



REMOTE AP GROUP NAME	test
BACKUP RADIUS SERVER 1	---
BACKUP RADIUS SERVER 2	---
BACKUP RADIUS SERVER 3	---

* Configuration > Security > AAA > RADIUS

Current Filter : None

Remote AP User List

□	ID	NAME	DEPARTMENT	E-MAIL
		No data		

Current Filter : None

Local Net User List

□	ID	NAME	DEPARTMENT	E-MAIL
□	1234			

Figure 71. Local Authentication Configuration Window for Remote AP Group

4.2.2.4 Role-based Access Control Configuration of Remote AP Group

If the remote AP is running in local switching mode, the ACL settings between the APC and the AP must be synchronized. The ACL settings are automatically synchronized when the AP capwap runs. However, if the operator changes ACL of the APC, the ACL settings must be synchronized as shown below.

Configuration using CLI

Perform the following commands to synchronize the settings for APs of all remote groups:

```
WEC8500# configure terminal
WEC8500/configure# rbac
WEC8500/configure/rbac# sync-config
```

Perform the following commands to synchronize the settings for APs of a specific remote group:

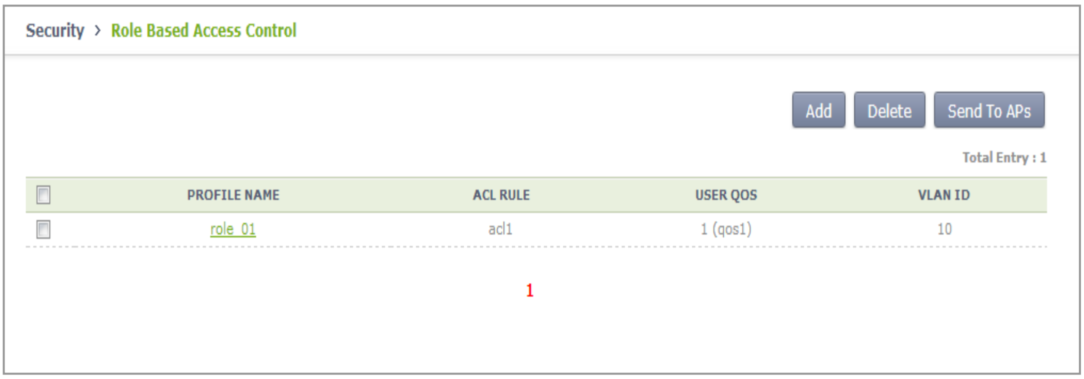
```
WEC8500# configure terminal
WEC8500/configure# remote-ap-group rmt_grp_01
WEC8500/configure/remote-ap-group rmt_grp_01# sync-rbac-config
```

Synchronization result can be checked as shown below.

```
WEC8500# show rbac config summary

 GRP_ID  GRP_NAME  Role Config File Name
 ====== ========= ==========================
     1     rmt_grp_01
etc/rmtapgrp/rbac_cfg_rmtapgrp1_20140307101643076655.tar
     2     rmt_grp_02   etc/rmtapgrp/rbac_cfg_20140305094752849046.tar
```

Configuration using Web UI

Configuration > Security > Role Based Access Control → ‘Send To Aps’

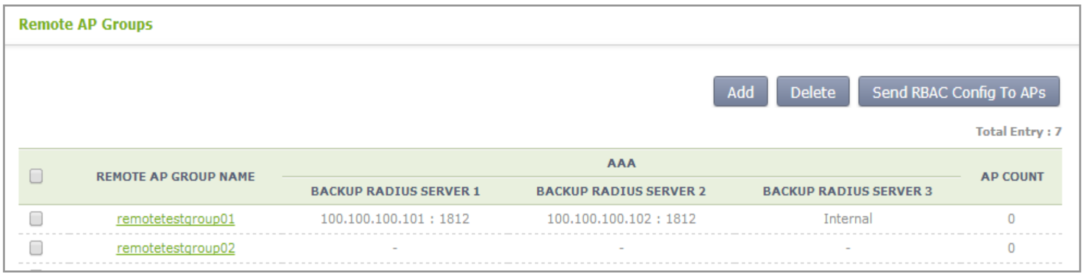


Total Entry : 1

□	PROFILE NAME	ACL RULE	USER QOS	VLAN ID
□	role_01	acl1	1 (qos1)	10

Figure 72. ACL Settings Synchronization-All

Configuration > Remote AP Groups
→ select remote ap group & ‘Send RBAC Config To Aps’



Total Entry : 7

□	REMOTE AP GROUP NAME	AAA			AP COUNT
		BACKUP RADIUS SERVER 1	BACKUP RADIUS SERVER 2	BACKUP RADIUS SERVER 3	
□	remotetestgroup01	100.100.100.101 : 1812	100.100.100.102 : 1812	Internal	0
□	remotetestgroup02	-	-	-	0

Figure 73. ACL Settings Synchronization-Remote Group

4.2.3 AP Time Synchronization per Group

The AP can configure its time information using either the time stamp method or the NTP method.

In the Time Stamp type, the APC periodically transmits the time of APC to an AP and the AP is operating based on the received time. Unless a user changes the configuration, the default is Time Stamp type and the interval is set to 7200 seconds (2 hours).

In the NTP type, the NTP server information is transmitted to an AP and the AP synchronizes the time with the NTP server. A NTP server list must be created to transmit the NTP server information to an AP and maximum 10 lists can be added. The ntp-interval (2^N) is the interval when an AP receives the time information from the NTP server.
For example, if the ntp-interval is set to 6, an AP receives the time information from the NTP server at every 2^6, i.e. 128 seconds.

The APC provides a function for configuring the time configuration method of the AP.

Configuring Time Stamp type using CLI

1) Go to configure → apc → ap-time-config configuration mode of CLI.

```
WEC8500# configure terminal
WEC8500/configure# apc
WEC8500/configure/apc# ap-time-config
WEC8500/configure/apc/ap-time-config#
```

2) Configure how to transmit the time information to an AP using ‘ac-stamp’ and configure the interval.
   - mode ac-stamp
   - ac-stamp-interval [INTERVAL]

3) To check the information, execute the ‘show apc ap-time-config’ command.

Configuring NTP type using CLI

1) Go to configure → apc → ap-time-config configuration mode of CLI.

```
WEC8500# configure terminal
WEC8500/configure# apc
WEC8500/configure/apc# ap-time-config
WEC8500/configure/apc/ap-time-config#
```

2) Add the NTP server information to transmit to an AP. Maximum 10 NTP server information can be added. To delete the configured NTP server information, enter ‘no’ parameter in front of the command

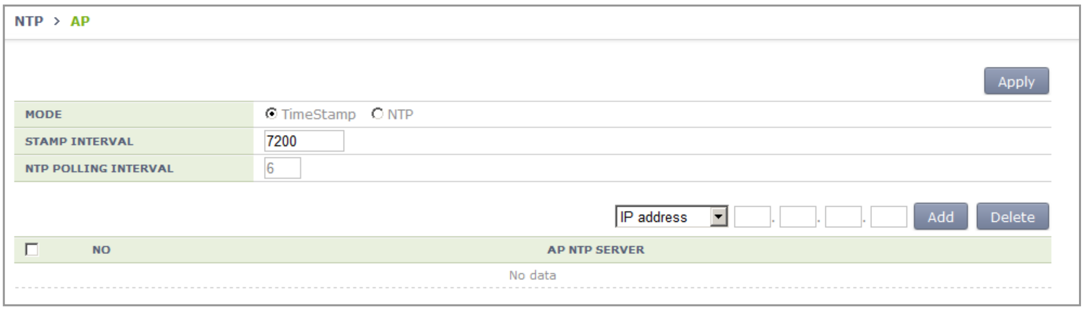
- add-ntp [NTP_SERVER_ADDRESS]
- no add-ntp [NTP_SERVER_ADDRESS]
- ntp-interval [NUMBER]

3) Configure the method of transmitting the time information to an AP as ‘ntp’.
    - mode ntp

4) Use the ‘show apc ap-time-config’ command to check the configured information.

Configuration using Web UI

In the menu bar of **<WEC Main Window>**, select **<Configuration>**, select **<NTP>** in the submenu, and then select a time setting mode of the AP (TimeStamp or NTP), timestamp interval, and NTP polling interval. Also, you can add/remove NTP server from which to fetch time access information for the AP.



NTP > AP

MODE	● TimeStamp ○ NTP
STAMP INTERVAL	7200
NTP POLLING INTERVAL	6

□	NO	AP NTP SERVER
		No data

Figure 74. AP Time Synchronization Configuration Options

4.2.4 AP Configuration

NOTE

The management interface of APC must be configured for the connection between APC and W-EP AP.

4.2.4.1 Configuring MAC address

Configuration using CLI

To configure AP information, execute the command as follows:

1) Go to configure → AP configuration mode of CLI.

```
WEC8500# configure terminal
WEC8500/configure# ap [ap profile name]
WEC8500/configure/ap ap_1#
```

If there exists the same AP when entering [ap profile name], you are guided to the mode where operator can configure the AP. If there is no same AP, the new AP information is created.

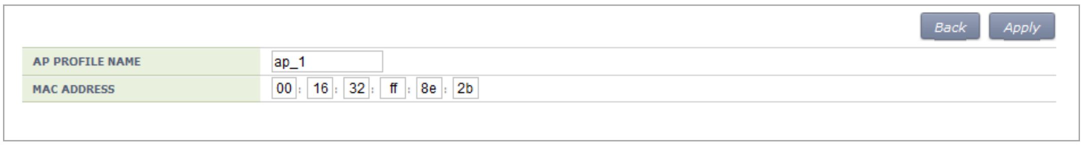
2) Register the MAC address of the AP.
   - profile mac [MAC_ADDRESS]

3) To check the information of a configured AP, use the 'show ap summary config' command.

Configuration using Web UI

In the menu bar of <**WEC Main window**>, select <**Configuration**> and then select the <**Access Points**> menu in the sub-menus.

1) Click the <**Add**> button.
2) Set AP PROFILE NAME and MAC ADDRESS and click the <**Apply**> button.



AP PROFILE NAME	ap_1
MAC ADDRESS	00 : 16 : 32 : ff : 8e : 2b

Figure 75. Adding Access Points

4.2.4.2 Configuring AP Profile

Configuration using CLI

To configure an AP profile configuration, execute the command as follows:

1) Go to configure → AP configuration → AP profile mode of CLI.

```
WEC8500# configure terminal
WEC8500/configure# ap ap_1
WEC8500/configure/ap ap_1# profile
WEC8500/configure/ap ap_1/profile#
```

2) Configure the profile of an AP using the below command.
   - name [STRING]: Configures the name of an AP. If it is not entered, the 'AP_' + 'MAC address' is used as a name.
     E.g. MAC address: f4:d9:fb:24:cb:a0
     AP name: AP_f4d9fb24cba0
   - ap-mode [generalAp/rootAp/repeaterAp/snifferAp]: Configures the AP operation mode.
   - ap-stats-history-enable: Configures whether to enable the AP statistics history.
   - client-ip [IP_ADDRESS]: Configures the client IP address, if the AP operation mode is set to Sniffer AP.
   - console-enable: This configures whether to allow console access to the AP.
   - discovery [ap-followed/apc-referal/multicast/broadcast/DHCP]: Configures the discovery type of an AP to find APC.
     - ap-followed: Finds the APC using the discovery type and discovery list configured in an AP.
     - apc-referal: Uses the APC list information configured in an APC as the discovery list
     - DHCP: Uses the APC list information that is received through DHCP option 138 (IPv4) or option 52 (IPv6) as the discovery list.
     - auto: Discovery type is automatically changed by the AP for automatic connection to the APC.
   - discovery-interval [INTERVAL]: Configures the time waiting for a CAPWAP discovery response message (unit: seconds)
   - dtls-policy: Configures the DTLS Policy of an AP.
   - echo-interval [INTERVAL]: Configures the time when an AP transmits an echo request to the joined APC (Unit: seconds)
   - echo-retransmit-interval [INTERVAL]: Waiting time to retransmit an echo request message if there is no reply. The APC configures the echo timeout as much as two times of echo-interval. If the APC cannot receive an echo message from an AP until two times of echo-interval is elapsed, the APC assumes that the AP is down (Unit: seconds)

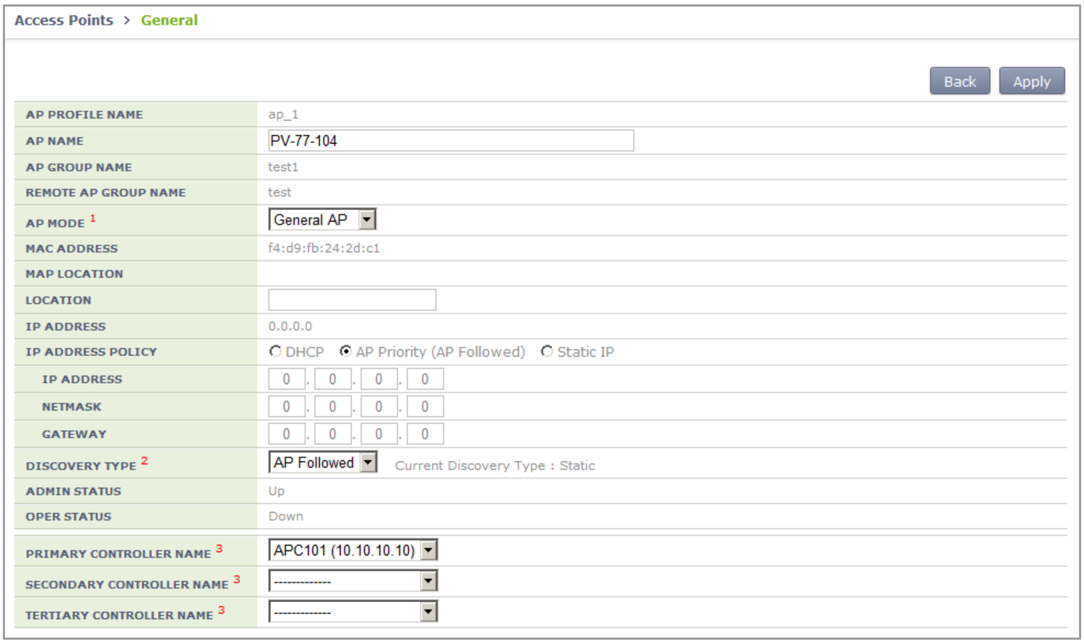
- edge-ap: Configures whether to enable the Edge AP function.
- edge-ap-opmode: Smart Handover is enabled as operation mode of the edge AP. In RSSI mode, handover is determined by looking up the RSSI value. In Force mode, handover is performed by force.
- edge-ap-threshold: Configures a threshold value for performing smart handover at the edge AP (range: -60 to -100 dBm, default: -80 dBm).
- edge-ap-window: Configures a window value for performing smart handover at the edge AP (range: 200-1000 ms, default: 200 ms).
- fragment-size [SIZE]: Configures a fragment size based on MTU to prevent the fragmentation of a CAPWAP packet that is transmitted by an AP to the APC.
- ip-mode [dhcp/static/ap]: Configures the IP address of an AP to DHCP, Static or AP Followed.
  - dhcp: Configures the AP IP operation type to DHCP
  - static: Configures the AP IP operation type to static
  - ap: Operates with an IP configured in an AP
- led-config: Configures LED on/off setting of the AP.
  - on: Sets LED of the AP on.
  - off: Sets LED of the AP off.
  - off-time: Sets LED of the AP off only for specific hours.
- local-bridging: Configures WLAN-VLAN Mapping of the Local Switching WLAN, ACL, and Pre-Authentication ACL of Captive Portal for each remote AP.
  - vlan-id: Configures a VLAN ID to allocate to the Local Switching WLAN.
  - acl-name: Configures an ACL name to allocate to the Local Switching WLAN for packet allowance/blocking.
  - pre-auth-name: Configures a Pre-Authentication ACL name for Captive Portal operation of the Local Switching WLAN.
- location [STRING]: Configures the information of location where an AP is installed.
- mac [MAC_ADDRESS]: Configures the MAC address of an AP
- max-echo-retransmit [COUNT]: Configures the maximum number of retransmission times of an echo request message.
- max-retransmit [COUNT]: Configures the maximum number of retransmission times of a CAPWAP control message.
- name [STRING]: Configures an AP name.
- native-vlanId [VLAN_ID]: Configures the native VLAN in an AP.
- primary-apc [APC_AME]: Configures the name of a primary APC.
- secondary-apc [APC_AME]: Configures the name of a secondary APC.
- tertiary-apc [APC_AME]: Configures the name of a tertiary APC. The WEC8050 model does not support the tertiary-apc function.
- repeater-whitelist [MAC ADDRESS]: Adds the Repeater AP Whitelist.
- report-interval [INTERVAL]: Configures the time interval for an AP to transmit the description error to the APC (Unit: seconds)
- retransmit-interval [INTERVAL]: Configures the waiting time until the AP retransmits a CAPWAP control message when there is no reply from the APC (unit: seconds)

- ssh-enable: Configures whether to enable the SSH server of an AP.
- static-ip [IP_ADDRESS] [NETMASK] [GATEWAY]: Configures the static IP address of an AP.
- statistics-timer [TIMER]: Configures the time interval of transmitting the statistics information provided by CAPWAP (unit: seconds)
- telnet-enable: Configures whether to enable the telnet server of an AP.
- time-config: Configure the timezone per AP.
- vlan-support: Configures whether to enable the native VLAN of an AP.

3) To check the information of a configured AP profile, use the ‘show ap detail [AP_NAME]’ command.

Configuration using Web UI

In the menu bar of <**WEC Main window**>, select <**Configuration**> and then select the <**Access Points**> → **AP selection** → <**General**> menu in the sub-menus.
The setting options in the General tab are as follows. Click the <**Apply**> button to apply the settings.



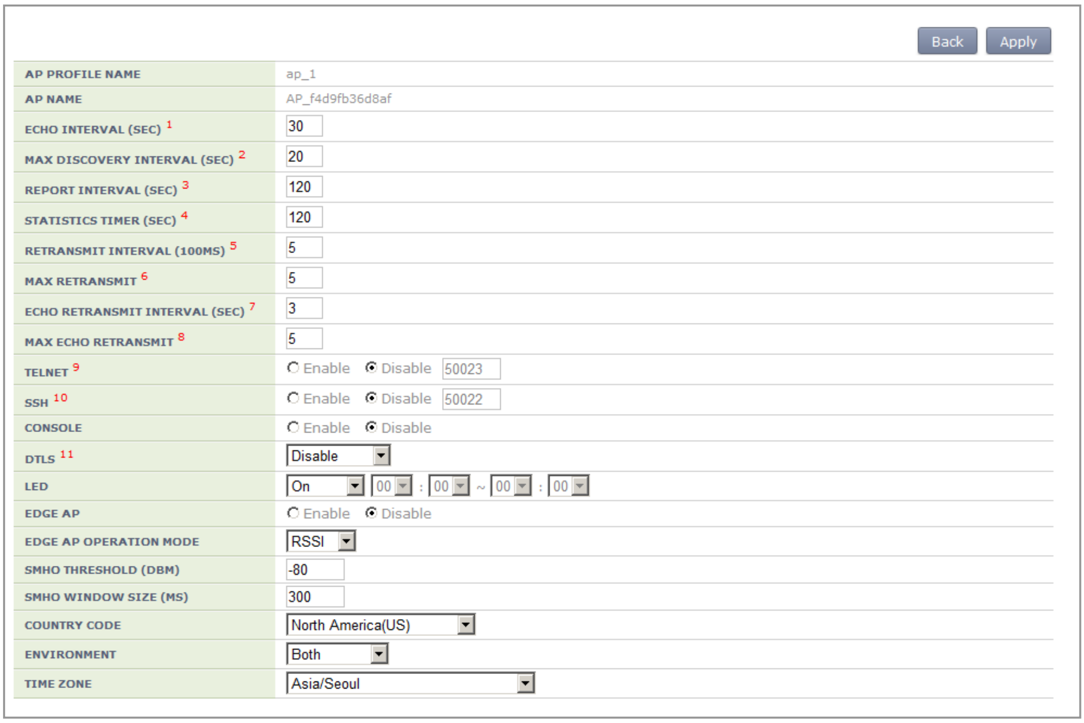
AP PROFILE NAME	ap_1
AP NAME	PV-77-104
AP GROUP NAME	test1
REMOTE AP GROUP NAME	test
AP MODE [1]	General AP
MAC ADDRESS	f4:d9:fb:24:2d:c1
MAP LOCATION	
LOCATION	
IP ADDRESS	0.0.0.0
IP ADDRESS POLICY	○ DHCP ● AP Priority (AP Followed) ○ Static IP
IP ADDRESS	0 . 0 . 0 . 0
NETMASK	0 . 0 . 0 . 0
GATEWAY	0 . 0 . 0 . 0
DISCOVERY TYPE [2]	AP Followed Current Discovery Type : Static
ADMIN STATUS	Up
OPER STATUS	Down
PRIMARY CONTROLLER NAME [3]	APC101 (10.10.10.10)
SECONDARY CONTROLLER NAME [3]	------------
TERTIARY CONTROLLER NAME [3]	------------

Figure 76. AP Profile Setting (1)

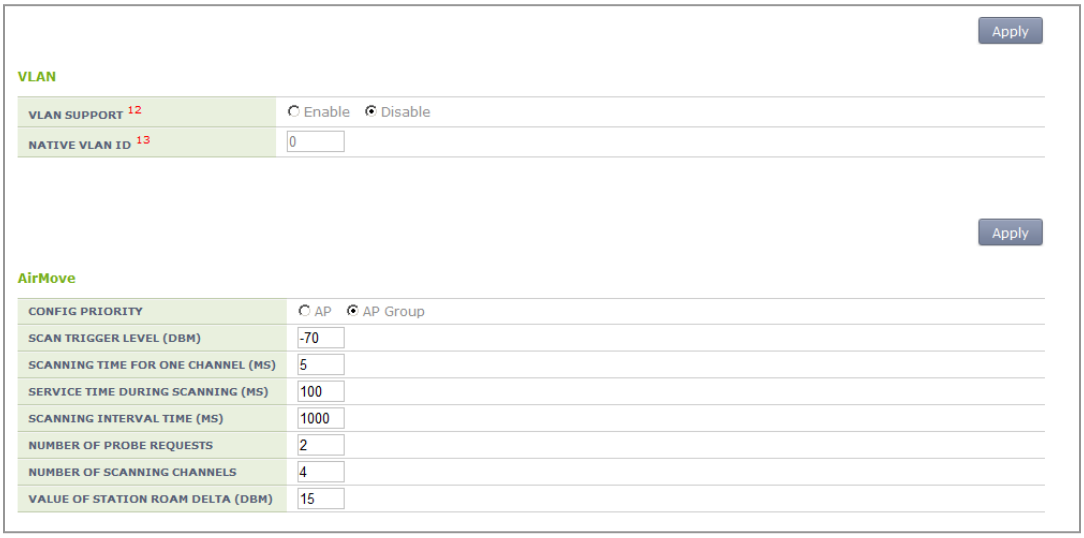
- AP NAME: AP name
- AP GROUP NAME: Indicates name of the AP GROUP to which the AP belongs.
- REMOTE AP GROUP NAME: Indicates name of the REMOTE AP GROUP to which the AP belongs.
- AP MODE: AP operational mode (General AP/Root AP/Repeater AP/Sniffer AP)
- MAC ADDRESS: Cannot be changed to the MAC address of an AP.

- MAP LOCATION
- LOCATION: Information of location where an AP is installed
- IP ADDRESS: IP address of AP
- IP ADDRESS POLICY: IP address mode
- DISCOVERY TYPE: AP discovery type
- ADMIN STATUS: AP administrative status
- OPER STATUS: Current AP operational status
  PRIMARY CONTROLLER NAME, SECONDARY CONTROLLER NAME, TERTIARY CONTROLLER NAME: Redundancy mode
  For WEC8050, the TERTIARY CONTROLLER NAME is not supported.

In the menu bar of <**WEC Main window**>, select <**Configuration**> and then select the <**Access Points**> → **AP** → <**Advanced**> menu in the sub-menus.
The setting options in the Advance tab are as follows. Fill in each item and click the <**Apply**> button to apply the settings.



AP PROFILE NAME	ap_1
AP NAME	AP_f4d9fb36d8af
ECHO INTERVAL (SEC) [1]	30
MAX DISCOVERY INTERVAL (SEC) [2]	20
REPORT INTERVAL (SEC) [3]	120
STATISTICS TIMER (SEC) [4]	120
RETRANSMIT INTERVAL (100MS) [5]	5
MAX RETRANSMIT [6]	5
ECHO RETRANSMIT INTERVAL (SEC) [7]	3
MAX ECHO RETRANSMIT [8]	5
TELNET [9]	○ Enable ● Disable 50023
SSH [10]	○ Enable ● Disable 50022
CONSOLE	○ Enable ● Disable
DTLS [11]	Disable
LED	On 00 : 00 ~ 00 : 00
EDGE AP	○ Enable ● Disable
EDGE AP OPERATION MODE	RSSI
SMHO THRESHOLD (DBM)	-80
SMHO WINDOW SIZE (MS)	300
COUNTRY CODE	North America(US)
ENVIRONMENT	Both
TIME ZONE	Asia/Seoul



VLAN

VLAN SUPPORT [12]	○ Enable ● Disable
NATIVE VLAN ID [13]	0

AirMove

CONFIG PRIORITY	○ AP ● AP Group
SCAN TRIGGER LEVEL (DBM)	-70
SCANNING TIME FOR ONE CHANNEL (MS)	5
SERVICE TIME DURING SCANNING (MS)	100
SCANNING INTERVAL TIME (MS)	1000
NUMBER OF PROBE REQUESTS	2
NUMBER OF SCANNING CHANNELS	4
VALUE OF STATION ROAM DELTA (DBM)	15

Figure 77. AP Profile Setting (2)

4.2.4.3 AP Mode Configuration

Configuration using CLI

To configure AP mode, execute the command as follows.

1) Go to configure → AP configuration → AP profile mode of CLI.

```
WEC8500# configure terminal
WEC8500/configure# ap ap_1
WEC8500/configure/ap ap_1# profile
WEC8500/configure/ap ap_1/profile#
```

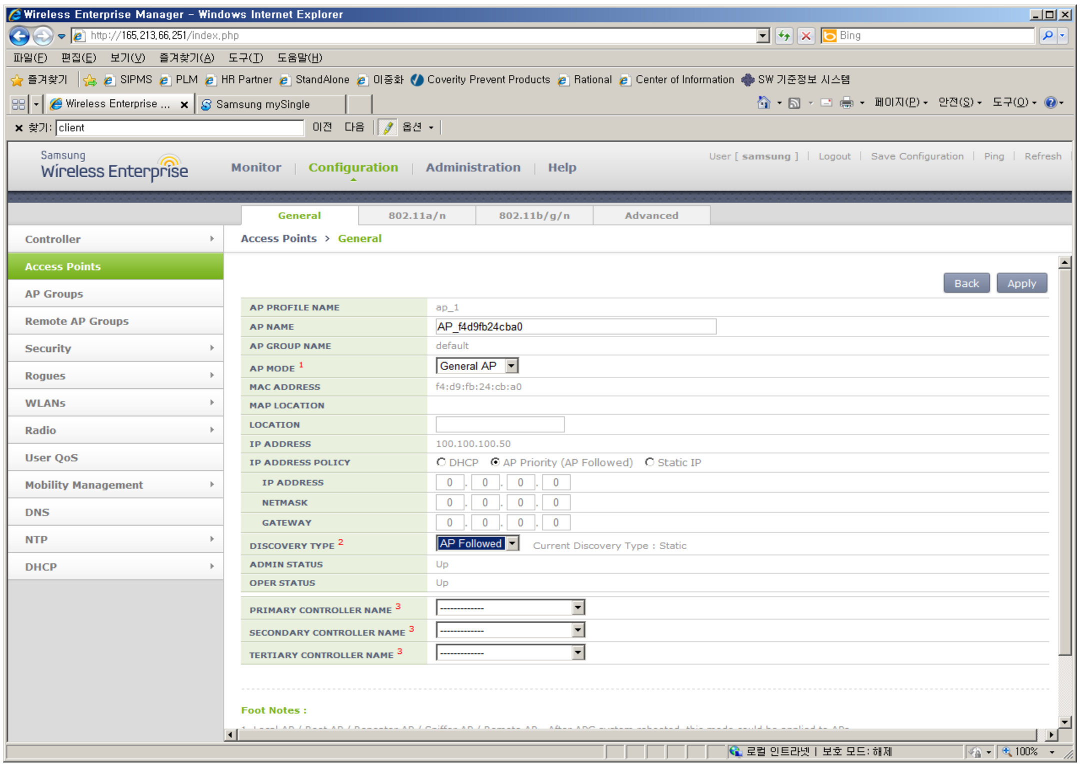
2) Configure the AP mode.
   - ap-mode [MODE]

Parameter	Description
MODE	AP operation mode (generalAp/rootAp/repeaterAp/snifferAp) - generalAp: Typical operation mode. Default value. - rootAp: AP mode where a repeater AP can be connected. - repeasterAp: AP mode that is connected to a wireless area and the APC through the root AP. - snifferAp: AP mode where the packets operating in a wireless environment can be captured.

3) To check the information of a configured AP, use the ‘show ap detail [AP_NAME]’ command.

Configuration using Web UI

In the menu bar of <**WEC Main window**>, select <**Configuration**> and then select the <**Access Points**> → **AP selection** → <**General**> menu in the sub-menus.
After selecting the AP MODE NAME item, click the <**Apply**> button to apply the configuration.



AP PROFILE NAME	ap_1
AP NAME	AP_f4d9fb24cba0
AP GROUP NAME	default
AP MODE [1]	General AP
MAC ADDRESS	f4:d9:fb:24:cb:a0
MAP LOCATION	
LOCATION	
IP ADDRESS	100.100.100.50
IP ADDRESS POLICY	○ DHCP ● AP Priority (AP Followed) ○ Static IP
IP ADDRESS	0 . 0 . 0 . 0
NETMASK	0 . 0 . 0 . 0
GATEWAY	0 . 0 . 0 . 0
DISCOVERY TYPE [2]	AP Followed Current Discovery Type : Static
ADMIN STATUS	Up
OPER STATUS	Up
PRIMARY CONTROLLER NAME [3]	-------------
SECONDARY CONTROLLER NAME [3]	-------------
TERTIARY CONTROLLER NAME [3]	-------------

Figure 78. AP mode configuration

4.2.4.4 AP CLI Access Account

The APC operator can add or remove account information relating to the AP CLI. When the APC is first installed, a default account is provided (id: root, password: samsung).
Up to three AP CLI accounts can be added, and at least one account must be configured. Therefore, if there is only one remaining account, it cannot be deleted.
(* While each account may be in any of the three available levels (Administrator/Operator/Monitor), there are currently no functional differences for the APs.)

Configuration using CLI

Execute the following commands to configure the AP access account.

1) Go to configure → APC mode of CLI.

```
WEC8500# configure terminal
WEC8500/configure# apc
WEC8500/configure/apc #
```

2) Add an AP CLI account.
   - ap-account [ID] [PASSWORD] [LEVEL]

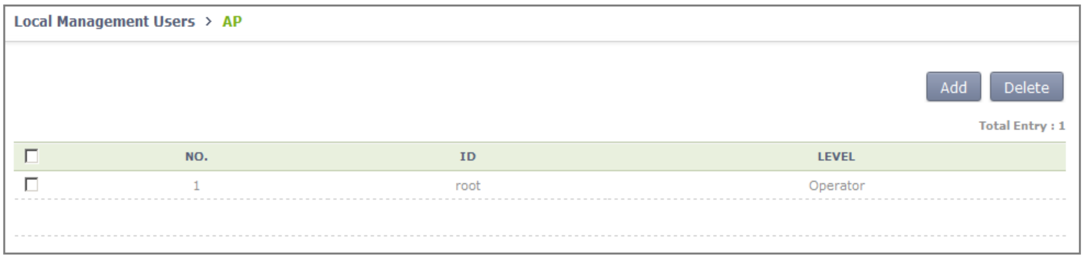
Parameter	Description
ID	This is the ID of the AP CLI account. Only an alphanumeric value of up to eight characters can be entered.
Password	This is the password of the AP CLI account. Only an alphanumeric value of up to eight characters can be entered.
Level	This is the level of the AP CLI account. Available values are administrator/operator/monitor.

3) An account can be deleted by entering the 'no' parameter as shown below.
   - no ap-account [ID]

4) Use the ‘show apc ap-account’ command to retrieve the AP configuration information.

Configuration using Web UI

In the menu bar of <**WEC Main Window**>, select <**Configuration**>, and then select <**Local Management Users**> → **AP** in the submenu.
Click the ‘Add’ or ‘Delete’ button to add or delete the AP CLI account.



Total Entry : 1

□	NO.	ID	LEVEL
□	1	root	Operator

Figure 79. AP CLI Account Add/Remove Window

4.2.4.5 AP SNMP Agent Configuration

The APC operator can configure SNMP Agent settings for all APs.

Configuration using CLI

Execute the following commands to configure the SNMP Agent settings of the AP.

1) Go to configure → snmp → ap mode of CLI.

```
WEC8500# configure terminal
WEC8500/configure# snmp
WEC8500/configure/snmp# ap
WEC8500/configure/snmp/ap#
```

2) Configure the snap agent information of the AP.
Enable/disable SNMP of the AP.

- enable or no enable

Configure the SNMP port number of the AP.

- Port [PORT NUMBER]

Configure the Read Only Community Name of the AP.

- ro-community [COMMUNITY NAME]

Configure the Write Only Community Name of the AP.

- rw-community [COMMUNITY NAME]

Configure the user information of the AP.

- Use r[USER NAME] [AUTHENTICATION TYPE] [AUTHENTICATION KEY] [PRIVATE PROTOCOL] [PRIVATE KEY]

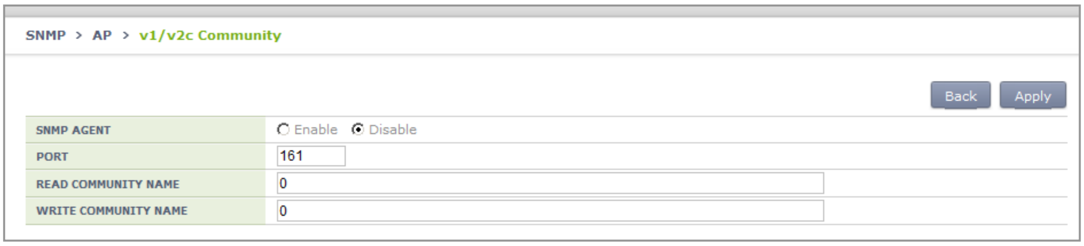
Parameter	Description
PORT NUMBER	This is the SNMP port number.
COMMUNITY NAME	This is the SNMP Read Only or Write Only Community name.
USER NAME	This is the SNMP user name.
AUTHENTICATION TYPE	This is the SNMP authentication type. Either of the following two can be selected: - MD5 - SHA
AUTHENTICATION KEY	A number in the range of 8 to 20 can be entered.
PRIVATE PROTOCOL	Either of the following two can be selected: - DES - AES

Parameter	Description
PRIVATE KEY	A number in the range of 8 to 20 can be entered.

3) Use the ‘show snmp ap’ command to retrieve the agent information configured for the AP.

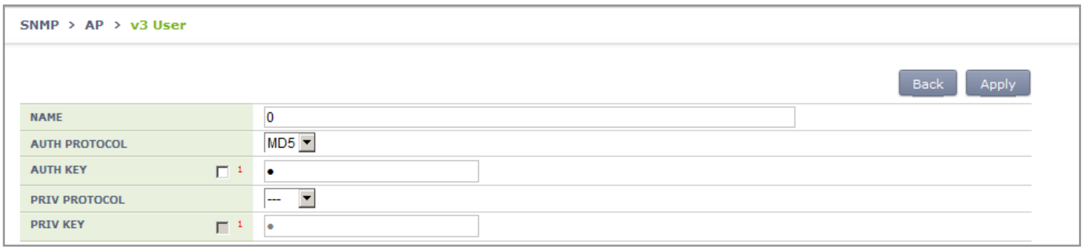
Configuration using Web UI

In the menu bar of <**WEC Main Window**>, select <**Administration**>, select <**AP**> in the submenu, and then select <**v1/v2c Community**> or <**v3 User**> to configure the SNMP agent information.



SNMP AGENT	○ Enable ● Disable
PORT	161
READ COMMUNITY NAME	0
WRITE COMMUNITY NAME	0

Figure 80. AP SNMP v1/v2c Community Configuration Window



NAME	0
AUTH PROTOCOL	MD5
AUTH KEY □ 1	•
PRIV PROTOCOL	---
PRIV KEY □ 1	•

Figure 81. AP v3 User Configuration Window

4.2.5 Information Management

The APC manages the history statistics information, real-time interface statistics information, and tech support information of the AP.

AP History Statistics

The AP transmits the interface (WAN and WLAN) and CPU load/memory usage statistics information collected for 5 min. to the APC. The APC forwards the information to the WEM via FTP. If the APC does not interoperate with the WEM, the APC stores the information for 3 days. (Future Release)

AP real-time statistics

If the APC requests the interface information to an AP, the AP transmits the interface information (WAN and WLAN) to the APC at every 5 second and the APC stores the information in its internal DB. An operator can retrieve the information by using CLI or WEC.

AP Tech Support

If there occurs a problem with a specific AP, an operator can download the Tech Support information from the AP. Execute the following command to use the function.

The Tech Support from an AP includes the following information.

- System log message file
- System crash information file
- System report files (status/configuration information)
- Core file used to check application malfunctioning

4.2.5.1 History Statistics Information

To check the history statistics information relay status of an AP, use the ‘show ap stats-history’ command.

4.2.5.2 Real-time Interface Statistics Information

Configuration using CLI

1) Go to configure → AP configuration.

```
WEC8500# configure terminal
WEC8500/configure# ap ap_1
WEC8500/configure/ap ap_1#
```

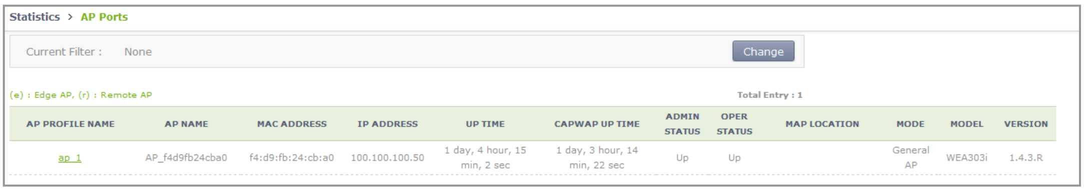
2) Configure to make real-time interface statistics information updated periodically.

```
WEC8500/configure/ap ap_1# get-if-stats
```

3) To check the interface statistics information of an AP, use the 'show ap if-stats [AP_NAME]' command.

Configuration using Web UI

In the menu bar of **<WEC Main window>**, select **<Monitor>** and then select the **<Statistics>** → **<AP Ports>** menu in the sub-menus.
As shown below, you can retrieve the real-time interface statistics of the AP.



Current Filter : None

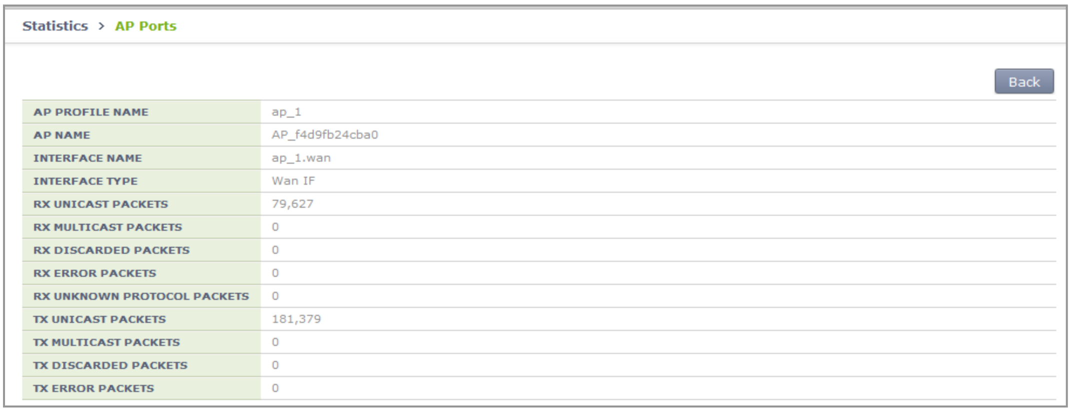
(e) : Edge AP, (r) : Remote AP

Total Entry : 1

AP PROFILE NAME	AP NAME	MAC ADDRESS	IP ADDRESS	UP TIME	CAPWAP UP TIME	ADMIN STATUS	OPER STATUS	MAP LOCATION	MODE	MODEL	VERSION
ap_1	AP_f4d9fb24cba0	f4:d9:fb:24:cb:a0	100.100.100.50	1 day, 4 hour, 15 min, 2 sec	1 day, 3 hour, 14 min, 22 sec	Up	Up		General AP	WEA303i	1.4.3.R

Select an item in the list, and then you can check detail information.

Figure 82. AP Ports window



AP PROFILE NAME	ap_1
AP NAME	AP_f4d9fb24cba0
INTERFACE NAME	ap_1.wan
INTERFACE TYPE	Wan IF
RX UNICAST PACKETS	79,627
RX MULTICAST PACKETS	0
RX DISCARDED PACKETS	0
RX ERROR PACKETS	0
RX UNKNOWN PROTOCOL PACKETS	0
TX UNICAST PACKETS	181,379
TX MULTICAST PACKETS	0
TX DISCARDED PACKETS	0
TX ERROR PACKETS	0

Figure 83. AP Ports detail information window

4.2.5.3 Tech Support Information

Execute the below command to download the Tech Support information from an AP.

Configuration using CLI

1) Go to configure → AP configuration → tech-support of CLI.

```
WEC8500# configure terminal
WEC8500/configure# ap [ap profile name]
WEC8500/configure/ap ap_1# tech-support
WEC8500/configure/ap ap_1/tech-support#
```

2) Request the coredump file of the AP.

```
WEC8500/configure/ap ap_1/tech-support# get-coredump (system / radio-
coredump)
```

3) Request the crashfile of the AP.

```
WEC8500/configure/ap ap_1/tech-support# get-crash-file (system /
radio-coredump)
```

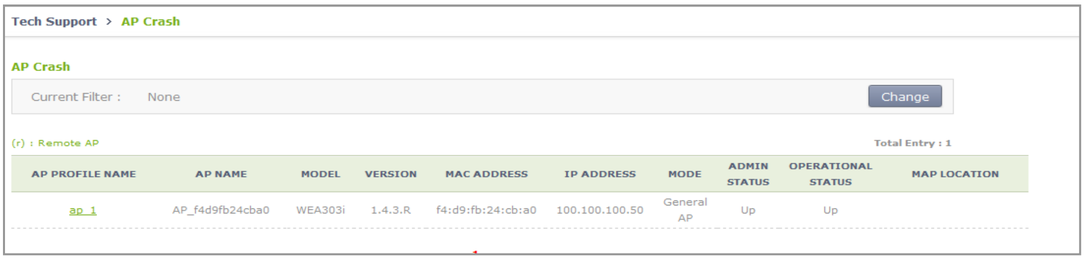
4) Request the log file of the AP.

```
WEC8500/configure/ap ap_1/tech-support# get-log-file
```

5) Use ‘show ap tech-support’ command to check the Tech Support file information of APs. Operator can use FTP or sFTP to download Tech Support files.

Configuration using Web UI

In the menu bar of <**WEC Main window**>, select <**Administrator**> and then select the <**Tech Support**> → <**AP Crash**> menu in the sub-menus.
By clicking the profile name of an AP, operator can download the Tech Support file.



Current Filter : None

(r) : Remote AP

Total Entry : 1

AP PROFILE NAME	AP NAME	MODEL	VERSION	MAC ADDRESS	IP ADDRESS	MODE	ADMIN STATUS	OPERATIONAL STATUS	MAP LOCATION
ap_1	AP_f4d9fb24cba0	WEA303i	1.4.3.R	f4:d9:fb:24:cb:a0	100.100.100.50	General AP	Up	Up	

Figure 84. AP Tech Support Information Receiving Window

4.2.6 Outdoor AP Configuration

The APC system provides outdoor AP connection diagnostic functions for outdoor APs. The AP connection diagnostics function checks ping status of outdoor APs and displays the results on the operator's monitor.

Procedure of using the outdoor AP connection diagnostics function is as follows:

1) The operator creates/deletes outdoor APWEC using CLI.
2) The APC system periodically pings the outdoor AP to check the network connection of the AP and stores the results.
3) The operator uses the WEC, WEM(Future Release) or CLI to determine network connection status of the outdoor AP.

Concerning outdoor AP count:

1) Outdoor APs are not included in the AP count of the APC license.
2) Outdoor APs are not included in the ordinary AP count.
3) The maximum up-ported outdoor AP count is 300 for the WEC8500 model and 75 for the WEC8050 model.
4) The APC system can retrieve the total/up/down outdoor AP count using the WEC or CLI.

4.2.6.1 Outdoor AP Addition/Removal

The APC system allows creation/deletion of outdoor AP information using the WEC or CLI.

Configuration using CLI

1) Go to configure mode of CLI.

```
WEC8500# configure terminal
WEC8500/configure#
```

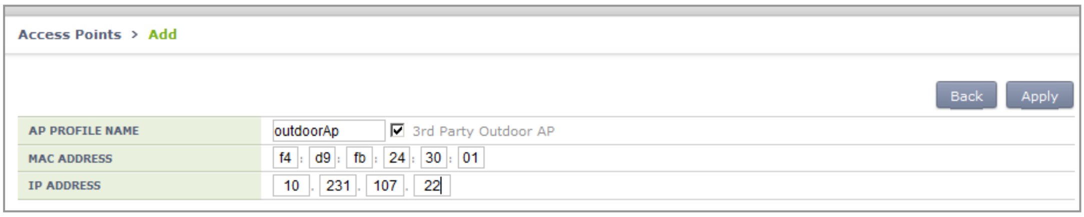
2) Create or delete an AP. Use the 'no' parameter in front of the command to delete an outdoor AP.
   - outdoor-ap [PROFILE_NAME] [MAC_ADDRESS] [IP_ADDRESS]
   - no outdoor-ap [PROFILE_NAME]

3) Create or delete an outdoor AP. Use the 'no' parameter in front of the command to delete an outdoor AP.

4) Use the 'show ap summary' command to check the outdoor AP information.

Configuration using Web UI

In the menu bar of <**WEC Main Window**>, select <**Configuration**> and then select the <**Access Points**> menu in the sub-menus. To create an outdoor AP, click <**Add**>, select <**3rd Party Outdoor AP**>, enter AP PROFILE NAME, MAC ADDRESS, and IP ADDRESS, and then select <**Apply**>.



AP PROFILE NAME	outdoorAp ☑ 3rd Party Outdoor AP
MAC ADDRESS	f4 : d9 : fb : 24 : 30 : 01
IP ADDRESS	10 . 231 . 107 . 22

Figure 85. Outdoor AP Create Window

4.2.7 AP Package Upgrade

Configuration using CLI (Upgrade Function)

To manage the AP upgrade function, execute the command as follows:

1) Go to configure → AP configuration mode of CLI.

```
WEC8500# configure terminal
WEC8500/configure# ap ap_1
```

2) Request the image file of an AP to upgrade.

```
WEC8500/configure/ap ap_1# upgrade-request weafama_1.2.4.R.bin

WARNING: AP will be upgrade.
Are you sure you want to continue? (y/n) : y
WEC8500/configure/ap ap_1#
```

3) To check the upgrade file information of the requested AP, use the following command.

```
WEC8500/configure/ap ap_1# show ap upgrade list

   /* (RC/FR/RC)  : RetryCount/FailReason/RebootCause
   /* Pri         : VersionPriority (MD-model,A-AP config)
 AP_ID  Model    Version(config/current) Status(RC/FR/RC)   Pri   force
    1    WEA302i  1.2.4.R/ 1.2.4.R         Success( 0/ 0/146) AP    No
```

Configuration using CLI (Upgrade environment)

To configure AP upgrade related environment, the following command is provided. First of all, go to the configure → AP-all → upgrade mode of CLI.

```
WEC8500# configure terminal
WEC8500/configure# ap-all
WEC8500/configure/ap-all# upgrade
WEC8500/configure/ap-all/upgrade#
```

[select-package]

This command configures a package to use during AP upgrade.

- select-package [UPGRADE_TYPE] [FILE_NAME]

Parameter	Description
UPGRADE_TYPE	Configures upgrade type (default/quick-upgrade/predownload) - default: AP image that is referred to during provision upgrade. - quick-upgrade: AP image that is referred to for entire AP upgrade upon an operator's request. - predownload: AP image that is referred to download AP image to AP during entire AP upgrade.
FILE_NAME	Image file name that will be used for AP upgrade

[target]

During entire upgrade, you can select whether to maintain individual configured AP version of an AP or perform upgrade.

- Target [AP UPGRADE TARGET]

Parameter	Description
UPGRADE TARGET	Upgrade target (all/ keeping-individual) - all: Perform upgrade for all the APs. (default) - keeping-individual: While maintaining individually configured ap version, perform upgrade for the rest APs.

[transfer-protocol]

This command selects a transmission protocol that is used to transmit the package file of an AP from the WEC8500 to the AP.

- Transfer-protocol [AP TRANSFER MODE]

Parameter	Description
TRANSFER_MODE	File transmission protocol (ftp/sftp) - ftp: ftp is used for file transmission. - sftp: sftp is used for file transmission.

[max-download]

This command configures the maximum number of simultaneous downloads when transmitting the package file of an AP from the APC to the AP.

- Max-download [COUNT]

Parameter	Description
COUNT	Maximum number of simultaneous downloads of AP image file (range: 1-50, default: 10)

[max-retry]

This command configures maximum number of re-attempts when AP upgrade is failed.

- Max-retry [COUNT]

Parameter	Description
COUNT	Maximum number of AP upgrade re-attempts (range: 1-10, default: 3)

[start]

This command provides the entire AP upgrade function.

- start [UPGRADE_TYPE]

Parameter	Description
UPGRADE_TYPE	Configures upgrade type (quick-upgrade/predownload) - quick-upgrade: Perform entire ap upgrade upon an operator's request. - predownload: Download ap image to ap first during entire ap upgrade.

If you perform package upgrade after configuring AP upgrade type to predownload, restart all the APs in the following methods.

```
WEC8500# configure terminal
WEC8500/configure# ap-all
WEC8500/configure/ap-all# reboot upgrade
```

[stop]

This command provides the function of stopping the image upgrade of all the APs.

- stop

[show ap upgrade]

To check the upgrade information of an AP, use the following command.

- show ap upgrade summary

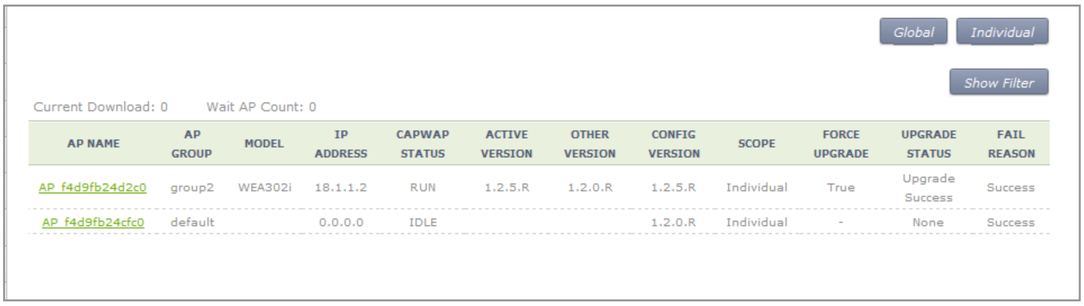
Configuration using Web UI

In the menu bar of <**WEC Main window**>, select <**Administrator**> and then select <**Package Upgrade**> → <**AP**> menu in the sub menu.

You can perform AP upgrade in the AP Upgrade tab and configure upgrade related environment in the Advanced tab.

[AP Upgrade tab]

AP Upgrade tab upgrades all the APs or a specific AP.



Current Download: 0 Wait AP Count: 0

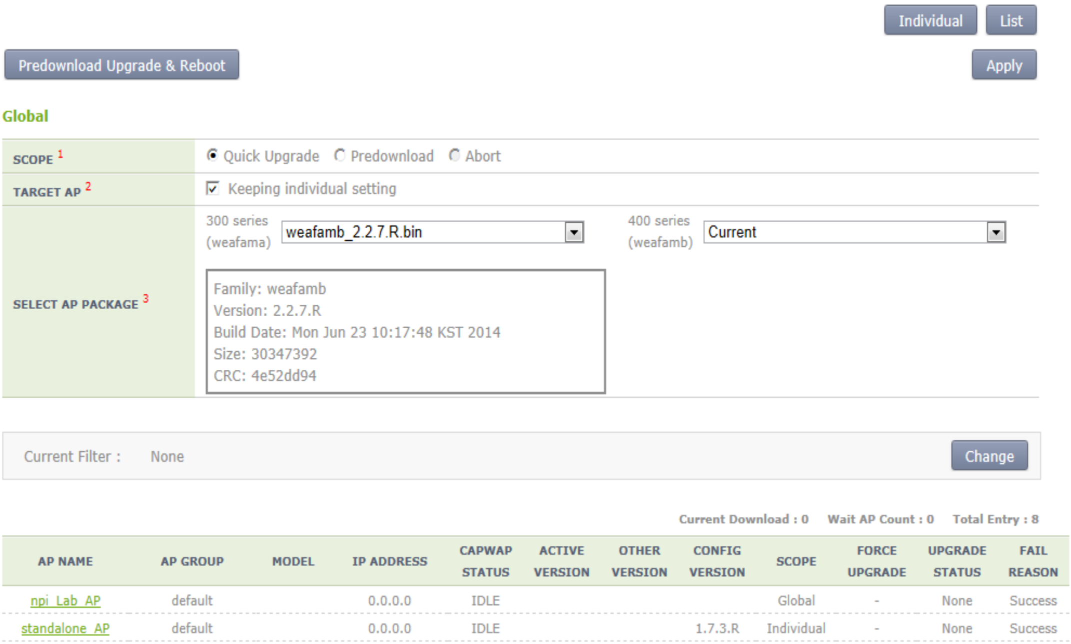
AP NAME	AP GROUP	MODEL	IP ADDRESS	CAPWAP STATUS	ACTIVE VERSION	OTHER VERSION	CONFIG VERSION	SCOPE	FORCE UPGRADE	UPGRADE STATUS	FAIL REASON
AP_f4d9fb24d2c0	group2	WEA302i	18.1.1.2	RUN	1.2.5.R	1.2.0.R	1.2.5.R	Individual	True	Upgrade Success	Success
AP_f4d9fb24cfc0	default		0.0.0.0	IDLE			1.2.0.R	Individual	-	None	Success

Figure 86. AP upgrade

The procedure of entire AP upgrade is as follows:

1) In the AP Upgrade window, click the <**Global**> button.

2) The <**Global**> area is displayed on the window. After configuring each item, click the <**Apply**> button.



Global

SCOPE [1]	● Quick Upgrade ○ Predownload ○ Abort
TARGET AP [2]	☑ Keeping individual setting
SELECT AP PACKAGE [3]	300 series (weafama): weafamb_2.2.7.R.bin 400 series (weafamb): Current Family: weafamb Version: 2.2.7.R Build Date: Mon Jun 23 10:17:48 KST 2014 Size: 30347392 CRC: 4e52dd94

Current Filter : None

Current Download : 0 Wait AP Count : 0 Total Entry : 8

AP NAME	AP GROUP	MODEL	IP ADDRESS	CAPWAP STATUS	ACTIVE VERSION	OTHER VERSION	CONFIG VERSION	SCOPE	FORCE UPGRADE	UPGRADE STATUS	FAIL REASON
npi_Lab_AP	default		0.0.0.0	IDLE				Global	-	None	Success
standalone_AP	default		0.0.0.0	IDLE			1.7.3.R	Individual	-	None	Success

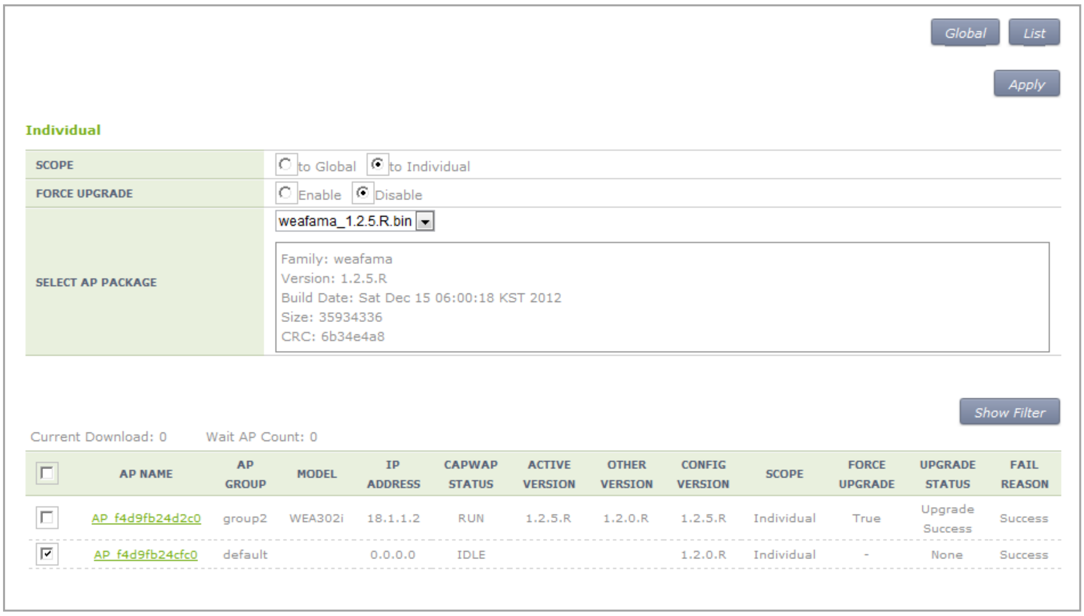
Figure 87. AP upgrade-global

- SCOPE: Selects upgrade method. To make the AP working as the package immediately after upgrade, select Quick Upgrade. To download the package to the AP, select the Predownload menu.
- TARGE AP: Select an AP target to upgrade. If you select <Keeping individual setting>, an AP that is configured as individual is excluded from upgrade.
- SELECT AP PACKAGE: Selects an AP package to upgrade.

3) If the SCOPE setup is Predownload upgrade, you must restart the AP once download is completed. After selecting the **<Administration>** → **<Reboot>** → **<AP>** menu, select Reboot All with Upgrade to restart the AP.

To upgrade a specific AP, follow the below procedure.

1) In the AP Upgrade window, click the **<Individual>** button.
2) The individual area is displayed on the window. After configuring each item, click the **<Apply>** button.



Individual

SCOPE	○ to Global ● to Individual
FORCE UPGRADE	○ Enable ● Disable
SELECT AP PACKAGE	weafama_1.2.5.R.bin Family: weafama Version: 1.2.5.R Build Date: Sat Dec 15 06:00:18 KST 2012 Size: 35934336 CRC: 6b34e4a8

Current Download: 0 Wait AP Count: 0

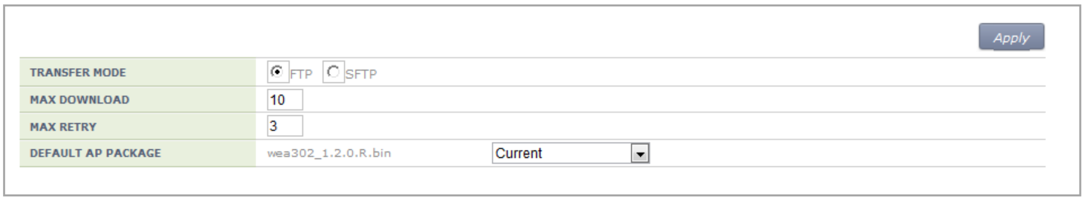
□	AP NAME	AP GROUP	MODEL	IP ADDRESS	CAPWAP STATUS	ACTIVE VERSION	OTHER VERSION	CONFIG VERSION	SCOPE	FORCE UPGRADE	UPGRADE STATUS	FAIL REASON
□	AP_f4d9fb24d2c0	group2	WEA302i	18.1.1.2	RUN	1.2.5.R	1.2.0.R	1.2.5.R	Individual	True	Upgrade Success	Success
☑	AP_f4d9fb24cfc0	default		0.0.0.0	IDLE			1.2.0.R	Individual	-	None	Success

Figure 88. AP upgrade-individual

- SCOPE: Selects upgrade method. The **<to individual>** upgrades the selected AP to a specific package and the **<to global>** makes a select AP working as global.
- FORCE UPGRADE: Enable or disable
- SELECT AP PACKAGE: Selects an AP package to upgrade..

[Advanced tab]

Configures AP upgrade related environment settings.



TRANSFER MODE	● FTP ○ SFTP
MAX DOWNLOAD	10
MAX RETRY	3
DEFAULT AP PACKAGE	wea302_1.2.0.R.bin Current

Figure 89. AP upgrade-advanced

- TRANSFER MODE: Selects a protocol that transmits an AP package.
- MAX DOWNLOAD: Configures maximum number of sessions that can be downloaded simultaneously.
- MAX RETRY: Configures maximum number of re-attempts when AP upgrade is failed.
- DEFAULT AP PACKAGE: Select an AP package that will be used for automatic upgrade during AP joint.

4.2.8 Remote AP Package Upgrade

APs in a remote group can be upgraded by downloading an AP package from a specific AP. This is useful for efficient management of APC-AP bandwidth.

A master AP can be selected for each AP package model. After downloading an AP package from the APC, the master AP allows the AP package to be downloaded to other APs in the remote group.

The operator can manage AP upgrade of the APs in the remote group by checking the AP package download status in the remote group and performing reboot and upgrade.

4.2.8.1 Activating Upgrade

The operator can enable/disable the AP upgrade in the remote group.
When the AP upgrade is enabled, version priority in AP upgrade status changes to Remote.

Configuration using CLI

Example:

```
WEC8500# configure terminal
WEC8500/configure# remote-ap-group rUpgrade
WEC8500/configure/remote-ap-group rUpgrade# upgrade
WEC8500/configure/remote-ap-group rUpgrade/upgrade# enable

WEC8500/configure/remote-ap-group rUpgrade/upgrade# no enable
```

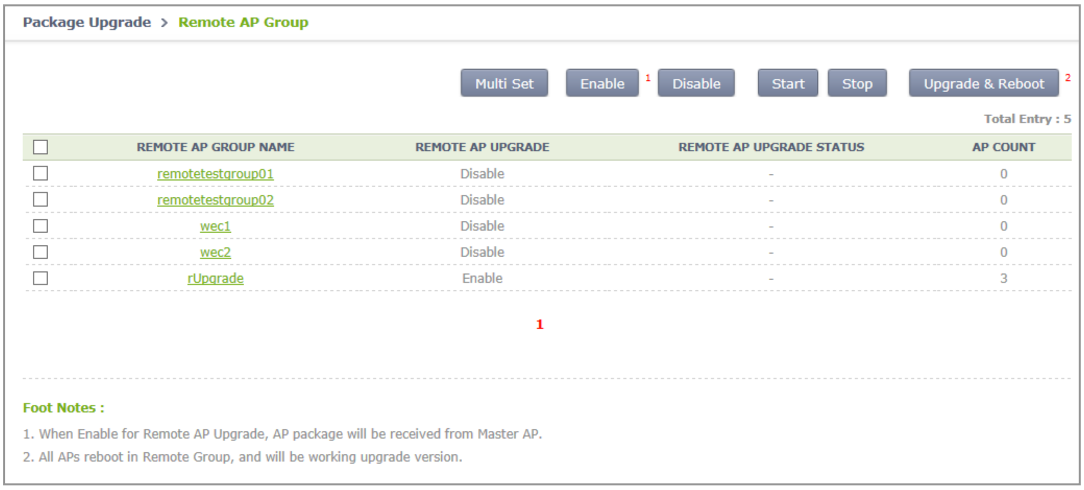
CLI for checking configuration:

```
WEC8500 # show remote-ap-group upgrade config rUpgrade

================== Remote Ap Group Upgrade Config =================

 Group Name              : rUpgrade
 Enable                  : Enable
 Type                    : Default
 Mode                            : FTP
 Path                    : package/ap
 PortNum                 : 21
 MAXretries              : 3
 ForceOption             : Disable

 weafama                 :  (APID:0, IP:0.0.0.0)
                         :  ()
 weafamb                 :  (APID:0, IP:0.0.0.0)
                         :  ()

WEC8500# show remote-ap-group upgrade list rUpgrade

   /* (RC/FR/RC) : RetryCount/FailReason/RebootCause
 AP_ID  Model  Version(config/current)    Status(RC/FR/RC)   MasterAp
    1   WEA303i     Remote/1.7.0.U2         None( 0/ 0/128)         -
    2   WEA312i     Remote/1.7.0.U2         None( 0/ 0/128)         -
    3   WEA303i     Remote/1.7.0.U1         None( 0/ 0/128)         -
```

Configuration using Web UI

Administration > Package Upgrade > Remote AP Group

Example:



Total Entry : 5

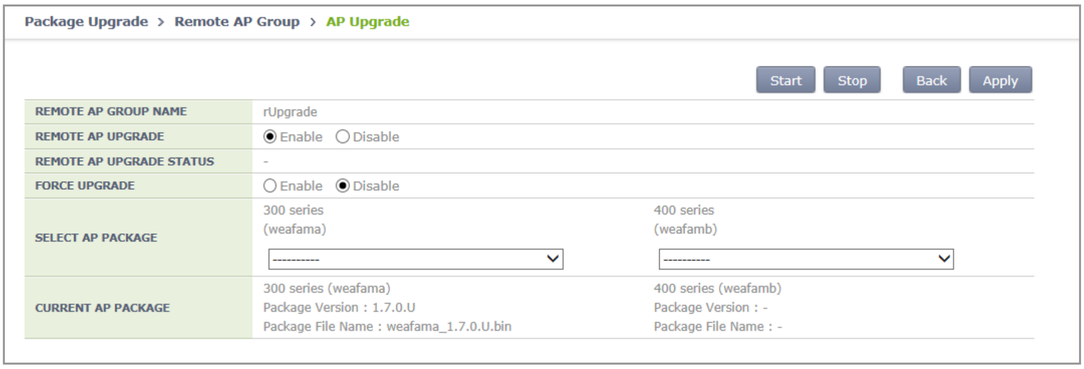
□	REMOTE AP GROUP NAME	REMOTE AP UPGRADE	REMOTE AP UPGRADE STATUS	AP COUNT
□	remotetestgroup01	Disable	-	0
□	remotetestgroup02	Disable	-	0
□	wec1	Disable	-	0
□	wec2	Disable	-	0
□	rUpgrade	Enable	-	3

1

Foot Notes :

1. When Enable for Remote AP Upgrade, AP package will be received from Master AP.
2. All APs reboot in Remote Group, and will be working upgrade version.

Figure 90. Remote AP Group Upgrade Activation_1



REMOTE AP GROUP NAME	rUpgrade	
REMOTE AP UPGRADE	● Enable ○ Disable	
REMOTE AP UPGRADE STATUS	-	
FORCE UPGRADE	○ Enable ● Disable	
SELECT AP PACKAGE	300 series (weafama) ----------	400 series (weafamb) ----------
CURRENT AP PACKAGE	300 series (weafama) Package Version : 1.7.0.U Package File Name : weafama_1.7.0.U.bin	400 series (weafamb) Package Version : - Package File Name : -

Figure 91. Remote AP Group Upgrade Activation_2

4.2.8.2 Master AP Configuration (Optional)

The operator can configure the master AP for AP upgrade in the remote group. If none is configured, a master AP is automatically selected.

Configuration using CLI

Example:

```
WEC8500# configure terminal
WEC8500/configure# remote-ap-group rUpgrade
WEC8500/configure/remote-ap-group rUpgrade# upgrade
WEC8500/configure/remote-ap-group rUpgrade/upgrade# select-masterAP
ap_1

WEC8500/configure/remote-ap-group rUpgrade/upgrade# delete-masterAP
[weafama/weafamb]
```

CLI for checking configuration:

```
WEC8500# show remote-ap-group upgrade config rUpgrade

================== Remote Ap Group Upgrade Config =================

 Group Name               : rUpgrade
 Enable                   : Enable
 Type                     Default
 Mode                     : FTP
 Path                     : package/ap
 PortNum                  : 21
 MAXretries               : 3
 ForceOption              : Disable

 weafama                  : ap_1 (APID:1, IP:10.10.10.160)
                          :  ()
 weafamb                  :  (APID:0, IP:0.0.0.0)
                          :  ()
```

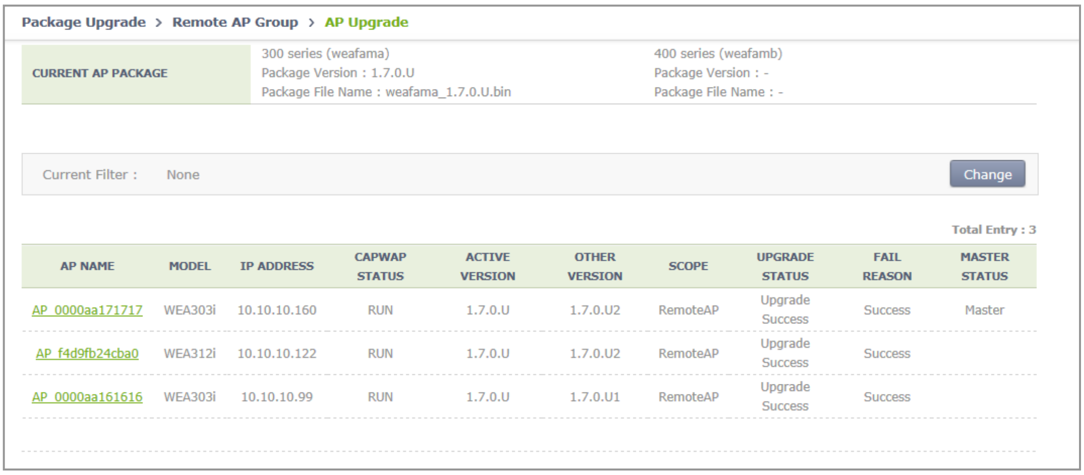
```
WEC8500# show remote-ap-group upgrade list rUpgrade
```

```
  /*  (RC/FR/RC)        : RetryCount/FailReason/RebootCause
AP_ID   Model  Version(config/current)     Status(RC/FR/RC)  MasterAp
   1   WEA303i      Global/1.7.0.U2         None( 0/ 0/128)   MasterApCfg
   2   WEA312i      Global/1.7.0.U2         None( 0/ 0/146)   -
   3   WEA303i      Global/1.7.0.U1         None( 0/ 0/146)   -
```

Configuration using Web UI

Administration > Package Upgrade > Remote AP Group

Example:



Package Upgrade > Remote AP Group > AP Upgrade

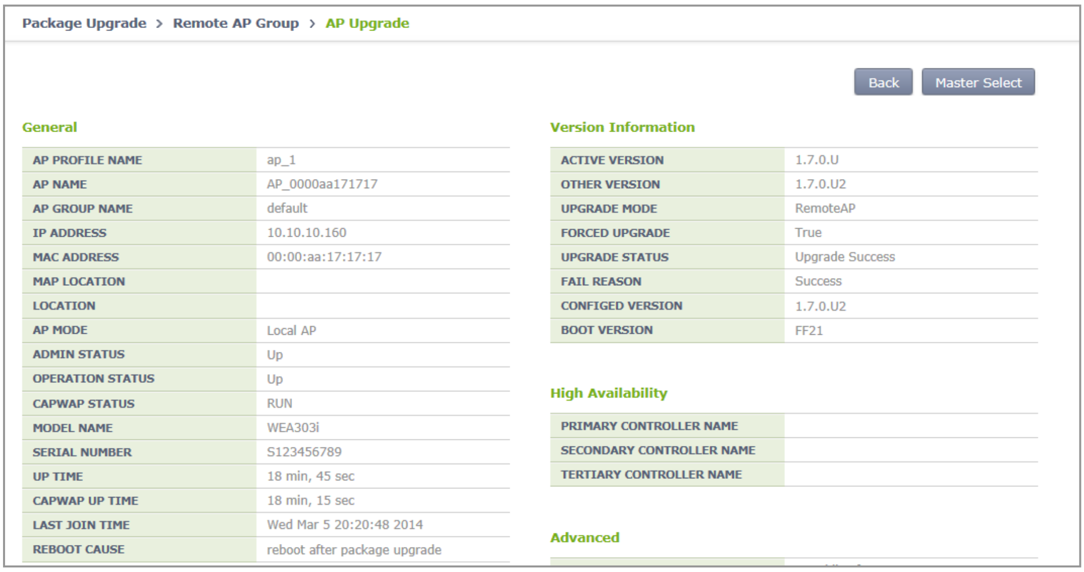
CURRENT AP PACKAGE	300 series (weafama) Package Version : 1.7.0.U Package File Name : weafama_1.7.0.U.bin	400 series (weafamb) Package Version : - Package File Name : -

Current Filter : None

Total Entry : 3

AP NAME	MODEL	IP ADDRESS	CAPWAP STATUS	ACTIVE VERSION	OTHER VERSION	SCOPE	UPGRADE STATUS	FAIL REASON	MASTER STATUS
AP_0000aa171717	WEA303i	10.10.10.160	RUN	1.7.0.U	1.7.0.U2	RemoteAP	Upgrade Success	Success	Master
AP_f4d9fb24cba0	WEA312i	10.10.10.122	RUN	1.7.0.U	1.7.0.U2	RemoteAP	Upgrade Success	Success	
AP_0000aa161616	WEA303i	10.10.10.99	RUN	1.7.0.U	1.7.0.U1	RemoteAP	Upgrade Success	Success	

Figure 92. Checking Master AP Configuration



Package Upgrade > Remote AP Group > AP Upgrade

General

AP PROFILE NAME	ap_1
AP NAME	AP_0000aa171717
AP GROUP NAME	default
IP ADDRESS	10.10.10.160
MAC ADDRESS	00:00:aa:17:17:17
MAP LOCATION	
LOCATION	
AP MODE	Local AP
ADMIN STATUS	Up
OPERATION STATUS	Up
CAPWAP STATUS	RUN
MODEL NAME	WEA303i
SERIAL NUMBER	S123456789
UP TIME	18 min, 45 sec
CAPWAP UP TIME	18 min, 15 sec
LAST JOIN TIME	Wed Mar 5 20:20:48 2014
REBOOT CAUSE	reboot after package upgrade

Version Information

ACTIVE VERSION	1.7.0.U
OTHER VERSION	1.7.0.U2
UPGRADE MODE	RemoteAP
FORCED UPGRADE	True
UPGRADE STATUS	Upgrade Success
FAIL REASON	Success
CONFIGED VERSION	1.7.0.U2
BOOT VERSION	FF21

High Availability

PRIMARY CONTROLLER NAME	
SECONDARY CONTROLLER NAME	
TERTIARY CONTROLLER NAME	

Advanced

Figure 93. Checking Master AP Configuration

4.2.8.3 AP Package Configuration

The operator can configure an AP package to upgrade in the remote group.

Configuration using CLI

Example:

```
WEC8500# configure terminal
WEC8500/configure# remote-ap-group rUpgrade
WEC8500/configure/remote-ap-group rUpgrade# upgrade
WEC8500/configure/remote-ap-group rUpgrade/upgrade# select-package
weafama weafama_1.7.0.U.bin

WEC8500/configure/remote-ap-group rUpgrade/upgrade#delete-package
[weafama/weafamb]
```

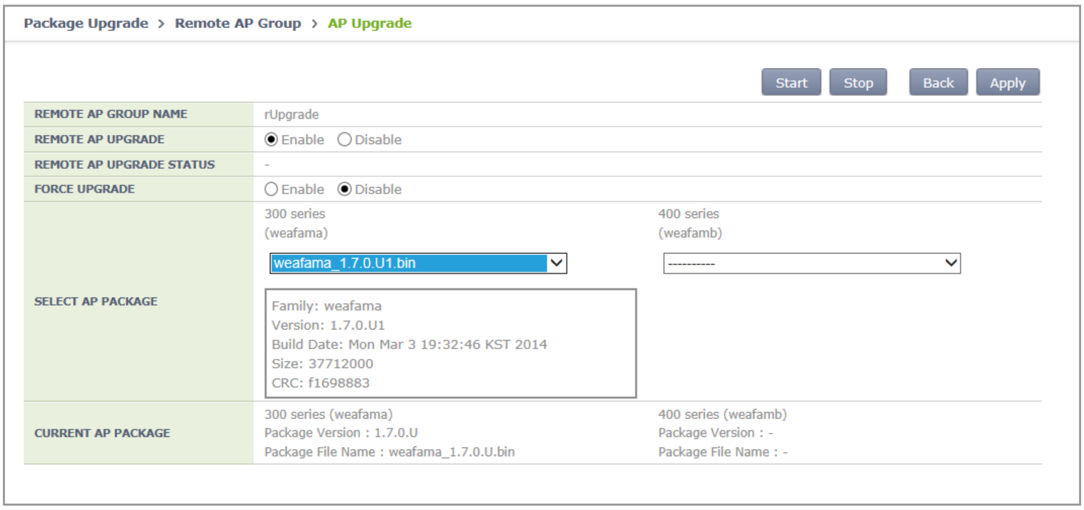
CLI for checking configuration:

```
WEC8500# show remote-ap-group upgrade config rUpgrade

================== Remote Ap Group Upgrade Config =================

 Group Name            : rUpgrade
 Enable                : Enable
 Type                  : Default
 Mode                  : FTP
 Path                  : package/ap
 PortNum               : 21
 MAXretries            : 3
 ForceOption           : Disable

 weafama               : ap_1 (APID:1, IP:10.10.10.160)
                       : weafama_1.7.0.U.bin (1.7.0.U)
 weafamb               :  (APID:0, IP:0.0.0.0)
                       :  ()
```

Configuration using Web UI

Administration > Package Upgrade > Remote AP Group

Example:



REMOTE AP GROUP NAME	rUpgrade	
REMOTE AP UPGRADE	● Enable ○ Disable	
REMOTE AP UPGRADE STATUS	-	
FORCE UPGRADE	○ Enable ● Disable	
SELECT AP PACKAGE	300 series (weafama) weafama_1.7.0.U1.bin Family: weafama Version: 1.7.0.U1 Build Date: Mon Mar 3 19:32:46 KST 2014 Size: 37712000 CRC: f1698883	400 series (weafamb) ----------
CURRENT AP PACKAGE	300 series (weafama) Package Version : 1.7.0.U Package File Name : weafama_1.7.0.U.bin	400 series (weafamb) Package Version : - Package File Name : -

Figure 94. AP Package Configuration

4.2.8.4 Starting AP Upgrade

The operator can start or stop AP upgrade in the remote group.

Configuration using CLI

Example:

```
WEC8500# configure terminal
WEC8500/configure# remote-ap-group rUpgrade
WEC8500/configure/remote-ap-group rUpgrade# upgrade
WEC8500/configure/remote-ap-group rUpgrade/upgrade# start

WEC8500/configure/remote-ap-group rUpgrade/upgrade# stop
```

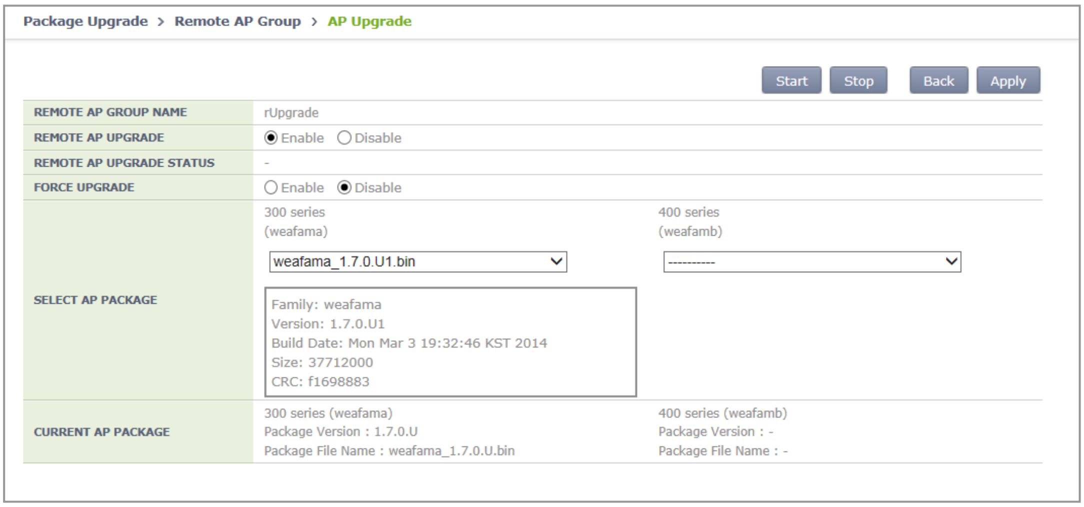
CLI for checking configuration:

```
WEC8500# show remote-ap-group upgrade config rUpgrade

================== Remote Ap Group Upgrade Config =================

 Group Name            : rUpgrade
 Enable                : Enable
 Type                  : Predownload
 Mode                  : FTP
 Path                    : package/ap
 PortNum                 : 21
 MAXretries              : 3
 ForceOption             : Disable

 weafama                 : ap_1 (APID:1, IP:10.10.10.160)
                         : weafama_1.7.0.U.bin (1.7.0.U)
 weafamb                 :  (APID:0, IP:0.0.0.0)
                         :  ()
WEC8500/configure/remote-ap-group rUpgrade/upgrade# show remote-ap-
group upgrade list rUpgrade

  /* (RC/FR/RC) : RetryCount/FailReason/RebootCause
 AP_ID Model    Version(config/current)    Status(RC/FR/RC)   MasterAp
    1  WEA303i Remote/1.7.0.U2   DownloadSuccess( 0/  0/128) MasterApCfg
    2  WEA312i Remote/1.7.0.U2   DownloadSuccess( 0/  0/146) -
    3  WEA303i Remote/1.7.0.U2   DownloadSuccess( 0/  0/146) -
```

Configuration using Web UI

Administration > Package Upgrade > Remote AP Group

Example:



REMOTE AP GROUP NAME	rUpgrade	
REMOTE AP UPGRADE	● Enable ○ Disable	
REMOTE AP UPGRADE STATUS	-	
FORCE UPGRADE	○ Enable ● Disable	
SELECT AP PACKAGE	300 series (weafama) weafama_1.7.0.U1.bin Family: weafama Version: 1.7.0.U1 Build Date: Mon Mar 3 19:32:46 KST 2014 Size: 37712000 CRC: f1698883	400 series (weafamb) ----------
CURRENT AP PACKAGE	300 series (weafama) Package Version : 1.7.0.U Package File Name : weafama_1.7.0.U.bin	400 series (weafamb) Package Version : - Package File Name : -

Figure 95. Starting AP Upgrade

4.2.8.5 Restarting and Upgrading AP

After downloading the AP package, APs in the remote group are restarted so that they can run on the upgraded version.

Configuration using CLI

Example:

```
WEC8500# configure terminal
WEC8500/configure# remote-ap-group rUpgrade
WEC8500/configure/remote-ap-group rUpgrade# reboot upgrade
```

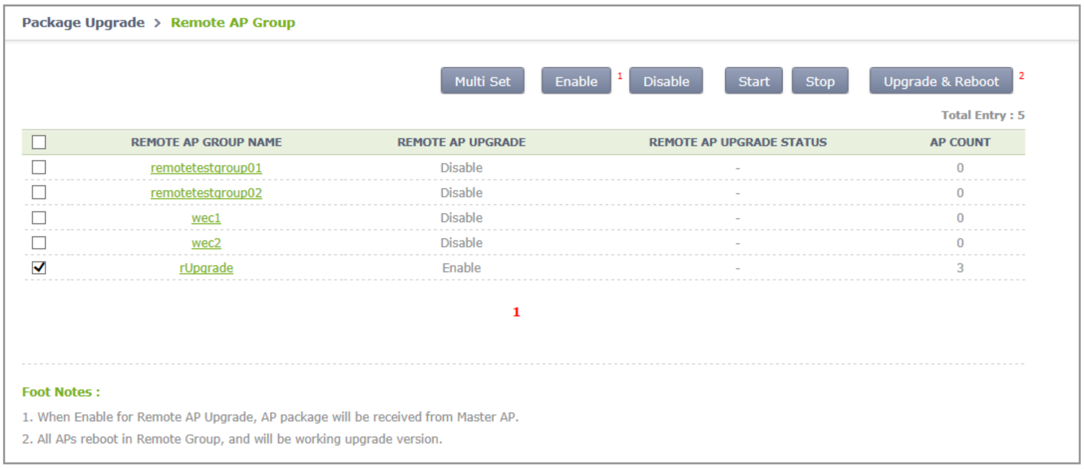
CLI for checking configuration:

```
WEC8500# show remote-ap-group upgrade config rUpgrade

================== Remote Ap Group Upgrade Config ==================

 Group Name            : rUpgrade
 Enable                : Enable
 Type                  : Default
 Mode                  : FTP
 Path                  : package/ap
 PortNum               : 21
 MAXretries            : 3
 ForceOption           : Disable

 weafama               : ap_1 (APID:1, IP:10.10.10.160)
                       : weafama_1.7.0.U.bin (1.7.0.U)
 weafamb               :  (APID:0, IP:0.0.0.0)
                       :  ()
WEC8500/configure/remote-ap-group rUpgrade/upgrade# show remote-ap-
group upgrade list rUpgrade

   /* (RC/FR/RC) : RetryCount/FailReason/RebootCause
 AP_ID  Model  Version(config/current)  Status(RC/FR/RC)    MasterAp
    1  WEA303i    Remote/1.7.0.U        Success( 0/ 0/128)  MasterApCfg
    2  WEA312i    Remote/1.7.0.U        Success( 0/ 0/146)  -
    3  WEA303i    Remote/1.7.0.U        Success( 0/ 0/146)  -
```

Configuration using Web UI

Administration > Package Upgrade > Remote AP Group

Example:



Package Upgrade > Remote AP Group

Total Entry : 5

□	REMOTE AP GROUP NAME	REMOTE AP UPGRADE	REMOTE AP UPGRADE STATUS	AP COUNT
□	remotetestgroup01	Disable	-	0
□	remotetestgroup02	Disable	-	0
□	wec1	Disable	-	0
□	wec2	Disable	-	0
☑	rUpgrade	Enable	-	3

1

Foot Notes :

1. When Enable for Remote AP Upgrade, AP package will be received from Master AP.
2. All APs reboot in Remote Group, and will be working upgrade version.

Figure 96. Restarting and Upgrading AP

CHAPTER 5. WLAN Management

This chapter describes how to create and configure WLAN that is the most fundamental basis for W-EP wireless LAN service.

5.1 WLAN Configuration

5.1.1 Basic WLAN Configuration

The WLAN profile helps configure and manage the WLAN connection service of an AP in the APC. To use WLAN service, it is necessary to basically configure AP group and interface group and specify Service Set Identifier (SSID).

Configuration using CLI

Go to the wlan configuration mode from the configure mode of CLI.

```
WEC8500# configure terminal
WEC8500/configure# wlan [WLAN ID]
```

Parameter	Description
WLAN_ID	WLAN ID (range: 1-255)

The WLAN configuration procedures are as follows:

1) Go to configure → wlan configuration mode of CLI.

```
WEC8500# configure terminal
WEC8500/configure# wlan 1
WEC8500/configure/wlan 1#
```

2) Add WLAN to an AP group.
Configure an AP group to which WLAN service will be provided. The AP group configuration is only possible in the AP group configuration mode instead of the wlan configuration mode. The below configuration allocates wlan 1 to the apg_01 AP group.

> NOTE
>
> A newly created WLAN is added to the 'default' AP group if the WLAN ID is in the range of 1-16. If its WLAN ID is 17 or above, the WLAN is not included in the AP group.

Maximum 16 WLANs can be allocated to each AP group.

```
WEC8500# configure terminal
WEC8500/configure# ap-group apg_01
WEC8500/configure/ap-group apg_01# add-wlan 1
```

3) Configure an interface group to which the WLAN service will be provided.
Several VLAN interfaces can be added to an interface group, and the WLAN service is available only through the interface.
   - if-group [INTERFACE_GROUP_NAME]

4) Configure a SSID. The SSID is an ID used to connect to each wireless terminal to provide the WLAN service.
Make sure to configure a SSID to use the WLAN service.
   - ssid [SSID_NAME]

5) Configure radio by selecting 2.4G, 5G or All (2.4G/5G).
   - radio [Radio ID: 1: 5 GHz, 2: 2.4 GHz, 3: ALL]

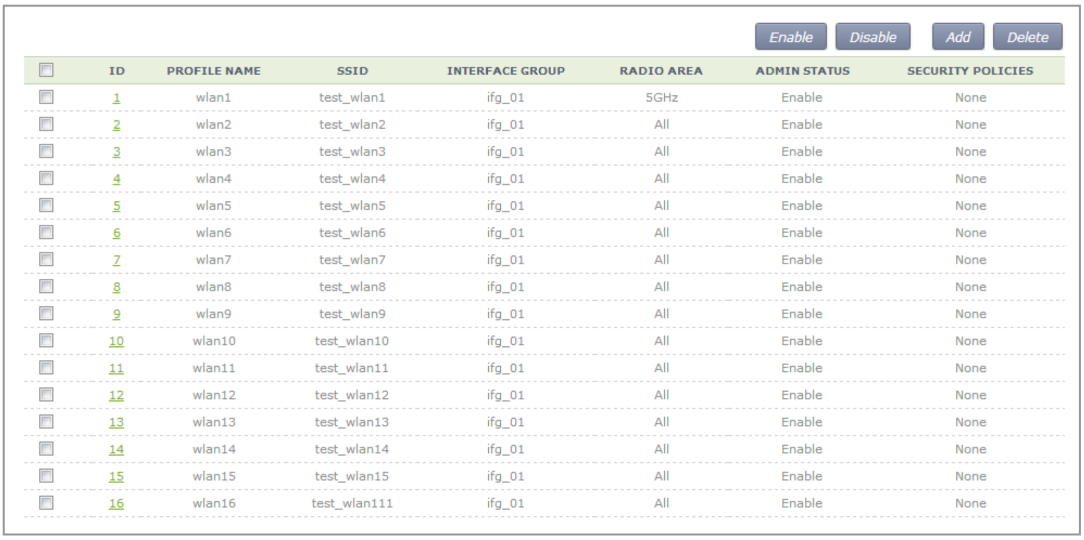
6) Configure whether to apply the WLAN service.

```
WEC8500/configure/wlan 1#enable
```

> NOTE
>
> To apply the various WLAN services to multiple wireless terminals, create the WLAN service in a profile format. Once the WLAN service is started, make each AP use the WLAN service by downloading the profile.

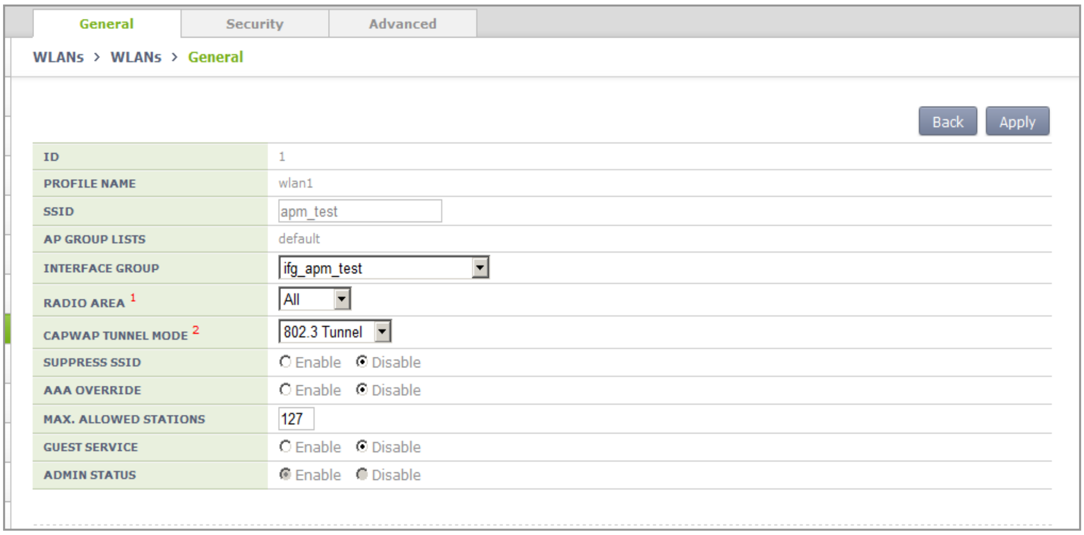
Configuration using Web UI

In the menu bar of <**WEC Main window**>, select <**Configuration**> and then select the <**WLANs**> menu in the sub-menus. Select a WLAN ID to change in the WLANs screen and go to the <**General**> tab. In the screen, you can use various functions such as adding or deleting a WLAN.



□	ID	PROFILE NAME	SSID	INTERFACE GROUP	RADIO AREA	ADMIN STATUS	SECURITY POLICIES
□	1	wlan1	test_wlan1	ifg_01	5GHz	Enable	None
□	2	wlan2	test_wlan2	ifg_01	All	Enable	None
□	3	wlan3	test_wlan3	ifg_01	All	Enable	None
□	4	wlan4	test_wlan4	ifg_01	All	Enable	None
□	5	wlan5	test_wlan5	ifg_01	All	Enable	None
□	6	wlan6	test_wlan6	ifg_01	All	Enable	None
□	7	wlan7	test_wlan7	ifg_01	All	Enable	None
□	8	wlan8	test_wlan8	ifg_01	All	Enable	None
□	9	wlan9	test_wlan9	ifg_01	All	Enable	None
□	10	wlan10	test_wlan10	ifg_01	All	Enable	None
□	11	wlan11	test_wlan11	ifg_01	All	Enable	None
□	12	wlan12	test_wlan12	ifg_01	All	Enable	None
□	13	wlan13	test_wlan13	ifg_01	All	Enable	None
□	14	wlan14	test_wlan14	ifg_01	All	Enable	None
□	15	wlan15	test_wlan15	ifg_01	All	Enable	None
□	16	wlan16	test_wlan111	ifg_01	All	Enable	None

Figure 97. WLAN basic configuration (1)



ID	1
PROFILE NAME	wlan1
SSID	apm_test
AP GROUP LISTS	default
INTERFACE GROUP	ifg_apm_test
RADIO AREA [1]	All
CAPWAP TUNNEL MODE [2]	802.3 Tunnel
SUPPRESS SSID	○ Enable ● Disable
AAA OVERRIDE	○ Enable ● Disable
MAX. ALLOWED STATIONS	127
GUEST SERVICE	○ Enable ● Disable
ADMIN STATUS	● Enable ○ Disable

Figure 98. WLAN basic configuration (2)

You can configure various functions such as interface group and SSID, etc.
The configurations available in the General tab are as follows:

- INTERFACE GROUP: Configures an interface group.
- RADIO AREA: Configures a radio area.
- CAPWAP TUNNEL MODE/LOCAL VLAN: Configures the local switching function.
- SUPRESS SSID: Enables or disables the function.
- AAA OVERRIDE: If the WLAN is enabled with the device authentication function using a AAA server, the AAA-override function can be enabled so that the user-specific settings configured in the AAA server are applied with priority over the APC settings.
- MAXIMUM ALLOWED STATIONS: Limits the number of users per WLAN.
- GUEST SERVICE: Enables or disables the Guest service.
- ADMIN STATUS: Enables or disables the function.

5.1.2 WLAN Additional Configuration

Each wireless terminal can receive a differentiated service according to the WLAN configuration. The procedure of configuring the WLAN additional function is as follows.

Configuration using CLI

1) Go to configure → wlan configuration mode of CLI.

```
WEC8500# configure terminal
WEC8500/configure# wlan 1
WEC8500/configure/wlan 1
```

2) If the WLAN is enabled with the device authentication function using a AAA server, the AAA-override function can be enabled so that the user-specific settings configured in the AAA server are applied with priority over the APC settings.

```
WEC8500/configure/wlan 1# aaa-override
```

3) Determine whether to configure the Guest service.
   - guest-flag

4) Configure a VLAN ID to use locally.
   - local-vlan [VLAN_ID]

Parameter	Description
VLAN_ID	VLAN ID (range: 1-4094)

5) Specify the service MAC type.
   - mac-type [MAC_TYPE]

Parameter	Description
MAC_TYPE	- localMac: An AP itself provides data service. - splitMac: Provides data service through the APC.

6) Select a radio bandwidth to provide the WLAN service.
   - radio [RADIO]

Parameter	Description
RADIO	- 1: 5 GHz - 2: 2.4 GHz - 3: Supports both 5/2.4 GHz

7) Select whether to provide the SSID as hidden. If it is set to ‘hidden’, the SSID is not found when other devices do searching.
   - suppress-ssid

8) Select the tunnel mode.
   - tunnel-mode [TUNNEL_MODE]

Parameter	Description
TUNNEL_MODE	- LocalBridging: Make all the user traffics are bridged at the AP. - 8023Tunnel: Make all the user traffics are transmitted in the 802.3 format (Not supported if the MAC type is split mac).

Configuration using Web UI

In the menu bar of <**WEC Main window**>, select <**Configuration**> and then select the <**WLANs**> menu in the sub-menus. For more information about configuration, see ‘5.1 Basic WLAN Configuration’.

5.1.3 WLAN-based ACL Configuration

To configure ACL to apply to the WLAN service, define IP-based ACL first and then configure it to the WLAN.

Configuration using CLI

The procedures for configuration are as follows.

1) Before applying ACL, retrieve ACL that is configured as WLAN ACL.

```
WEC8500# show running-config network

fqm-mode
…
ip access-group wireless acl1
!
```

2) Go to configure → wlan configuration mode of CLI.

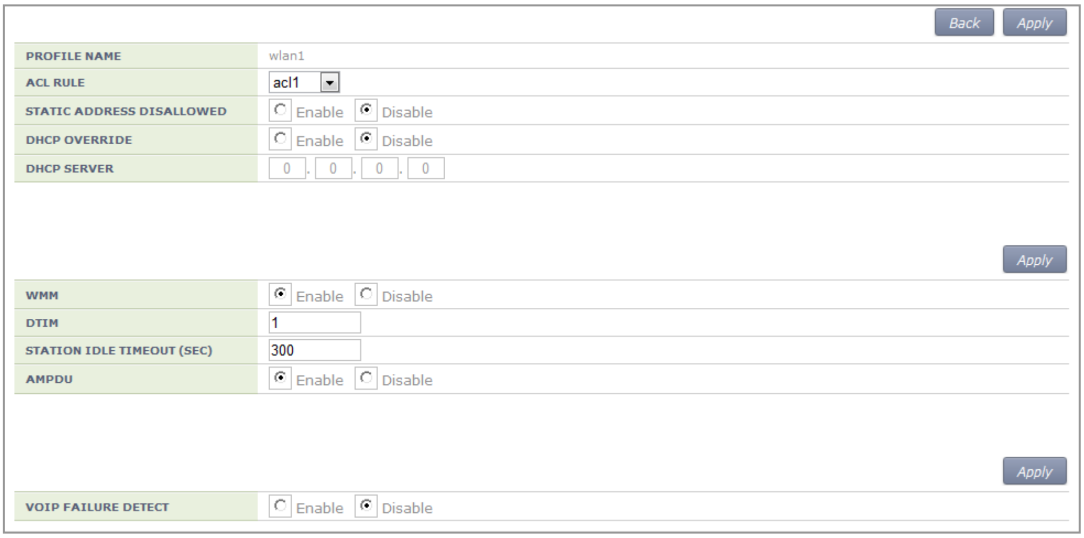
```
WEC8500# configure terminal
WEC8500/configure# wlan 1
WEC8500/configure/wlan 1
WEC8500# configure terminal
WEC8500/configure# wlan 1
WEC8500/configure/wlan 1
```

3) Among retrieved ACLs, enter an ACL name to apply to the WLAN with the ‘acl’ command.
   - acl [ACL-NAME]

4) To check the configured ACL, use the ‘show wlan detail’ command.

Configuration using Web UI

In the menu bar of **<WEC Main window>**, select **<Configuration>** and then select the **<WLANs>** menu in the sub-menus. Select a WLAN ID to change in the WLANs screen and go to the **<Advanced>** tab.



PROFILE NAME	wlan1
ACL RULE	acl1
STATIC ADDRESS DISALLOWED	○ Enable ● Disable
DHCP OVERRIDE	○ Enable ● Disable
DHCP SERVER	0 . 0 . 0 . 0
WMM	● Enable ○ Disable
DTIM	1
STATION IDLE TIMEOUT (SEC)	300
AMPDU	● Enable ○ Disable
VOIP FAILURE DETECT	○ Enable ● Disable

Figure 99. WLAN-based ACL configuration

- ACL RULE: Configures the WLAN-based ACL function.
- STATIC ADDRESS DISALLOWED
- DHCP OVERRIDE
- DHCP SERVER: Enter a DHCP server IP address.
- WMM: Configures the WiFi Multimedia (WMM) mode.
- DTIM: Enter a Delivery Traffic Indication Message (DTIM) value (1-255).
- STATION IDLE TIMEOUT: Enter a station idle timeout value. The value range is 30-3600 and it must be the multiple of 15.
- VOIP FAILURE DETECT: Configures call failure detection.

5.1.4 Managing Root Service

To provide a wireless LAN service where cable installation is difficult, a W-EP AP can be configured as a repeater mode to relay wireless LAN traffics. To configure this kind of network, the Repeater AP and Root AP are required. The Repeater AP is working as a wireless terminal and the Root AP connects a Repeater AP to a wireless terminal for connection to the APC.
The root AP must be enabled with the repeater service to allow repeater AP connections.

Configuration using CLI

1) Go to configure → apc configuration mode of CLI.

```
WEC8500# configure terminal
WEC8500/configure# apc
WEC8500/configure/apc#
```

2) Enable or disable the repeater service. The repeater service must be enabled for the repeater AP to connect to the root AP.
   - repeater-service: Enabled
   - no repeater-service: Disabled

3) Use the ‘show wlan detail repeater’ command to check the root WLAN settings.

```
WEC8500/configure/apc# show wlan detail repeater
```

[Changing to Root AP]
The procedure of changing a W-EP AP to a Root AP is as follows:

1) Go to configure mode of CLI.

```
WEC8500# configure terminal
```

2) Check the registered AP list.

```
WEC8500/configure# show ap summary
```

3) Go to AP configuration mode to change to a Root AP.

```
WEC8500/configure# ap ap_1
```

4) Configure it to a Root AP.

```
WEC8500/ configure/ap ap_1# profile ap-mode rootAp
```

5) Restart the configured AP.

[Changing to Repeater AP]

The procedure of changing a W-EP AP to a Repeater AP is as follows:

1) Go to configure mode of CLI.

```
WEC8500# configure terminal
```

2) Check the registered AP list.

```
WEC8500/configure# show ap summary
```

3) Go to AP configuration mode of an AP that will be changed to a Repeater AP.

```
WEC8500/configure# ap ap_2
```

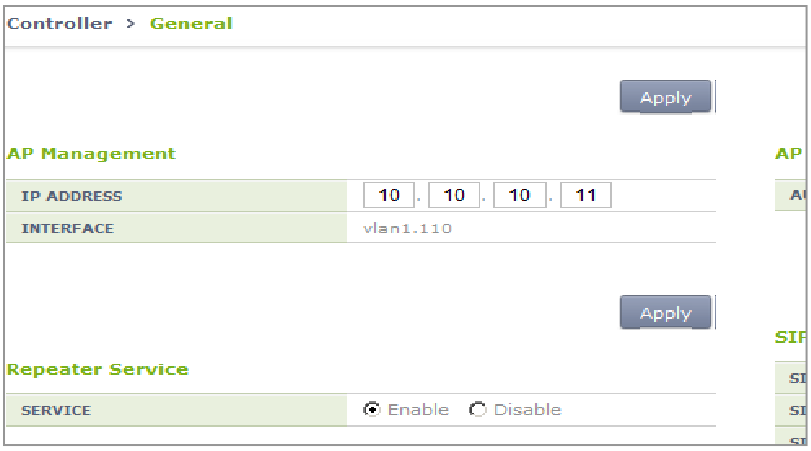
4) Configure it to a Repeat AP.

```
WEC8500/configure/ap ap_2# profile ap-mode repeaterAp
```

5) Restart the configured AP.

Configuration using Web UI

In the menu bar of <**WEC Main window**>, select <**Configuration**> and then select the <**Controller**> → <**General**> menu in the sub-menus. To enable repeater service, configure the INTERFACE GROUP in the Repeater Service of the window, select Enable in the SERVICE, and click the <**Apply**> button.



AP Management

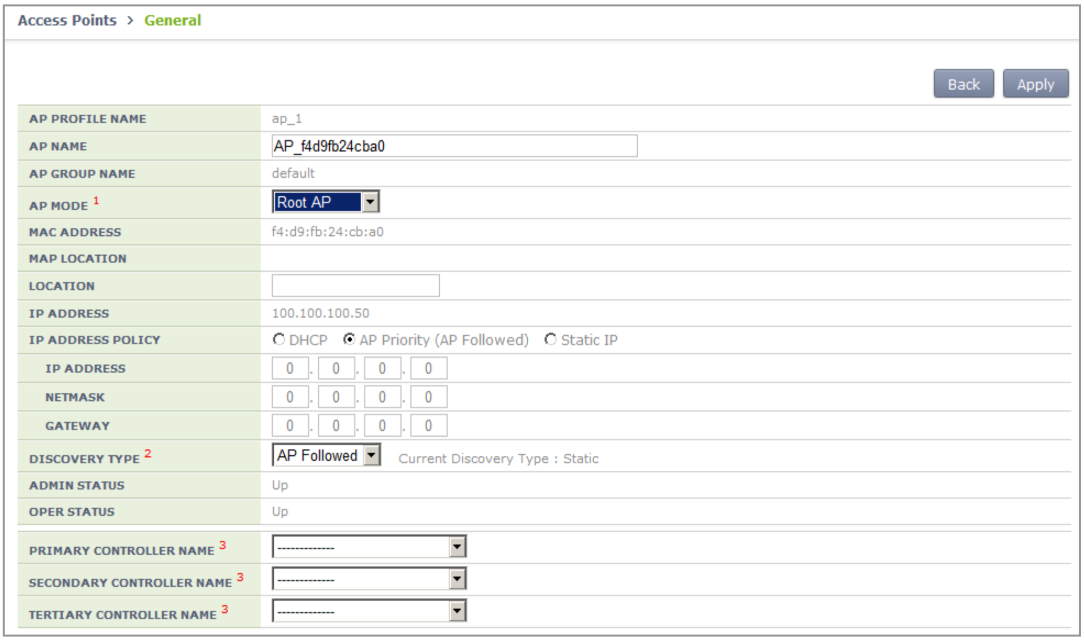
IP ADDRESS	10 . 10 . 10 . 11
INTERFACE	vlan1.110

Repeater Service

SERVICE	● Enable ○ Disable

Figure 100. Root service management (1)

In the menu bar of <**WEC Main window**>, select <**Configuration**> and then select the <**Access Points**> → **AP selection** → <**General**> menu in the sub-menus.
After selecting AP MODE item, click the <**Apply**> button and restart the AP.



AP PROFILE NAME	ap_1
AP NAME	AP_f4d9fb24cba0
AP GROUP NAME	default
AP MODE [1]	Root AP
MAC ADDRESS	f4:d9:fb:24:cb:a0
MAP LOCATION	
LOCATION	
IP ADDRESS	100.100.100.50
IP ADDRESS POLICY	○ DHCP ● AP Priority (AP Followed) ○ Static IP
IP ADDRESS	0 . 0 . 0 . 0
NETMASK	0 . 0 . 0 . 0
GATEWAY	0 . 0 . 0 . 0
DISCOVERY TYPE [2]	AP Followed Current Discovery Type : Static
ADMIN STATUS	Up
OPER STATUS	Up
PRIMARY CONTROLLER NAME [3]	-------------
SECONDARY CONTROLLER NAME [3]	-------------
TERTIARY CONTROLLER NAME [3]	-------------

Figure 101. Root service management (2)

5.2 Local Switching

The APC provides the local switching function to support a service to an individual network such as a branch office. The local switching function enables an AP to be connected to WAN for external connection in an individual network where the APC is not installed. The control packet of an AP and a wireless terminal is processed in the centralized APC and a general data packet is processed in an individual network. Therefore, if the tunnel mode of the WLAN is changed to local switching, part of the data packet forwarding process performed by the APC is performed by the AP.

The following AP functions must be configured in the WLAN which is configured for local switching:

1) WLAN-VLAN Mapping
   - The wireless device traffic connected to the configured local switching WLAN is forwarded by the AP with the configured VLAN tag.
2) ACL
   - Packet filtering ACL is performed for the wireless device traffic connected to the configured local switching WLAN.
3) Preauthetication ACL of Captive Portal
   - Web preauthentication packet forwarding ACL is processed for the wireless device traffic connected to the local switching WLAN configured for captive portal.

The functions above are activated only for the APs added to the remote AP group.

Configuration using CLI

The procedure of local switching configuration is as follows:

1) By referring to the ‘Configuring Remote AP Group’, add an AP to a remote AP group.

2) Enter into the configure → wlan configuration mode of CLI, and configure ‘tunnel-mode’ to ‘local-bridging’.

```
WEC8500# configure terminal
WEC8500/configure# wlan 1
WEC8500/configure/wlan 1# tunnel-mode local-bridging
```

- tunnel-mode local-bridging

3) Enter into the configure → AP configuration mode of CLI, and configure a local Vlan ID per WLAN.

```
WEC8500# configure terminal
WEC8500/configure# ap ap_1
```

```
WEC8500/configure/ap ap_1# profile
WEC8500/configure/ap ap_1/profile#
```

- local-bridging [WLAN_ID][VLAN_ID/ACL_NAME/PRE_AUTH_ACL_NAME]

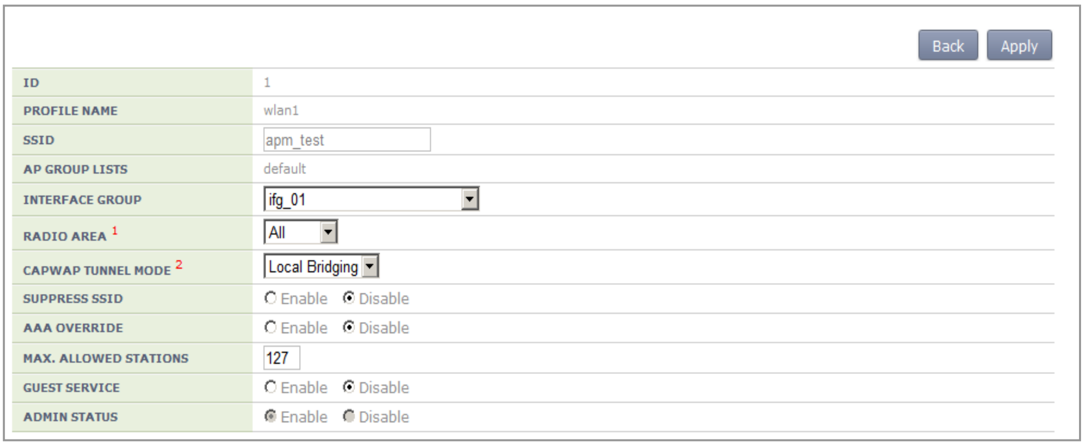
Parameter	Description
WLAN_ID	WLAN ID (Range: 1-254) (available only for WLANs the tunnel-mode of which is local-bridging)
VLAN_ID	VLAN ID (Range: 1-4094)
ACL_NAME	ACL name to configure for the WLAN service (only for options set in IP ACL)
PRE_AUTH_ACL_NAME	ACL name to configure for pre-authentication of the WLAN (only for options set in IP ACL)

4) Operator can check the configuration information by executing the 'show remote-ap-group summary', 'show wlan detail', 'show ap local-bridging [AP_PROFILE_ NAME]' command.

Configuration using Web UI

By referring to the 'Configuring Remote AP Group', add an AP to a remote AP group.

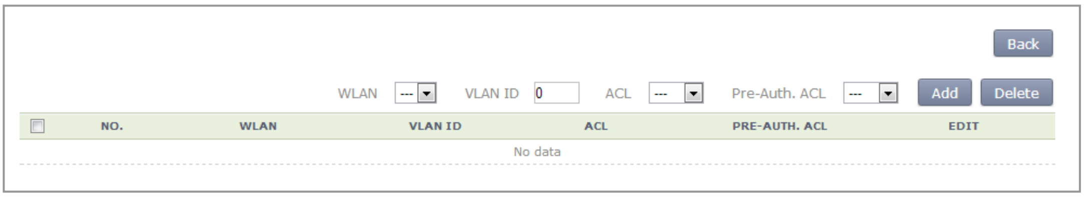
In the menu bar of <**WEC Main window**>, select <**Configuration**> and then select the <**WLANs**> menu in the sub-menus. Select a WLAN ID to change in the WLANs screen and go to the <**General**> tab. After changing the 'CAPWAP TUNNEL MODE' to 'Local Bridging', click the <**Apply**> button.



ID	1
PROFILE NAME	wlan1
SSID	apm_test
AP GROUP LISTS	default
INTERFACE GROUP	ifg_01
RADIO AREA [1]	All
CAPWAP TUNNEL MODE [2]	Local Bridging
SUPPRESS SSID	○ Enable ● Disable
AAA OVERRIDE	○ Enable ● Disable
MAX. ALLOWED STATIONS	127
GUEST SERVICE	○ Enable ● Disable
ADMIN STATUS	● Enable ○ Disable

Figure 102. Local Switching Configuration Window of WLAN

In the menu bar of <**WEC Main window**>, select <**Configuration**> and then select the <**Access Points**> menu in the sub-menus. In the Access Points screen, select an AP to change and go to the <**Remote AP**> tab. Select a WLAN that is configured as local bridging, enter a VLAN ID/ACL/Pre-Auth. ACL, and click the <**Add**> button.



WLAN --- VLAN ID 0 ACL --- Pre-Auth. ACL ---

□	NO.	WLAN	VLAN ID	ACL	PRE-AUTH. ACL	EDIT
			No data			

Figure 103. VLAN/ACL/Pre-Auth.ACL Configuration Window of WLAN Allocated to AP

5.3 Security and Authentication

The Samsung W-EP AP/APC supports the security and authentication function defined in the IEEE 802.11-based wireless LAN security standard and its main mechanism is as follows:

- Wired Equivalent Privacy (WEP)
- Wi-Fi Protected Access Version 1 (WPA1), Wi-Fi Protected Access Version 2 (WPA2)
- Authentication type: Pre-Shared Key (PSK), 802.1X
- Encryption type: Temporal Key Integrity Protocol (TKIP), AES-CCMP

When a new WLAN is added, the initial WLAN security configuration becomes all disabled. Therefore, an operator must configure the security function.

5.3.1 Initialization of WLAN Security Function

This is a procedure to disable WLAN, where the security function is configured, to the initial status.

Configuration using CLI

An example of initializing the security function of wlan 1 is show below.

1) Go to configure → wlan configuration mode of CLI.

```
WEC8500# configure terminal
WEC8500/configure# wlan 1
```

2) After entering into the security configuration mode, use the ‘setDefault’ command to initialize the security configuration.

```
WEC8500/configure/wlan 1# security
WEC8500/configure/wlan 1/security# setDefault
```

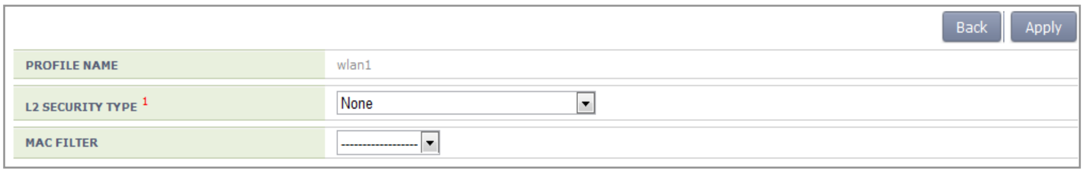
3) After applying the changed configuration, exit the security configuration mode.

```
WEC8500/configure/wlan 1/security# apply
WEC8500/configure/wlan 1/security# exit
```

4) To check configuration information, use the ‘show wlan security summary’ command.

Configuration using Web UI

In the menu bar of <**WEC Main window**>, select <**Configuration**> and then select the <**WLANs**> menu in the sub-menus. Select a WLAN ID to change in the WLANs screen and go to the <**Security**> → <**L2**> tab.



PROFILE NAME	wlan1
L2 SECURITY TYPE [1]	None
MAC FILTER	----------------

Figure 104. Initialization of WLAN security function

The configuration items available in the window are as follows.

Item		Description
PROFILE NAME		A WLAN configuration name is displayed.
L2 SECURITY TYPE		Layer2 security function type - None: Security function disabled (Select this to initialize the WLAN security function.) - Static WEP: Static WEP security function - 802.1x (Dynamic WEP): Dynamic WEP security function - Static WEP + 802.1x (Dynamic WEP): Static/Dynamic WEP security function - WPA + WPA2: WPA/WPA2 PSK/802.1x security function
WPA POLICY	WPA	WPA Version 1 function is enabled when selected
	ENCRYPTION TYPE	Encryption type - TKIP: TKIP type - CCMP: AES-CCMP type - Both: TKIP, AES-CCMP type
WPA2 POLICY	WPA2	The WPA Version 2 function is always enabled and cannot be changed.
	ENCRYPTION TYPE	The only supported encryption method is CCMP and this cannot be changed. - CCMP: AES-CCMP method
AUTH KEY MGMT	PSK/802.1x	Authentication key management type - PSK: PSK (shared key) authentication type - 802.1x: 802.1x authentication type through a RADIUS server
	PSK FORMAT	PSK key input type - ASCII: ASCII character string - HEX: Hexadecimal value
	PSK KEY	PSK key - 8-63 ASCII character string

Item		Description
		- 64-characters of hexadecimal value
PMK LIFETIME		PMK effective time (unit: s, range: 0-1000000, default: 43200)
EAPOL REAUTHENTICATION PERIOD		EAP re-authentication interval (unit: s, range: 0-100000, default: 0)
STATIC WEP	WEP KEY FORMAT	key input format - ASCII: ASCII character string - HEX: Hexadecimal value
	WEP KEY SIZE	Key length - 40: 40-bit (5-byte) - 104: 104-bit (13-byte)
STATIC WEP	WEP KEY INDEX	Key index (1-4)
	WEP KEY	key value
802.1X(DYNAMIC WEP)	WEP KEY SIZE	Key length - 40: 40-bit (5-byte) - 104: 104-bit (13-byte)

After selecting the L2 Security Type as None, click the <**Apply**> button.

5.3.2 WPA/WPA2 PSK Configuration

The WPA/WPA2 PSK, one of wireless LAN authentication types, can be used in a small size network where an authentication server is not installed.

The procedure of WPA/ WPA2 PSK configuration is as follows.

Configuration using CLI

1) Go to configure → wlan configuration mode of CLI.

```
WEC8500# configure terminal
WEC8500/configure# wlan 1
```

2) Go to security configuration mode and initialize the configuration.

```
WEC8500/configure/wlan 1# security
WEC8500/configure/wlan 1/security# setDefault
```

3) Configure the WPA type.

```
WEC8500/configure/wlan 1/security# [WPA_TYPE]
```

Parameter	Description
WPA_TYPE	WPA type (wpa/wpa2): WPA Version 2 must be enabled at all times. - wpa: WPA Version 1 - wpa2: WPA Version 2

4) Configure the PSK key.

```
WEC8500/configure/wlan 1/security# psk [KEY_TYPE] [KEY_STRING]
```

Parameter	Description
KEY_TYPE	PSK key input format (ascii/hex) - ASCII: ASCII character string - HEX: Hexadecimal value
KEY_STRING	PSK key

5) Configure the encryption type.

```
WEC8500/configure/wlan 1/security# [WPA_TYPE] [ENC_TYPE]
```

Parameter	Description
WPA_TYPE	WPA type (wpa/wpa2): Use the same value as the WPA type configured before. WPA Version 2 must be enabled at all times. - wpa: WPA Version 1 - wpa2: WPA Version 2
ENC_TYPE	Encryption type (tkip/ccmp) - tkip: TKIP type. TKIP cannot be configured for WPA Version 2. - ccmp: AES-CCMP type

6) Configure the key management algorithm to PSK.

```
WEC8500/configure/wlan 1/security# keymgmt psk
```

7) Disable the 802.1x key management algorithm.

```
WEC8500/configure/wlan 1/security# no keymgmt ieee8021x
```

8) Disable the 802.1x authentication.

```
WEC8500/configure/wlan 1/security# no ieee8021x
```

9) After applying the changed configuration, exit the security configuration mode.

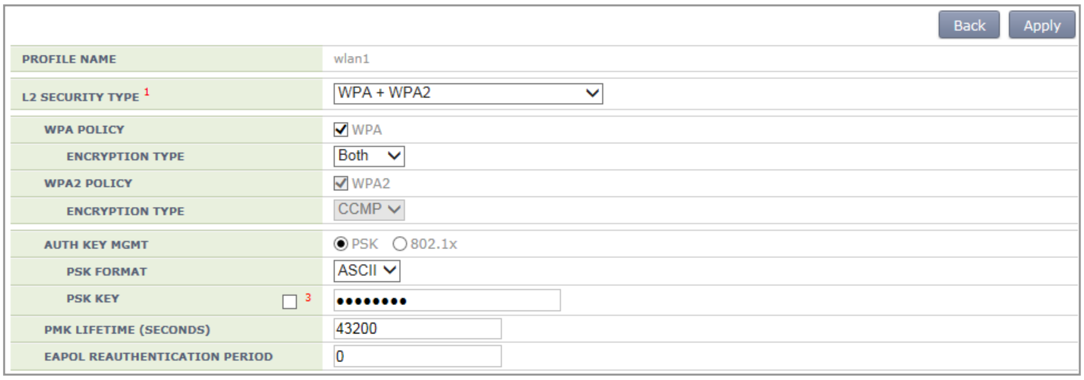
```
WEC8500/configure/wlan 1/security# apply
WEC8500/configure/wlan 1/security# exit
```

10) To check the configuration information, use the following command.

```
WEC8500/configure# show wlan security summary
```

Configuration using Web UI

In the menu bar of **<WEC Main window>**, select **<Configuration>** and then select the **<WLANs>** menu in the sub-menus. Select a WLAN ID to change in the WLANs screen and go to the **<Security>** → **<L2>** tab.



PROFILE NAME	wlan1
L2 SECURITY TYPE [1]	WPA + WPA2
WPA POLICY	☑ WPA
ENCRYPTION TYPE	Both
WPA2 POLICY	☑ WPA2
ENCRYPTION TYPE	CCMP
AUTH KEY MGMT	● PSK ○ 802.1x
PSK FORMAT	ASCII
PSK KEY □ [3]	••••••••
PMK LIFETIME (SECONDS)	43200
EAPOL REAUTHENTICATION PERIOD	0

Figure 105. WPA/WPA2 PSK configuration

After selecting the L2 Security Type as WPA + WPA2 and AUTH KEY MGMT as PSK, click the **<Apply>** button.

For more information about detail configuration item, see ‘5.3.1 Initialization of WLAN Security Function’.

5.3.3 WPA/WPA2 802.1x Configuration

The WPA/WPA2 802.1x, one of wireless LAN authentication types does authentication through an authentication server such as a Remote Authentication Dial-In User Service (RADIUS) server.

To configure WPA/WPA2 802.1x to WLAN, execute the command as follows:

NOTE

As the 802.1x authentication needs interoperation with a RADIUS server, the RADIUS server required for the WLAN security configuration must be configured first. For more information about RADIUS server configuration, see ‘8.1 RADIUS Server Configuration’.

Configuration using CLI

1) Go to configure → wlan configuration mode of CLI.

```
WEC8500# configure terminal
WEC8500/configure# wlan 1
```

2) Go to security configuration mode and initialize the configuration.

```
WEC8500/configure/wlan 1# security
WEC8500/configure/wlan 1/security# setDefault
```

3) Configure the WPA type.

```
WEC8500/configure/wlan 1/security# wpa_type
```

Parameter	Description
wpa_type	WPA type (wpa/wpa2): WPA Version 2 must be enabled at all times. - wpa: WPA Version 1 - wpa2: WPA Version 2

4) Configure the encryption type.

```
WEC8500/configure/wlan 1/security# [WPA_TYPE] [ENC_TYPE]
```

Parameter	Description
WPA_TYPE	WPA type (wpa/wpa2): Use the same value as the WPA type configured before. WPA Version 2 must be enabled at all times. - wpa: WPA Version 1 - wpa2: WPA Version 2

Parameter	Description
ENC_TYPE	Encryption type (tkip/ ccmp) - tkip: TKIP type. TKIP cannot be configured for WPA Version 2. - ccmp: AES-CCMP type

5) Disable the PSK key management algorithm.

```
WEC8500/configure/wlan 1/security# no keymgmt psk
```

6) Configure the key management algorithm to 802.1x.

```
WEC8500/configure/wlan 1/security# keymgmt ieee8021x
```

7) Enable the 802.1x authentication.

```
WEC8500/configure/wlan 1/security# ieee8021x
```

8) After enabling the RADIUS server function for authentication, specify the index of authentication RADIUS server. The RADIUS server information must be configured in advance.

```
WEC8500/configure/wlan 1/security# radius-server auth-servers
[RADIUS_SERVER_ID_LIST]
```

Parameter	Description
RADIUS_SERVER_ID_LIST	RADIUS server ID list (Up to 3 IDs can be configured.)

9) After enabling the RADIUS server function for accounting, specify the index of account RADIUS server. The RADIUS server information must be configured in advance.

```
WEC8500/configure/wlan 1/security# radius-server acct-servers
[RADIUS_SERVER_ID_LIST]
```

Parameter	Description
RADIUS_SERVER_ID_LIST	RADIUS server ID list (Up to 3 IDs can be configured.)

10) After applying the changed configuration, exit the security configuration mode.

```
WEC8500/configure/wlan 1/security# apply
WEC8500/configure/wlan 1/security# exit
```

11) To check the configuration information, use the following command.

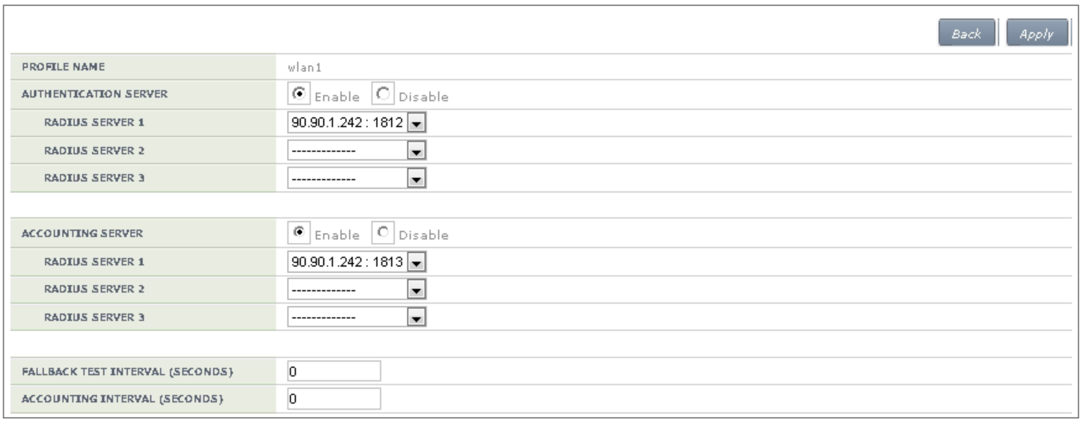
```
WEC8500/configure# show wlan security summary
```

12) To check configuration information, use the 'show wlan security summary' command.

Configuration using Web UI

In the menu bar of <**WEC Main window**>, select <**Configuration**> and then select the <**WLANs**> menu in the sub-menus.

1) Select a WLAN ID to change in the WLANs screen and go to the <**Security**> → <**Radius**> tab.



PROFILE NAME	wlan1
AUTHENTICATION SERVER	● Enable ○ Disable
RADIUS SERVER 1	90.90.1.242 : 1812
RADIUS SERVER 2	-------------
RADIUS SERVER 3	-------------
ACCOUNTING SERVER	● Enable ○ Disable
RADIUS SERVER 1	90.90.1.242 : 1813
RADIUS SERVER 2	-------------
RADIUS SERVER 3	-------------
FALLBACK TEST INTERVAL (SECONDS)	0
ACCOUNTING INTERVAL (SECONDS)	0

Figure 106. WPA/WPA2 802.1x Configuration (1)

Item		Description
PROFILE NAME		A WLAN configuration name is displayed.
AUTHENTICATION SERVER	Enable/ Disable	Whether the authentication function is enabled. - Enable: The authentication function is enabled. - Disable: The authentication function is disabled.
	RADIUS SERVER 1	Authentication server that will be used as the first priority (Can select one out of pre-configured RADIUS servers.)
	RADIUS SERVER 2	Authentication server that will be used as the second priority (Can select one out of pre-configured RADIUS servers.)
	RADIUS	Authentication server that will be used as the third priority

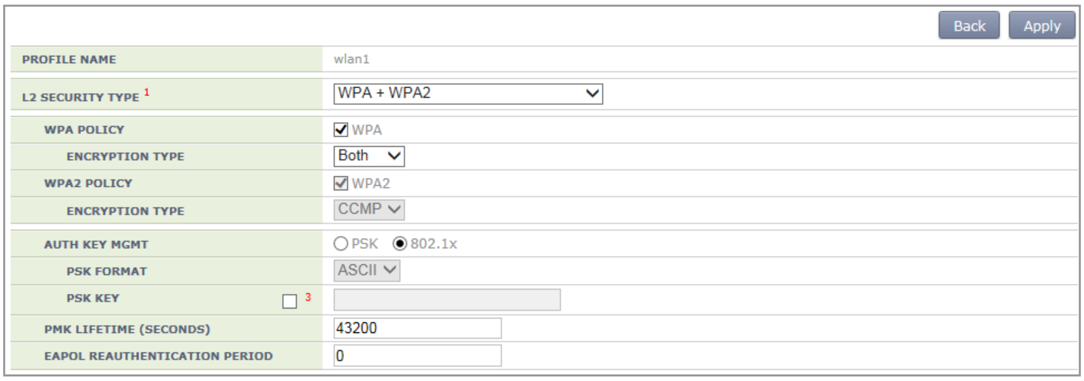
Item		Description
	SERVER 3	(Can select one out of pre-configured RADIUS servers.)
ACCOUNTING SERVER	Enable/ Disable	Whether the accounting function is enabled. - Enable: The accounting function is enabled. - Disable: The accounting function is disabled.
	RADIUS SERVER 1	Accounting server that will be used as the first priority (Can select one out of pre-configured RADIUS servers.)
	RADIUS SERVER 2	Accounting server that will be used as the second priority (Can select one out of pre-configured RADIUS servers.)
	RADIUS SERVER 3	Accounting server that will be used as the third priority (Can select one out of pre-configured RADIUS servers.)
FALLBACK TEST INTERVAL		RADIUS server Fallback attempt interval (unit: s, range: 0-500, default: 0), When set to 0, the fallback function is disabled.
ACCOUNTING INTERVAL		Accounting information transmission interval (unit: s, range: 0-10000, default: 600), When set to 0, the periodic accounting information transmission function is disabled.

Select AUTHENTICATION SERVER and ACCOUNTING SERVER as Enable and configure the rest items.

Internal RADIUS Server

Operator can use a RADIUS server in the APC. The internal RADIUS server only supports the authentication function and does not support the accounting or aaa-override, etc. To use an internal RADIUS server, select ‘Internal’ when selecting a RADIUS server during authentication server configuration.

2) Click the **<L2>** tab.



PROFILE NAME	wlan1
L2 SECURITY TYPE [1]	WPA + WPA2
WPA POLICY	☑ WPA
ENCRYPTION TYPE	Both
WPA2 POLICY	☑ WPA2
ENCRYPTION TYPE	CCMP
AUTH KEY MGMT	○ PSK ● 802.1x
PSK FORMAT	ASCII
PSK KEY □ [3]	
PMK LIFETIME (SECONDS)	43200
EAPOL REAUTHENTICATION PERIOD	0

Figure 107. WPA/WPA2 802.1x Configuration (2)

Select the L2 Security Type as WPA + WPA2 and AUTH KEY MGMT as 802.1x. After configuring the rest values as required, click the <**Apply**> button.

For more information about detail configuration item of L2 tab, see ‘5.3.1 Initialization of WLAN Security Function’.

5.3.4 Static WEP Configuration

The WEP is a security algorithm defined in the initial wireless LAN standard.
It provides security by using a cryptographic key and Initial Vector (IV) to encrypt the wireless transmission data exchanged between an AP and a wireless terminal connected to a wireless LAN.

Configuration using CLI

For static WEP configuration, execute the following commands.

1) Go to configure → wlan configuration mode of CLI.

```
WEC8500# configure terminal
WEC8500/configure# wlan 1
```

2) Go to security configuration mode and initialize the configuration.

```
WEC8500/configure/wlan 1# security
WEC8500/configure/wlan 1/security# setDefault
```

3) Disable WPA1, WPA2, and 802.1x authentication.

```
WEC8500/configure/wlan 1/security# no wpa
WEC8500/configure/wlan 1/security# no wpa2
WEC8500/configure/wlan 1/security# no ieee8021x
```

4) Enable the WEP.

```
WEC8500/configure/wlan 1/security# wep
```

5) Configure the WEP Shared Key mode.

```
WEC8500/configure/wlan 1/security# wep shared
```

6) Use the following command to configure the cryptographic key of WEP.

```
WEC8500/configure/wlan 1/security# wep encryption [KEY_TYPE]
[KEY_STRING] [KEY_INDEX] [KEY_LENGTH]
```

Parameter	Description
KEY_TYPE	WEP key Input format of WEP cryptographic key (ascii/hex) - ASCII: ASCII character string - HEX: Hexadecimal value
KEY STRING	WEP cryptographic key
KEY_INDEX	Key index (range: 1-4)
KEY_LENGTH	Key length (Bit unit) - 40 - 104

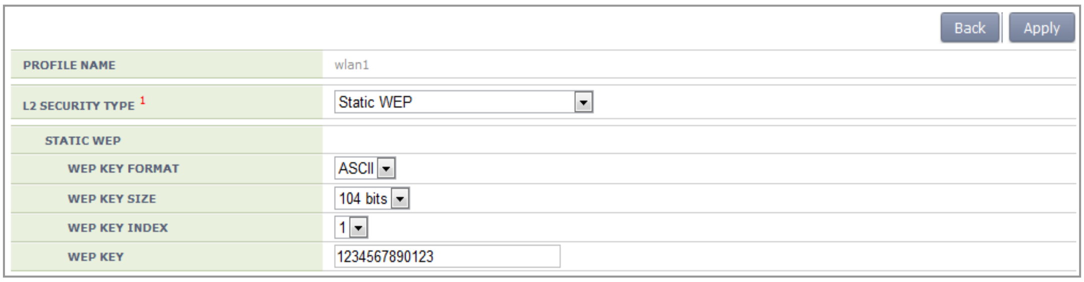
7) After applying the changed configuration, exit the security configuration mode.

```
WEC8500/configure/wlan 1/security# apply
WEC8500/configure/wlan 1/security# exit
```

8) To check configuration information, use the 'show wlan security summary' command.

Configuration using Web UI

In the menu bar of <**WEC Main window**>, select <**Configuration**> and then select the <**WLANs**> menu in the sub-menus. Select a WLAN ID to change in the WLANs screen and go to the <**Security**> → <**L2**> tab.



PROFILE NAME	wlan1
L2 SECURITY TYPE [1]	Static WEP
STATIC WEP	
WEP KEY FORMAT	ASCII
WEP KEY SIZE	104 bits
WEP KEY INDEX	1
WEP KEY	1234567890123

Figure 108. Static WEP configuration

Select the L2 Security Type as Static WEP. After configuring the rest values as required, click the <**Apply**> button.

For more information about detail configuration item of L2 tab, see '5.3.1 Initialization of WLAN Security Function'.

5.3.5 Dynamic WEP Configuration

The Dynamic WEP is a security algorithm that improves the security vulnerabilities of a static WEP by using 802.1x authentication. Unlike the static WEP that is based on a configured fixed key, it creates a cryptographic key by executing 802.1x authentication when a terminal is connected.

Configuration using CLI

For dynamic WEP configuration, execute the command as follows:

1) Go to configure → wlan configuration mode of CLI.

```
WEC8500# configure terminal
WEC8500/configure# wlan 1
```

2) Go to security configuration mode and initialize the configuration.

```
WEC8500/configure/wlan 1# security
WEC8500/configure/wlan 1/security# setDefault
```

3) Enable the 802.1x authentication.

```
WEC8500/configure/wlan 1/security# ieee8021x
```

4) To configure the length of a cryptographic key of dynamic WEP, execute the following command.

```
WEC8500/configure/wlan 1/security# ieee8021x encryption [KEY_LENGTH]
```

Parameter	Description
KEY_LENGTH	Key length (Bit unit) - 40 - 104

5) After enabling the RADIUS server function for authentication, specify the index of authentication RADIUS server. The RADIUS server information must be configured in advance.

```
WEC8500/configure/wlan 1/security# radius-server auth-servers
[RADIUS_SERVER_ID_LIST]
```

Parameter	Description
RADIUS_SERVER_ID_LIST	RADIUS server ID list (Up to 3 IDs can be configured.)

6) After enabling the RADIUS server function for accounting, specify the index of account RADIUS server. The RADIUS server information must be configured in advance.

```
WEC8500/configure/wlan 1/security# radius-server acct-servers
[RADIUS_SERVER_ID_LIST]
```

Parameter	Description
RADIUS_SERVER_ID_LIST	RADIUS server ID list (Up to 3 IDs can be configured.)

7) After applying the changed configuration, exit the security configuration mode.

```
WEC8500/configure/wlan 1/security# apply
WEC8500/configure/wlan 1/security# exit
```

8) To check the configuration information, execute the following command.

```
WEC8500/configure# show wlan security summary
```

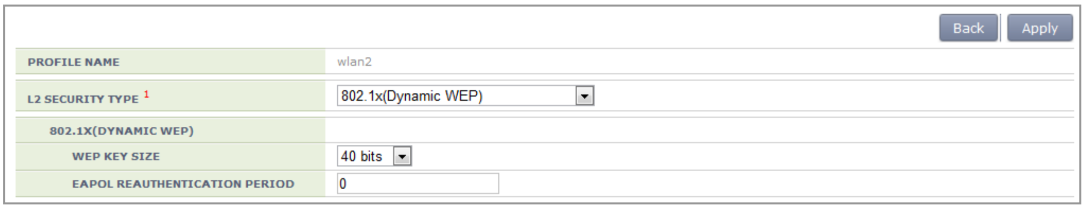
9) To check configuration information, execute the ‘show wlan security summary’ command.

Configuration using Web UI

In the menu bar of <**WEC Main window**>, select <**Configuration**> and then select the <**WLANs**> menu in the sub-menus.

1) Select a WLAN ID to change in the WLANs screen and go to the <**Security**> → <**Radius**> tab. For details about configuration, refer to the section 5.3.3.

2) Click the <**L2**> tab.



PROFILE NAME	wlan2
L2 SECURITY TYPE [1]	802.1x(Dynamic WEP)
802.1X(DYNAMIC WEP)	
WEP KEY SIZE	40 bits
EAPOL REAUTHENTICATION PERIOD	0

Figure 109. Dynamic WEP Configuration Window

Select the L2 Security Type as Dynamic WEP. After configuring the rest values as required, click the <**Apply**> button.
For more information about detail configuration item of L2 tab, see ‘5.3.1 Initialization of WLAN Security Function’.

5.4 DHCP Configuration

The DHCP service of APC consists of DHCP server, DHCP relay, and DHCP proxy.

5.4.1 DHCP Server

5.4.1.1 DHCP Server Configuration

A DHCP server in the APC dynamically allocates an IP address to a client.

Configuration using CLI

1) Go to configure mode of CLI.

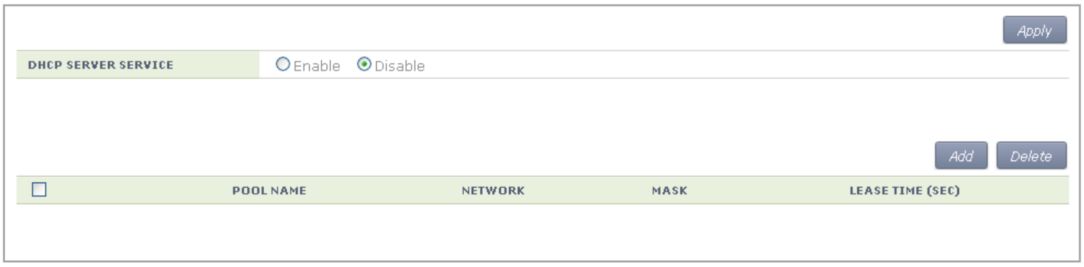
```
WEC8500# configure terminal
WEC8500/configure #
```

2) To enable or disable the DHCP server, enter the ‘ip dhcp’ command. Use ‘no’ in front of the command to disable the configuration.
   - ip dhcp enable
   - no ip dhcp enable

3) To check configuration information, use the ‘show ip dhcp’ command.

Configuration using Web UI

In the menu bar of **<WEC Main window>**, select **<Configuration>** and then select the **<DHCP>** → **<Internal Server>** menu in the sub-menus.



DHCP SERVER SERVICE ○ Enable ● Disable

□	POOL NAME	NETWORK	MASK	LEASE TIME (SEC)

Figure 110. DHCP server configuration

Enable/Disable the DHCP SERVER SERVICE item in the Internal Server window to enable or disable a DHCP server.

5.4.1.2 DHCP Pool

The DHCP pool includes the range of IP address to be allocated to a client, DNS server that will be used by a DHCP client, NTP server, and default router IP address information, etc.

Configuration using CLI

[Pool Creation]

The procedure of creating a pool in an internal DHCP server and entering into the pool mode is as follows:

1) Go to configure mode of CLI.

```
WEC8500# configure terminal
WEC8500/configure #
```

2) Enter the ‘ip dhcp pool’ command. Use ‘no’ in front of the command to delete a DHCP pool.
   - ip dhcp pool [POOL_NAME]
   - no ip dhcp pool [POOL_NAME]

3) To check configuration information, use the ‘show ip dhcp’ command.
   To configure the DHCP Pool related function, execute the command as follows to go to the DHCP pool mode.

```
WEC8500# configure terminal
WEC8500/configure # ip dhcp pool test
WEC8500/configure/ip/dhcp/pool test#
```

[Configuring IP address]

Before configuring a DHCP pool, you should configure a network first. If the network is not configured, you cannot execute other commands.

Enter the command as follows to configure the network bandwidth of a DHCP pool to serve. Enter ‘no’ parameter to delete a configured network bandwidth. After entering a separator ‘/’ after an IP address, enter the length of a netmask address or enter a netmask address after the IP address.

- network [IP_ADDRESS] [NETMASK]
- network [IP_ADDRESS]/[LENGTH]
- no network

Parameter	Description
IP_ADDRESS	IP address
NETMASK	Netmask address
LENGTH	Netmask length

[Configuring Gateway]

This command configures the gateway address of a DHCP client. Enter ‘no’ parameter to delete a configured address.

- default-router [IP_ADDRESS]
- no default-router

Parameter	Description
IP_ADDRESS	Gateway IP address

[Configuring DNS Server]

Up to 3 IP addresses can be configured for a DNS server. Enter ‘no’ parameter to delete a configured DNS server. The lower command ‘all’ is used to delete all the IP addresses of a configured DNS server.

- dns-server [IP_ADDRESS]
- no dns-server [IP_ADDRESS]
- no dns-server all

Parameter	Description
IP_ADDRESS	DNS Server’s IP address

[Configuring Domain Name]

This command configures or deletes a domain name.

- domain-name [DOMAIN]
- no domain-name [DOMAIN]

Parameter	Description
DOMAIN	Domain name to configure (e.g. samsung APC.co.kr)

[Configuring Fixed IP Address to MAC Address]

This command configures a fixed IP address to a specific MAC address or deletes the configuration.

The ‘range’ of IP address to configure cannot be overlapped with the IP range and maximum 255 IP addresses can be configured. In addition, use the ‘no fix-address all’ command to delete all the configured values.

- fix-address [aa:bb:cc:dd:ee:ff A.B.C.D]
- no fix-address [aa:bb:cc:dd:ee:ff A.B.C.D]
- fix-address all

As shown in the below example, 100.100.100.10 can be always allocated to the IP address of a wireless terminal whose MAC address is 11:22:33:44:55:66.

```
WEC8500/configure/ip/dhcp/pool test# fix-address 11:22:33:44:55:66
100.100.100.10
```

[Configuring IP Address Lease Time]

Configure the time when a wireless terminal receives an IP address. The ‘lease infinite’ command configures the time infinitely. If ‘no’ parameter is entered in front of the command, it is configured to 24 hours (default).

- lease [TIME]
- lease infinite
- no lease

Parameter	Description
TIME	Lease time (range: 120-8640000, Unit: s)

[Configuring NTP Server]

Up to 3 IP addresses of a NTP server can be configured or deleted. In addition, use the ‘no ntp-server all’ command to delete all the configured addresses of a NTP server.

- ntp-server [IP_ADDRESS]
- no ntp-server [IP_ADDRESS]
- no ntp-server all

Parameter	Description
IP_ADDRESS	The IP address of the NTP server

[Ping check]

When a DHCP server allocates an IP address to a client, ping check can be used to check if an IP address to allocate is being used in the current network.

- ping-check [enable/disable]

Parameter	Description
enable/disable	Configures whether to use ping check (default: disable)

[Configuring IP Address Range]

A DHCP server configures the range of IP address to allocate to a client. The range of IP address to add is up to 16 and the IP address specified in the range cannot be duplicated with the IP address of fix-address. Enter ‘no’ to delete the range of configured IP address and enter ‘no range all’ to delete all the ranges.

- range [IP_ADDRESS]
- range [IP_ADDRESS1] [IP_ADDRESS2]
- no range [IP_ADDRESS]
- no range [IP_ADDRESS1] [IP_ADDRESS2]
- no range all

Parameter	Description
IP_ADDRESS	IP address. Use to configure one IP address.
IP_ADDRESS1	Start address of IP address range
IP_ADDRESS2	Last address of IP address range

[Capwap Access Controller Address Configuration]

Up to three IP addresses for a Capwap controller can be configured or deleted. Also, all Capwap controller addresses can be deleted using the ‘no capwap-dhcp-option’ command.

- capwap-dhcp-option [IP_ADDRESS]
- no capwap-dhcp-option

Parameter	Description
IP_ADDRESS	IP address of the Capwap Controller

[Configuring Option Data]

Use the ‘user-option’ command to configure or delete the DHCP option. Use ‘no’ to delete each option and use ‘no user-option all’ to delete all the options.

- Option: Up to 254 can be entered (1-254).
- Data type: string (character string), octet (hex string), int (32 bit integer), uint (32-bit unsigned integer), int16 (16-bit integer), uint16 (16-bit unsigned integer), ipaddress (IP address)

- Mode: Can be configured to the active/passive mode.
  - active: Although a client does not request data transmission, the DHCP server transmits user-option data (Default).
  - passive: The DHCP server transmits data upon a client’s request.

Command	Description
- user-option [1-254] string [string] [active/passive] - user-option [1-254] octet aa:bb:cc [active/passive] - user-option [1-254] int [integer] [active/passive] - user-option [1-254] uint [unsigned integer] [active/passive] - user-option [1-254] int16 [16 bit integer] [active/passive] - user-option [1-254] uint16 [16 bit unsigned integer] [active/passive] - user-option [1-254] ipaddress A.B.C.D [active/passive]	Configures an option.
- no user-option [1-254] string [string] [active/passive] - no user-option [1-254] octet aa:bb:cc [active/passive] - no user-option [1-254] int [integer] [active/passive] - no user-option [1-254] uint [unsigned integer] [active/passive] - no user-option [1-254] int16 [16 bit integer] [active/passive] - no user-option [1-254] uint16 [16 bit unsigned integer] [active/passive] - no user-option [1-254] ipaddress A.B.C.D [active/passive]	Deletes a configured option.
no user-option all	Deletes all the configured options.

A usage example is given below.

```
WEC8500/configure/ip/dhcp/pool test# user-option 3 string “hi, there”
active
WEC8500/configure/ip/dhcp/pool test# user-option 200 octet
33:4A:5C:6F:DD passive
WEC8500/configure/ip/dhcp/pool test# user-option 201 int -3000
WEC8500/configure/ip/dhcp/pool test# user-option 202 uint16 300
WEC8500/configure/ip/dhcp/pool test# user-option 203 ipaddress
111.22.22.33
```

[Retrieving Pool Information]

To check the entire information of a DHCP pool, execute the ‘show ip dhcp pool’ command. If you enter a pool name as a parameter as shown in ‘show ip dhcp pool [POOL NAME]’, you can check the information of a specific pool.

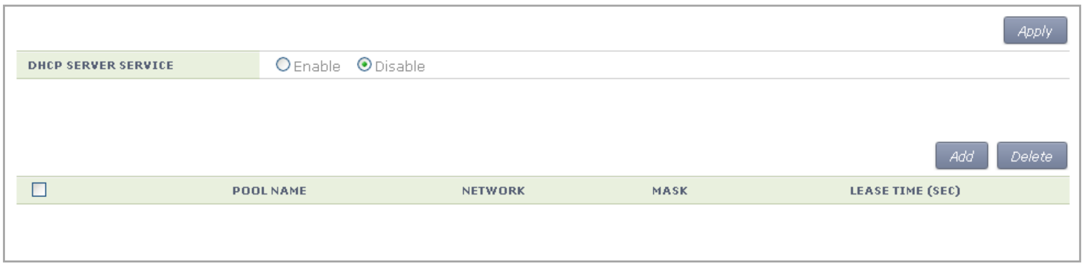
[Retrieving DHCP Lease Information]

To check the DHCP lease information, execute the ‘show ip dhcp lease’ command.

Configuration using Web UI

In the menu bar of **<WEC Main window>**, select **<Configuration>** and then select the **<DHCP>** → **<Internal Server>** menu in the sub-menus.

Click the **<Add>** or **<Delete>** button to add or delete a DHCP pool.

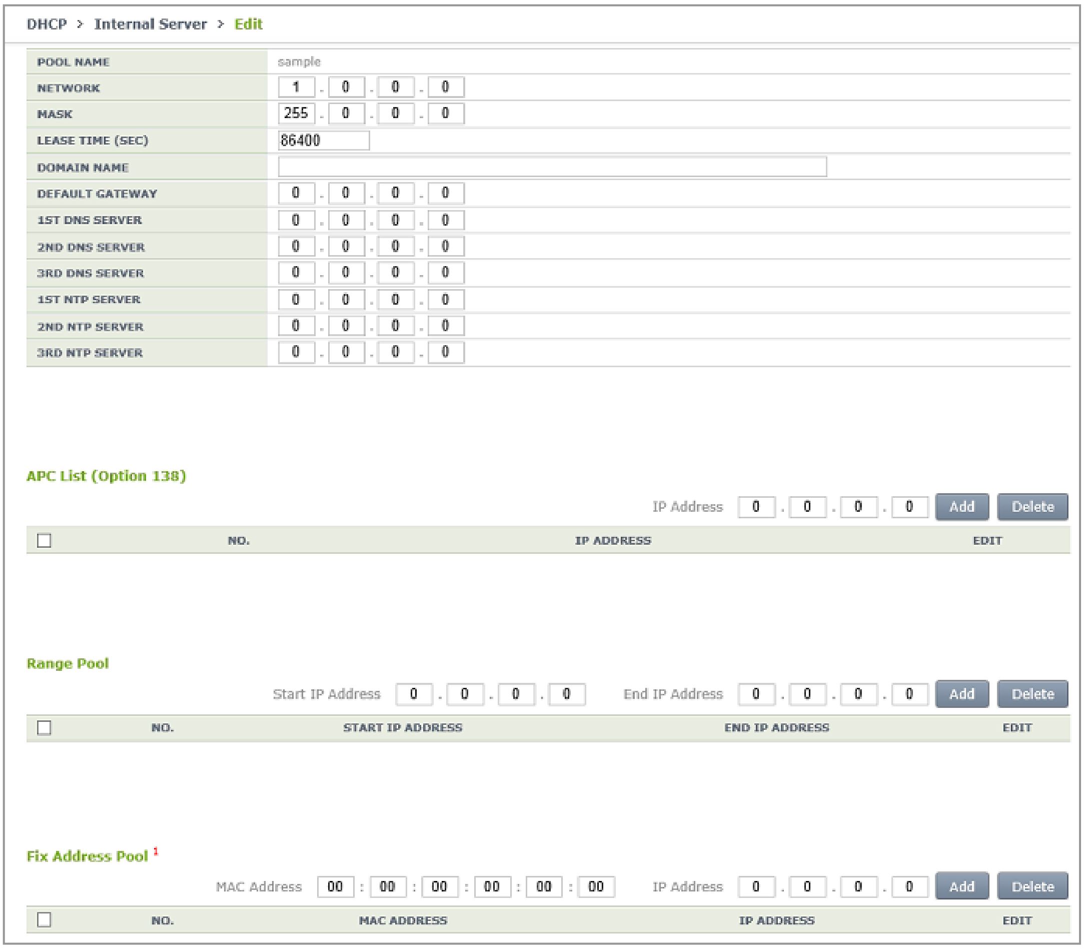


DHCP SERVER SERVICE	○ Enable ● Disable

□	POOL NAME	NETWORK	MASK	LEASE TIME (SEC)

Figure 111. DHCP Pool (1)

The window where a DHCP pool can be added is shown below.



DHCP > Internal Server > Edit

POOL NAME	sample
NETWORK	1 . 0 . 0 . 0
MASK	255 . 0 . 0 . 0
LEASE TIME (SEC)	86400
DOMAIN NAME	
DEFAULT GATEWAY	0 . 0 . 0 . 0
1ST DNS SERVER	0 . 0 . 0 . 0
2ND DNS SERVER	0 . 0 . 0 . 0
3RD DNS SERVER	0 . 0 . 0 . 0
1ST NTP SERVER	0 . 0 . 0 . 0
2ND NTP SERVER	0 . 0 . 0 . 0
3RD NTP SERVER	0 . 0 . 0 . 0

APC List (Option 138)

IP Address 0 . 0 . 0 . 0

□	NO.	IP ADDRESS	EDIT

Range Pool

Start IP Address 0 . 0 . 0 . 0 End IP Address 0 . 0 . 0 . 0

□	NO.	START IP ADDRESS	END IP ADDRESS	EDIT

Fix Address Pool [1]

MAC Address 00 : 00 : 00 : 00 : 00 : 00 IP Address 0 . 0 . 0 . 0

□	NO.	MAC ADDRESS	IP ADDRESS	EDIT

Figure 112. DHCP Pool (2)

- POOL NAME: DHCP pool name (mandatory input item)
- NETWORK: Network bandwidth IP that a DHCP server will serve (mandatory input item)
- MASK: Netmask length IP of an IP that is entered into the NETWORK item (mandatory input item)
- LEASE TIME: DHCP IP address lease time (Unit: s, default: 3600 s, Maximum value: 8640000 s)
- DOMAIN NAME: Configures a domain name that will be used by a DHCP client in a DNS.
- DEFAULT GATEWAY: Gateway IP that will be configured by a DHCP client
- 1ST/2ND/3RD DNS SERVER: Configures a DNS server that will be used by a DHCP client.
- 1ST/2ND/3RD NTP SERVER: Configures a NTP server that will be used by a DHCP client.
- APC List (Option 138): Configures APL list value corresponding to DHCP user option #138.
- Range Pool: Configures the range of IP address that will be leased to a DHCP client. Enter an IP address into the Start IP Address IP box and End Ip Address IP box each and then click the **<Add>** button to create a list. In addition, select one in the created list and click the **<Delete>** button to delete it. The IP address range cannot be overlapped with the IP address in a network bandwidth and also the IP address fixed to a MAC address.
- Fixed Address Pool: Configures a fixed IP address to the MAC address of a specific DHCP client.
  Enter a MAC address and an IP address and click the **<Add>** button to create the list. In addition, select one in the created list and click the **<Delete>** button to delete it. The IP address fixed to a MAC address cannot be overlapped with the IP address in a network bandwidth and also the IP address range.

5.4.1.3 Retrieving Number of DHCP Packets

To check the number of DHCP packets that the DHCP server receives, execute the ‘show ip dhcp statistics’ command.

5.4.2 DHCP Relay

The DHCP relay forwards a DHCP packet received from a client through broadcast to the DHCP server. Because it switches with the DHCP proxy, the DHCP relay is enabled when the DHCP proxy is disabled.
The DHCP relay is working in the unit of interface. It is disabled in the ‘mgmt0’ and ‘lo’ interface. The DHCP relay is not working even when no IP address is configured in the interface.

Configuration using CLI

The procedure of changing to the DHCP relay is as follows:

1) Go to configure mode of CLI.

```
WEC8500# configure terminal
```

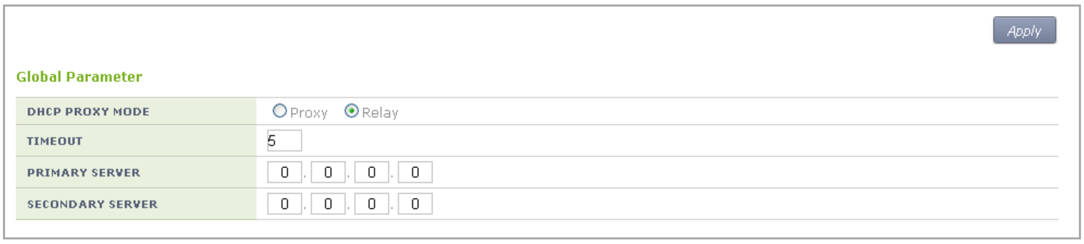
2) Switch to the DHCP relay.
The relay and proxy are operating in the switching mode. If a proxy is not used, it is operating in the relay mode.

```
WEC8500/configure # no ip dhcp-proxy enable
```

3) To check the configured DHCP information, use the ‘show ip dhcp-proxy’ command.

Configuration using Web UI

In the menu bar of **<WEC Main window>**, select **<Configuration>** and then select the **<DHCP>** → **<Proxy>** menu in the sub-menus.
You can configure the Proxy mode of DHCP to relay/proxy. Change the radio box for configuration in the DHCP PROXY MODE of Global Parameter item.



Global Parameter

DHCP PROXY MODE	○ Proxy ● Relay
TIMEOUT	5
PRIMARY SERVER	0 . 0 . 0 . 0
SECONDARY SERVER	0 . 0 . 0 . 0

Figure 113. DHCP Relay

5.4.3 DHCP Proxy

The procedure of changing to the DHCP proxy is as follows.

Configuration using CLI

The CLI configuring a DHCP proxy is located as a command under ‘ip dhcp-proxy’ in the configure mode.

1) Go to configure mode of CLI.

```
WEC8500# configure terminal
```

2) Switch to the DHCP proxy.

```
WEC8500/configure#ip dhcp-proxy enable
```

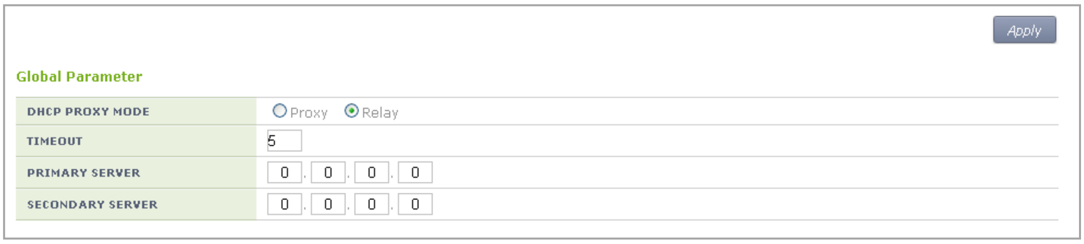
3) To check the configured information, use the ‘show ip dhcp-proxy’ command.

4) Use the below command to check an IP address that is leased through the DHCP proxy.

```
WEC8500t#show ip dhcp proxy-lease
IP address   |    Server IP   |    MAC address    | Lease Expiration time
10.10.10.100      1.1.1.1      00:1c:bf:c1:50:28   2012/08/31 12:00:24
```

Configuration using Web UI

In the menu bar of **<WEC Main window>**, select **<Configuration>** and then select the **<DHCP>** → **<Proxy>** menu in the sub-menus.
You can configure the Proxy mode of DHCP to relay/proxy. Change the radio box for configuration in the DHCP PROXY MODE of Global Parameter item.



Global Parameter

DHCP PROXY MODE	○ Proxy ● Relay
TIMEOUT	5
PRIMARY SERVER	0 . 0 . 0 . 0
SECONDARY SERVER	0 . 0 . 0 . 0

Figure 114. DHCP Proxy

5.4.4 Option 82 Configuration

The APC uses the DHCP Option 82 to provide various services during IP allocation by forwarding the information such as access control, QoS, or security policy, etc. when a wireless terminal connected to an AP receives an IP address.

The Option 82 has two fields, i.e. remote ID and circuit ID. Enter the name of an interface for which the APC constantly does relay/proxy in the circuit ID and enter a part of AP information in the remote ID accordingly. One of the following three data can be used as the remote id of Option 82.

- ap-mac: 802.11 MAC data of the AP. The length is 12-byte (Default).
- ap-mac-ssid: The character string of SSID is added to the data of AP-MAC. The length is variable.
- ap-mac-ssid: Ethernet MAC data of the AP. The length is 12-byte.

To configure Option 82 related functions, go to the interface mode by executing the following command.

```
WEC8500# configure terminal
WEC8500/configure#interface vlan10
WEC8500/configure/interface vlan10#
```

Configuration using CLI

[Configuring Option 82]

This command enables or disables the Option 82 function. It can be configured for each interface.

- dhcp option-82 [MODE]

Parameter	Description
MODE	Configures whether to use the Option 82 function (enable/disable).

[Configuring Remote ID]

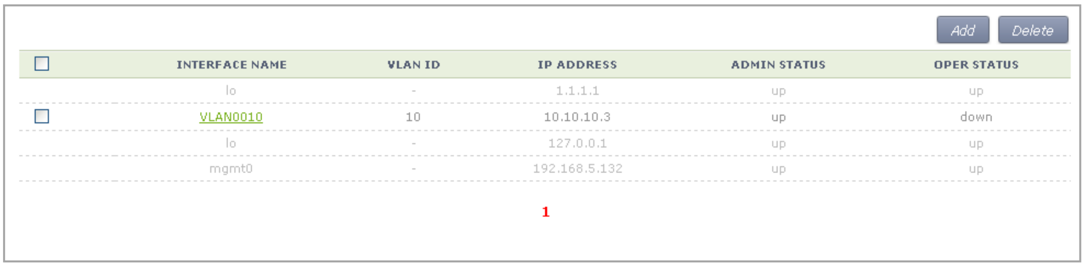
The command is shown below.

- dhcp option-82 remote-id [MODE]

Parameter	Description
MODE	Specifies one out of the following three data to the Option 82 remote-id. - ap-mac: MAC address of an AP - ap-mac-ssid: MAC address and SSID of an AP - ap- ethermac: Ethernet MAC address of an AP

Configuration using Web UI

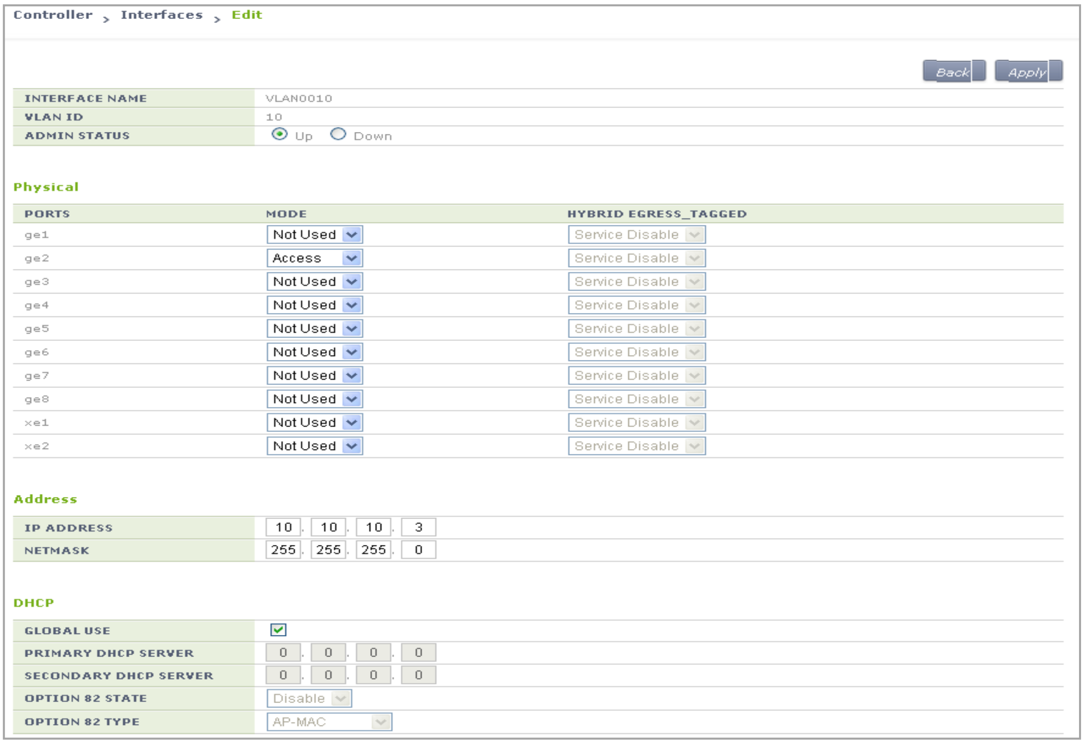
In the menu bar of <**WEC Main window**>, select <**Configuration**> and then select the <**Controller**> → <**Interfaces**> menu in the sub-menus. In the interface, you can see the page where you can change the Option 82.



□	INTERFACE NAME	VLAN ID	IP ADDRESS	ADMIN STATUS	OPER STATUS
	lo	-	1.1.1.1	up	up
□	VLAN0010	10	10.10.10.3	up	down
	lo	-	127.0.0.1	up	up
	mgmt0	-	192.168.5.132	up	up

Figure 115. Option 82 configuration (1)

Select an item in the list and perform detail configuration.



INTERFACE NAME	VLAN0010
VLAN ID	10
ADMIN STATUS	● Up ○ Down

Physical

PORTS	MODE	HYBRID EGRESS_TAGGED
ge1	Not Used	Service Disable
ge2	Access	Service Disable
ge3	Not Used	Service Disable
ge4	Not Used	Service Disable
ge5	Not Used	Service Disable
ge6	Not Used	Service Disable
ge7	Not Used	Service Disable
ge8	Not Used	Service Disable
xe1	Not Used	Service Disable
xe2	Not Used	Service Disable

Address

IP ADDRESS	10 . 10 . 10 . 3
NETMASK	255 . 255 . 255 . 0

DHCP

GLOBAL USE	☑
PRIMARY DHCP SERVER	0 . 0 . 0 . 0
SECONDARY DHCP SERVER	0 . 0 . 0 . 0
OPTION 82 STATE	Disable
OPTION 82 TYPE	AP-MAC

Figure 116. Option 82 configuration (2)

After unchecking the GLOBAL USE check box in the DHCP part, configure OPTION 82 STATE and OPTION 82 TYPE and then click the <**Apply**> button.

In the OPTION 82 STATE, configure Enable/Disable for Option 82 and configure ap-mac, ap-mac-ssid, or ap-ethermac for OPTION 82 TYPE.

5.4.5 Primary/Secondary Server Configuration

The DHCP relay/proxy can transmit a DHCP packet received from a client through broadcast to maximum two DHCP servers. Here, the two servers are called a primary server and a secondary server.

The configuration of primary/secondary servers can be done in the interface mode, but it is also possible in the global mode. If the configuration exists both in the interface mode and global mode, the configuration in the interface mode has a higher priority.

Configuration using CLI

[Configuration at Interface]

1) Go to configure → interface mode of CLI.

```
WEC8500# configure terminal
WEC8500/configure#interface [INTERFACE_NAME]
```

2) Enter the 'dhcp server' command.
To configure only a primary server, do not enter the information of a secondary server.
   - dhcp server primary A.B.C.D secondary A.B.C.D: Configures both primary/ secondary servers.
   - dhcp server primary A.B.C.D: Configures only a primary server.
   - no dhcp server primary A.B.C.D secondary A.B.C.D: Deletes both primary/ secondary servers.
   - no dhcp server primary A.B.C.D: Deletes a primary server.

[Configuration at Global]

1) Go to configure mode of CLI.

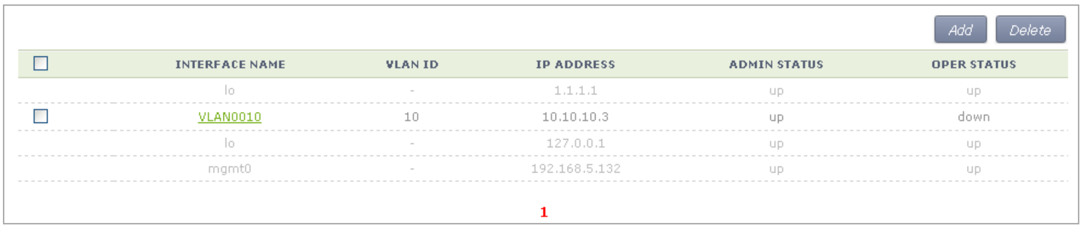
```
WEC8500# configure terminal
WEC8500/configure#
```

2) Enter the 'ip dhcp-proxy default-dhcp-server' command.
To configure only a primary server, do not enter the information of a secondary server.
   - ip dhcp-proxy default-dhcp-server primary A.B.C.D secondary A.B.C.D: Configures both global primary/secondary servers.
   - ip dhcp-proxy default-dhcp-server primary A.B.C.D: Configures only a global primary server.
   - no ip dhcp-proxy default-dhcp-server primary A.B.C.D secondary A.B.C.D: Deletes both global primary/secondary servers.
   - no ip dhcp-proxy default-dhcp-server primary A.B.C.D: Deletes a global primary server.

Configuration using Web UI

[Configuration at Interface]

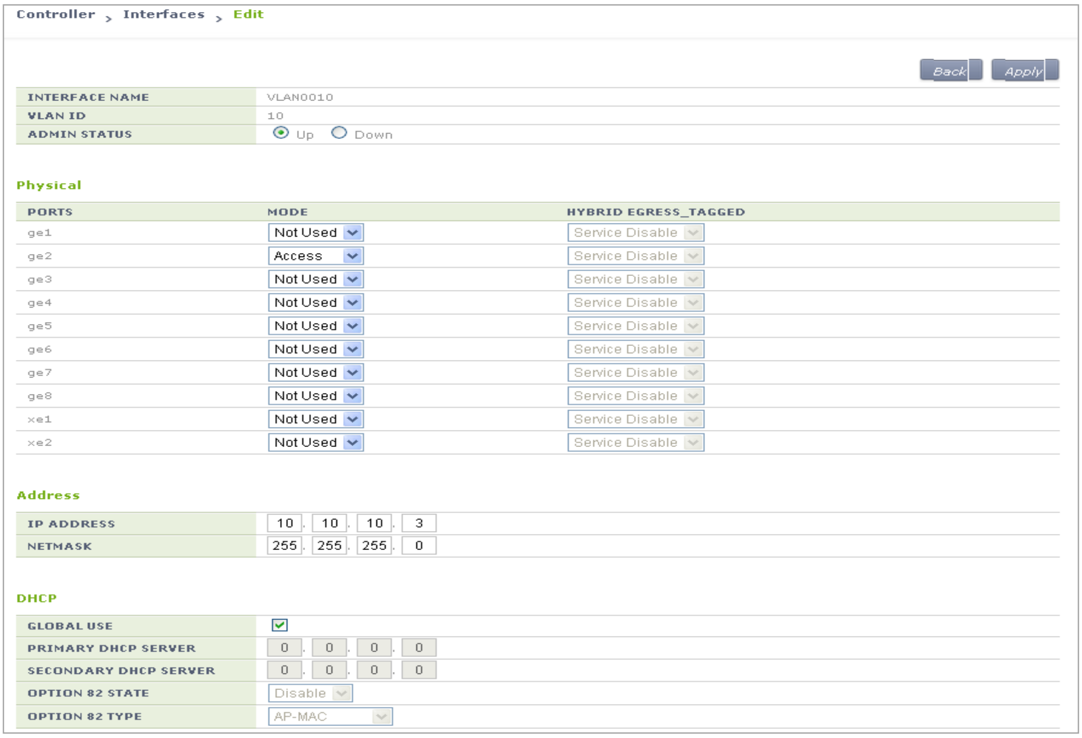
In the menu bar of <**WEC Main window**>, select <**Configuration**> and then select the <**Controller**> → <**Interfaces**> menu in the sub-menus. In the interface, you can see the page where you can change the Option 82.



□	INTERFACE NAME	VLAN ID	IP ADDRESS	ADMIN STATUS	OPER STATUS
	lo	-	1.1.1.1	up	up
□	VLAN0010	10	10.10.10.3	up	down
	lo	-	127.0.0.1	up	up
	mgmt0	-	192.168.5.132	up	up

Figure 117. Primary/Secondary server configuration (1)

Select an item in the list and perform detail configuration.



INTERFACE NAME	VLAN0010
VLAN ID	10
ADMIN STATUS	● Up ○ Down

Physical

PORTS	MODE	HYBRID EGRESS_TAGGED
ge1	Not Used	Service Disable
ge2	Access	Service Disable
ge3	Not Used	Service Disable
ge4	Not Used	Service Disable
ge5	Not Used	Service Disable
ge6	Not Used	Service Disable
ge7	Not Used	Service Disable
ge8	Not Used	Service Disable
xe1	Not Used	Service Disable
xe2	Not Used	Service Disable

Address

IP ADDRESS	10 . 10 . 10 . 3
NETMASK	255 . 255 . 255 . 0

DHCP

GLOBAL USE	☑
PRIMARY DHCP SERVER	0 . 0 . 0 . 0
SECONDARY DHCP SERVER	0 . 0 . 0 . 0
OPTION 82 STATE	Disable
OPTION 82 TYPE	AP-MAC

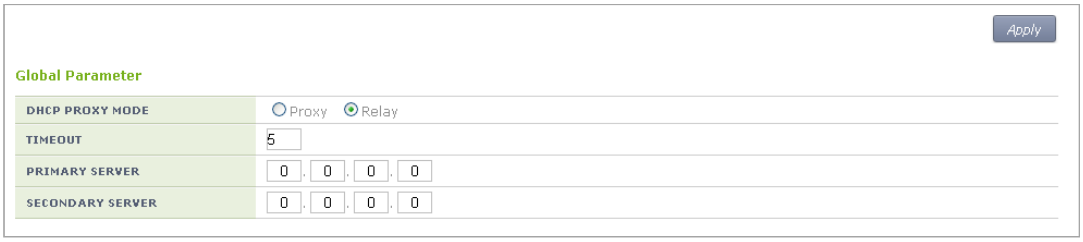
Figure 118. Primary/Secondary server configuration (2)

After unchecking the GLOBAL USE checkbox in the DHCP part, configure PRIMARY DHCP SERVER and 'SECONDARY DHCP SERVER' and then click the <**Apply**> button.

[Configuration at Global]

In the menu bar of **<WEC Main window>**, select **<Configuration**> and then select the **<DHCP>** → **<Proxy>** menu in the sub-menus.

Configure the PRIMARY SERVER and SECONDARY SERVER of the Global Parameter. If you does Global configuration, the configuration is applied to all the interfaces whose ‘GLOBAL USE’ checkbox is checked in the DHCP configuration of APC interface.



Global Parameter

DHCP PROXY MODE	○ Proxy ● Relay
TIMEOUT	5
PRIMARY SERVER	0 . 0 . 0 . 0
SECONDARY SERVER	0 . 0 . 0 . 0

Figure 119. Primary/Secondary server configuration (3)

5.5 Radio Service Configuration

The APC supports WLAN-based radio configuration. You can enable or disable WMM based on WLAN and change DTIM and station idle timeout.

Configuration using CLI

1) Go to configure → wlan-radio-service mode of CLI.

```
APC# configure terminal
APC/configure# wlan-radio-service
APC/configure/wlan-radio-service#
```

2) Configure whether to enable or disable WMM.
   - wmm-mode [WLAN_ID] [MODE]

Parameter	Description
WLAN_ID	WLAN ID (range: 1-240)
MODE	WMM configuration mode (disable/enable)

3) Configure DTIM.
   - dtim [WLAN_ID] [DTIM]

Parameter	Description
WLAN_ID	WLAN ID (range: 1-240)
DTIM	Beacon DTIM: 1~255(default: 1)

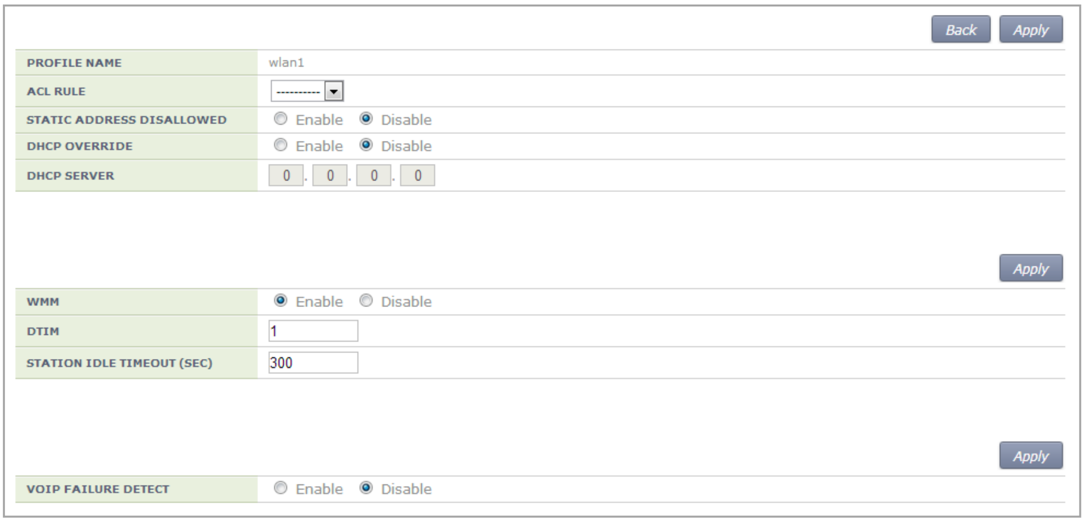
4) Configure station idle timeout.
   - sta-idle-timeout [WLAN_ID] [TIMEOUT]

Parameter	Description
WLAN_ID	WLAN ID (range: 1-240)
TIMEOUT	Station idle timeout (range: 30-3600, unit: 15 s, default: 300)

5) To check the configured information, use the ‘show wlan-radio-service’ command.

Configuration using Web UI

In the menu bar of **<WEC Main window>**, select **<Configuration>** and then select the **<WLANs>** menu in the sub-menus. Select a WLAN ID to change in the WLANs screen and go to the **<Advanced>** tab.



PROFILE NAME	wlan1
ACL RULE	----------
STATIC ADDRESS DISALLOWED	○ Enable ● Disable
DHCP OVERRIDE	○ Enable ● Disable
DHCP SERVER	0 . 0 . 0 . 0
WMM	● Enable ○ Disable
DTIM	1
STATION IDLE TIMEOUT (SEC)	300
VOIP FAILURE DETECT	○ Enable ● Disable

Figure 120. Radio service configuration

After configuring the below items, click the **<Apply>** button.

- WMM: Configures the WMM mode.
- DTIM: Enter a DTIM value (1-255).
- STATION IDLE TIMEOUT: Enter a station idle timeout value. The value range is 30-3600 and it must be the multiple of 15.

CHAPTER 6. Wi-Fi Configuration

This chapter describes how to manage the 802.11a, 80211.bg, 802.11n or 80211ac device of W-EP AP.
An 802.11n device supports 2.4 GHz and 5 GHz wireless bandwidth and high data processing speed.

6.1 802.11a/b/g/n/ac Radio Property

6.1.1 802.11a/b/g Configuration

The configuration of radio property for 802.11a/b/g/ac is as follows:

Configuration using CLI

1) Go to configure → radio mode to configure of CLI. The radio mode can be either ‘80211a’ or ‘80211bg’.
   An example of entering into 80211a is shown below.

```
APC# configure terminal
APC/configure# 80211a
APC/configure/80211a#
```

2) Configure the channel of an AP.
   - channel [CHANNEL] ap [AP_ID]: Configures the channel of an AP.
   - channel [CHANNEL] ap [AP_ID] fixed: A channel is designed to be fixed and it is not affected by the automatic adjustment function such as RRM. (When executing the ‘show 80211a summary’ or ‘show 80211bg summary’, the channel value is displayed in ‘*’.)

Parameter	Description
CHANNEL	Channel Configuration - Range for 80211a: 36-165 - Range for 80211bg: 1-14
AP_ID	AP ID (range: 1-3000)

3) Configure channel of multiple APs belonging to the group.
   - channel [CHANNEL] group [GROUP_ID] all-ap/active-ap: Channel is configured for multiple APs.
   - channel [CHANNEL] group [GROUP_ID] all-ap/active-ap fixed: Channel is fixed and is not affected by automatic adjustment functions such as RRM. (Channel values are indicated as * when retrieved by 'show 80211a summary' or 'show 80211bg summary'.)

Parameter	Description
CHANNEL	Channel Configuration - Range for 80211a: 36-165 - Range for 80211bg: 1-14
GROUP_ID	ID of the AP group
all-ap	Applies to all APs in the group
active-ap	Applies to all live APs in the group

4) Configure the TX power of an AP.
   - txPower [POWER] ap [AP_ID]: Configures a TX power.
   - txPower [POWER] ap [AP_ID]fixed: The TX power is configured as fixed and it is not affected by the automatic adjustment function such as RRM. (When executing the 'show 80211a summary' or 'show 80211bg summary', the channel value is displayed in '*'.)

Parameter	Description
POWER	TX power value (range: 3-23)
AP_ID	AP ID (range: 1-3000)

5) Configure TX power of multiple APs belonging to the group.
   - txPower [POWER] group [GROUP_ID] all-ap/active-ap: TX Power Setting
   - txPower [POWER] group [GROUP_ID] all-ap/active-ap fixed: TX power is fixed and is not affected by automatic adjustment functions such as RRM. (Channel values are indicated as * when retrieved by 'show 80211a summary' or 'show 80211bg summary'.)

Parameter	Description
POWER	TX power value (range: 3-23)
GROUP_ID	ID of the AP group
all-ap	Applies to all APs in the group
active-ap	Applies to all live APs in the group

6) To check the configured channel and TX power information, use the following command.

```
WEC8500# show 80211a[|80211bg] summary
AP Name           MAC Address        Operation State  Channel   TxPower
----------------- ----------------- ---------------- -------- --------
AP_f4d9fb23bfb9   F4:D9:FB:23:BF:B9  1                 161       10 *
AP_f4d9fb23c2b9   F4:D9:FB:23:C2:B9  1                 157        5
AP_f4d9fb23c079   F4:D9:FB:23:C0:79  1                 153        5
AP_f4d9fb23baf9   F4:D9:FB:23:BA:F9  1                 149        5
AP_f4d9fb23beb9   F4:D9:FB:23:BE:B9  1                  64        5
```

In this example, the AP_f4d9fb23bfb9 whose Tx Power is displayed as 10* has a fixed TX power.

7) Configure the beacon period of an AP.
- beacon period [PERIOD] global

Parameter	Description
PERIOD	Beacon period (range: 40-3500)

8) Configure the fragmentation threshold of an AP.
- threshold fragmentation [THRESHOLD] global

Parameter	Description
THRESHOLD	Fragmentation threshold (range: 256-8000)

9) Configure the data rate of an AP.
- rate [MODE] [RATE] global

Parameter	Description
MODE	Mode (basic/supported) - basic: Basic rate at which a terminal connects to an AP. - supported: A connected terminal that supports the supported rate can communicate with an AP at the supported rate.
RATE	Data rate - Range for 80211a: 6, 9, 12, 18, 24, 36, 48, or 54 Mbps - Range for 80211bg: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, or 54 Mbps

10) To check the configured beacon period, fragmentation threshold, and data rate information, uses the ‘show 80211a radio-config global’ command.

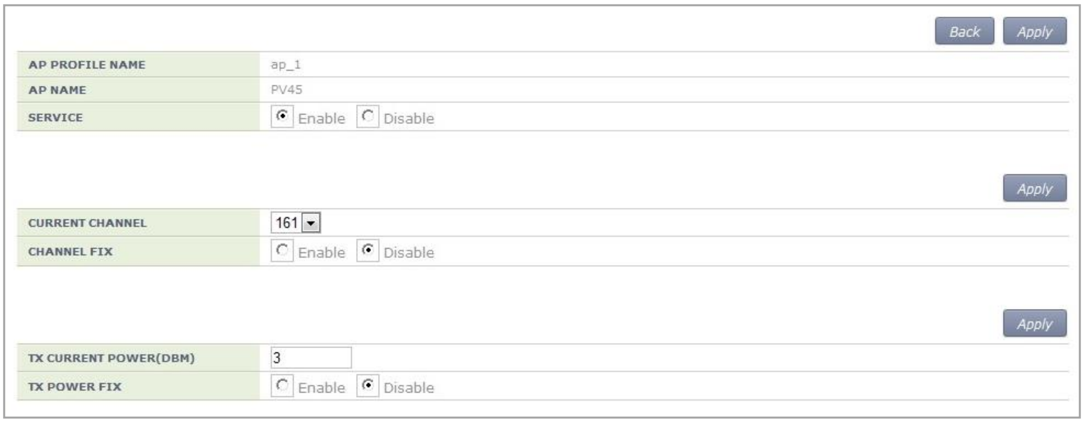
11) Configure the bandwidth of the AP. Bandwidth can be configured only for 80211a/n/ac.

- bandwidth [BANDWIDTH] ap [AP_ID]: Bandwidth is configured for a specific AP.
- bandwidth [BANDWIDTH] global: Bandwidth is configured for all APs.

Parameter	Description
BANDWIDTH	- 20: 20 MHz - 40: 40 MHz - 80: 80 MHz - 160: 160 MHz (to be supported in the future) - 8080: 80 + 80 MHz (to be supported in the future)
AP_ID	ID of the AP (range: 1-3000)

Configuration using Web UI

In the menu bar of **<WEC Main window>**, select **<Configuration>** and then select the **<Access Points>** → **<802.11a/n>** or **<802.11b/g/n>** menu in the sub-menus.
An example of selecting 802.11a/n is shown below.



AP PROFILE NAME	ap_1
AP NAME	PV45
SERVICE	● Enable ○ Disable

CURRENT CHANNEL	161
CHANNEL FIX	○ Enable ● Disable

TX CURRENT POWER(DBM)	3
TX POWER FIX	○ Enable ● Disable

Figure 121. 802.11a/b/g/n radio (1)

The configuration items are as follows:

[AP Service Configuration]

- SERVICE: Enable or disable the radio service.

[Channel Configuration]

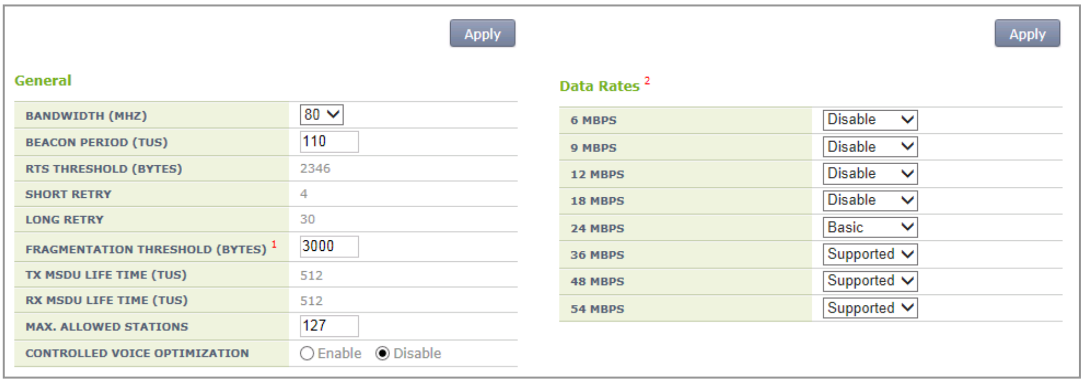
- CURRENT CHANNEL: Configures a channel.
  - Range for 80211a: 36-165
  - Range for 80211bg: 1-14
- CHANNEL FIX: The configured channel is configured as fixed and it is not affected by the automatic adjustment function such as RRM. When selecting the **<Monitor>** → **<Access Points>** → **<Radio>** → **<802.11a/n/ac>** or **<802.11b/g/n>** menu, the channel value is displayed as *. (Optional)

[TX power Configuration]

- TX CURRENT POWER: TX Power (range: 3-23)
- TX POWER FIX: The configured TX power is configured as fixed and it is not affected by the automatic adjustment function such as RRM. When selecting the **<Monitor>** → **<Access Points>** → **<Radio>** → **<802.11a/n/ac>** or **<802.11b/g/n>** menu, the Tx power value is displayed as *. (Optional)

> NOTE
>
> To check the configured channel and TX power information, go to **<Monitor>** → **<Access Points>** → **<Radio>** → **<802.11a/n/ac>** or **<802.11b/g/n>**.

In the menu bar of **<WEC Main window>**, select **<Configuration>** and then select the **<Radio>** → **<802.11a/n/ac>** or **<802.11b/g/n>** → **<802.11h>** menu in the sub-menus. An example of selecting 802.11a/n/ac is shown below.



General

BANDWIDTH (MHZ)	80
BEACON PERIOD (TUS)	110
RTS THRESHOLD (BYTES)	2346
SHORT RETRY	4
LONG RETRY	30
FRAGMENTATION THRESHOLD (BYTES) [1]	3000
TX MSDU LIFE TIME (TUS)	512
RX MSDU LIFE TIME (TUS)	512
MAX. ALLOWED STATIONS	127
CONTROLLED VOICE OPTIMIZATION	○ Enable ● Disable

Data Rates [2]

6 MBPS	Disable
9 MBPS	Disable
12 MBPS	Disable
18 MBPS	Disable
24 MBPS	Basic
36 MBPS	Supported
48 MBPS	Supported
54 MBPS	Supported

Figure 122. 802.11a/b/g/n radio (2)

[General]

- BANDWIDTH: Configures bandwith (range: 20, 40, 80). Available for 802.11a/n/ac only.
- BEACON PERIOD: Beacon period (range: 40-3500)
- FRAGMENTATION THRESHOLD: AP fragmentation threshold (range: 256-8000)
- MAX. CLIENT COUNTS: Limits the number of connected clients per radio
- CONTROLLED VOICE OPTIMIZATION: Configures voice optimization.

[Data Rates]

The data rate selection options are as follows:

- Basic: Basic rate supported for a terminal to connect to an AP.
- Supported: A connected terminal that supports the supported rate can communicate with an AP at the supported rate.
- Data Rates: data rate
  - Range for 80211a: 6, 9, 12, 18, 24, 36, 48, or 54 Mbps
  - Range for 80211bg: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, or 54 Mbps

6.1.2 802.11n Configuration

The 802.11n configuration is as follows:

Configuration using CLI

1) Go to configure → radio mode (80211a or 80211bg) to configure of CLI.

```
WEC8500# configure terminal
WEC8500/configure# 80211a
```

2) Go to the 11n-support mode.

```
WEC8500/configure/80211a#11n-support
```

3) Configure an AP so that it can support 802.11n property.

```
WEC8500/configure/80211a/11n-support# enable [AP_ID]
```

Parameter	Description
AP_ID	AP ID (range: 1-500)

4) Configure the Modulation and Coding Scheme (MCS) rate.

```
WEC8500/configure/80211a/11n-support# mcs [RATE] ap [AP_ID]
```

Parameter	Description
RATE	MSC rate (range: 0-23)
AP_ID	AP ID (range: 1-500)

5) To check the configured 11n-support information, use the ‘show 80211a radio-config ap [AP_ID]’ command.

Configuration using Web UI

In the menu bar of **<WEC Main window>**, select **<Configuration>** and then select the **<Access Points>** → **<802.11a/n/ac>** or **<802.11b/g/n>** → **<General>** menu in the sub-menus.

Perform the configuration by referring to ‘6.1.1 802.11a/b/g Configuration’.

6.1.3 802.11ac Configuration

The 802.11ac configuration is as follows:

Configuration using CLI

1) Go to configure radio mode of 80211a to configure.

```
WEC8500# configure terminal
WEC8500/configure# 80211a
```

2) Enter 11ac-support mode.

```
WEC8500/configure/80211a#11ac-support
```

3) Configure the AP so that it can support the 802.11ac property.

```
WEC8500/configure/80211a/11ac-support# enable [AP_ID]
```

Parameter	Description
AP_ID	ID of the AP (range: 1-500)

4) Configure the Modulation and Coding Scheme (MCS) rate.

```
WEC8500/configure/80211a/11n-support# mcs [RATE] ap [AP_ID]
```

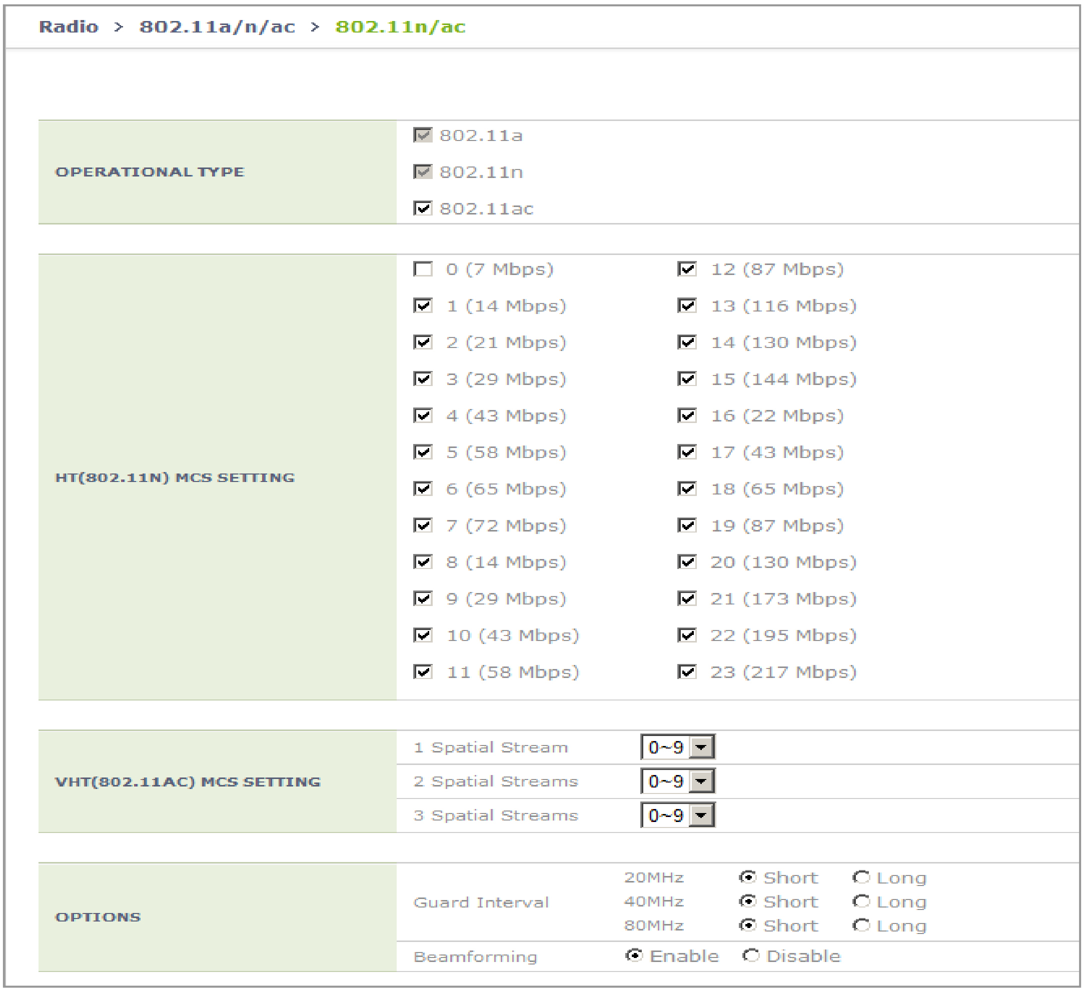
Parameter	Description
RATE	MSC rate (range: 0-23)
AP_ID	ID of the AP (range: 1-500)

5) To check the configured 11ac-support information, use the ‘show 80211a radio-config ap[AP_ID]’ command.

Configuration using Web UI

In the menu bar of <**WEC Main Window**>, select <**Configuration**> and then select <**Access Points**> → <**802.11a/n/ac**> or <**Radio**> → <**802.11a/n/ac**> → <**802.11n/ac**> in the submenu.

An example of selecting 802.11a/n/ac is shown below.



Radio > 802.11a/n/ac > 802.11n/ac

OPERATIONAL TYPE	☑ 802.11a ☑ 802.11n ☑ 802.11ac

HT(802.11N) MCS SETTING	□ 0 (7 Mbps)	☑ 12 (87 Mbps)
	☑ 1 (14 Mbps)	☑ 13 (116 Mbps)
	☑ 2 (21 Mbps)	☑ 14 (130 Mbps)
	☑ 3 (29 Mbps)	☑ 15 (144 Mbps)
	☑ 4 (43 Mbps)	☑ 16 (22 Mbps)
	☑ 5 (58 Mbps)	☑ 17 (43 Mbps)
	☑ 6 (65 Mbps)	☑ 18 (65 Mbps)
	☑ 7 (72 Mbps)	☑ 19 (87 Mbps)
	☑ 8 (14 Mbps)	☑ 20 (130 Mbps)
	☑ 9 (29 Mbps)	☑ 21 (173 Mbps)
	☑ 10 (43 Mbps)	☑ 22 (195 Mbps)
	☑ 11 (58 Mbps)	☑ 23 (217 Mbps)

VHT(802.11AC) MCS SETTING	1 Spatial Stream	0~9
	2 Spatial Streams	0~9
	3 Spatial Streams	0~9

OPTIONS	Guard Interval	20MHz	● Short	○ Long
		40MHz	● Short	○ Long
		80MHz	● Short	○ Long
	Beamforming	● Enable	○ Disable	

[OPERATIONAL TYPE]

Enable/disable 11ac operation.

[VHT (802.11AC) MCS SETTING]

- Determine the spatial stream count for each AP model and enter maximum MCS value for each spatial stream count.
- Example: maximum of seven MCS for one spatial stream, maximum of eight MCS for two spatial streams, and maximum of nine MCS for three spatial streams
  - 1 spatial stream: 7
  - 2 spatial streams: 8
  - 3 spatial streams: 9

[OPTIONS]

- Guard-interval (11n): Select short/long for Guard-interval 20/40 Mhz respectively.
- Guard-interval (11ac): Select short/long for Guard-interval 20/40/80 Mhz respectively.

6.2 Wi-Fi QoS Configuration

The APC provides various QoS in the wire/wireless section for every packet type (voice, video, best-effort, or background). The QoS can be configured for each wireless section (2.4 GHz, 5 GHz).

6.2.1 QoS Configuration of Wireless Terminal

The system provides probable QoS by changing the Enhanced Distributed Channel Access (EDCA) parameter in a wireless section.

Configuration using CLI

To configure an EDCA profile in the upward wireless section of a wireless terminal, execute the command as follows:

1) Go to configure → radio mode to configure of CLI.

```
APC# configure terminal
APC/configure# [80211a/80211bg]
```

2) Apply the EDCA profile.
   - edca-parameters [PROFILE] station

Parameter	Description
PROFILE	Configures each EDCA profile (wmm_default_sta/wmm_default_ap/ edca_user1/edca_user2).

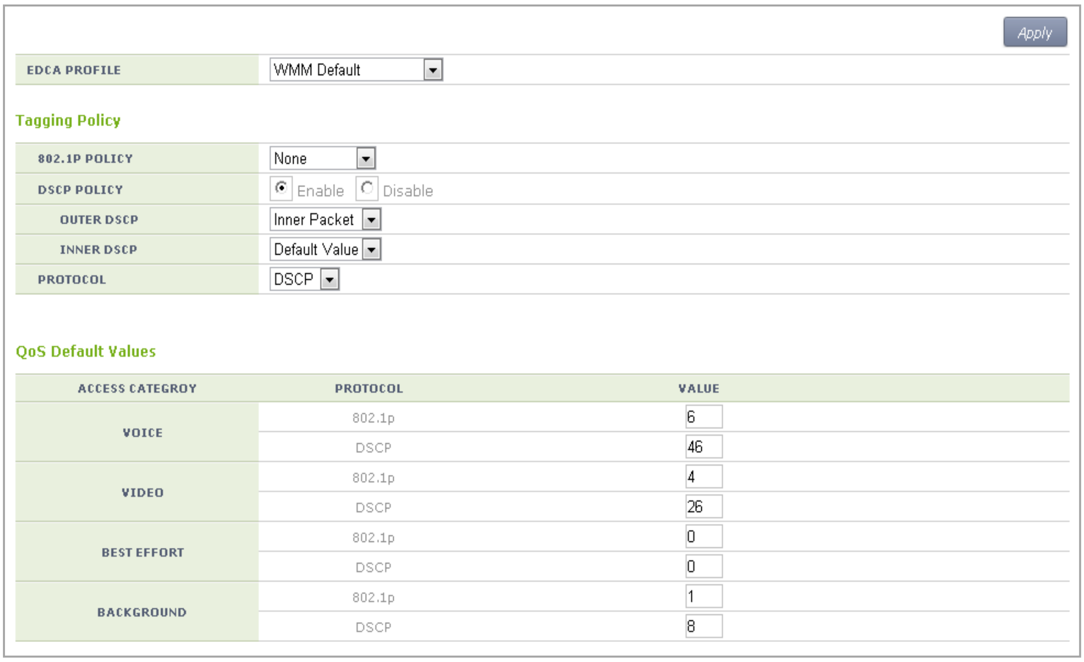
3) To check the application status of a configured EDCA profile, use the 'show 80211a [80211bg] qos edca-parameters wmm_default_sta' command.

Configuration using Web UI

In the menu bar of **<WEC Main window>**, select **<Configuration>** and then select the **<Radio>**→ **<802.11a/n>** or **<802.11b/g/n>** → **<QoS>** menu in the sub-menus.

In the Qos menu, there are Wired and Wireless tab. To change the Station EDCA parameter, select the Wired tab. If you want to change the AP EDCA parameter to configure the QoS of an AP wireless section, select the Wireless tab.

[Wired tab]



EDCA PROFILE	WMM Default

Tagging Policy

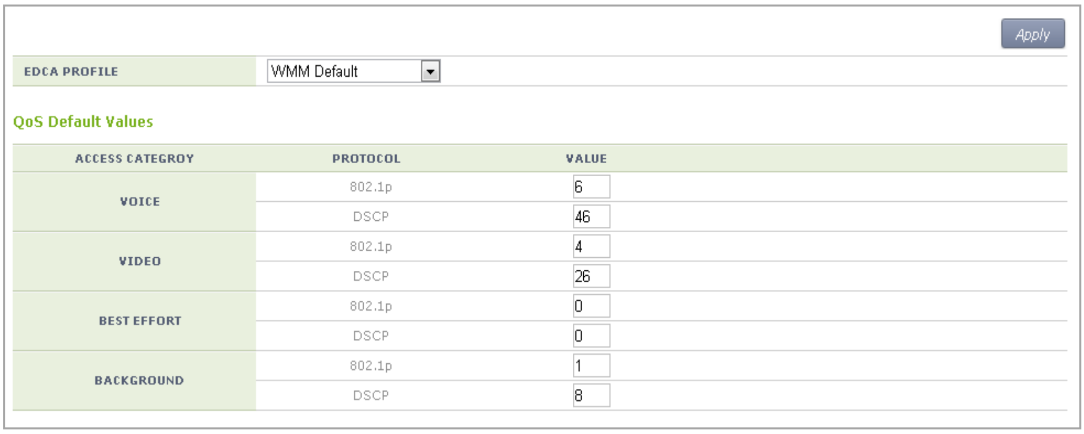
802.1P POLICY	None
DSCP POLICY	● Enable ○ Disable
OUTER DSCP	Inner Packet
INNER DSCP	Default Value
PROTOCOL	DSCP

QoS Default Values

ACCESS CATEGROY	PROTOCOL	VALUE
VOICE	802.1p	6
	DSCP	46
VIDEO	802.1p	4
	DSCP	26
BEST EFFORT	802.1p	0
	DSCP	0
BACKGROUND	802.1p	1
	DSCP	8

Figure 123. QoS configuration of a wireless terminal (1)

[Wireless tab]



EDCA PROFILE	WMM Default

QoS Default Values

ACCESS CATEGROY	PROTOCOL	VALUE
VOICE	802.1p	6
	DSCP	46
VIDEO	802.1p	4
	DSCP	26
BEST EFFORT	802.1p	0
	DSCP	0
BACKGROUND	802.1p	1
	DSCP	8

Figure 124. QoS configuration of a wireless terminal (2)

6.2.2 QoS Configuration of AP

6.2.2.1 Wire Section

The APC provides QoS in a wire section using 802.1p and Differentiated Services Code Point (DSCP) marking and it can adjust packet traffics because it can adjust queue length depending on packet type.

Configuration using CLI

To configure the Station QoS parameter that will be applied to the wire section between APC and AP, execute the command as follows:

1) Go to configure → QoS mode of a wireless section of CLI.

```
APC# configure terminal
APC/configure# [80211a/80211bg] qos
APC/configure/80211a/qos#
```

2) Configure a QoS policy to a wire section packet.
- 802.1P Policy: enable policy [802_1P]
- DSCP Policy: enable policy [DSCP_OUTER] [DSCP_INNER]

Parameter	Description
enable	Enables 802.1p or DSCP marking.
802_1P	802.1p configuration (user_priority/default) - user_priority: Marks the 802.1p or User Priority value of an incoming packet into the 802.1p field. - default: Marks pre-configured basic value to the 802.1p field.
DSCP_OUTER	DSCP Outer configuration (inner_packet/default) - inner_packet: Marks the DSCP value of an incoming packet into the Outer DSCP field. - default: Marks pre-configured basic value to the Outer DSCP field.
DSCP_INNER	DSCP Inner configuration (no_mark/default) - no_mark: Marks no value into the Inner DSCP field. - default: Marks pre-configured basic value to the Inner DSCP field.

3) Configure a default 802.1p value per packet.
- dot1p-tag [PACKET_TYPE] [802.1P_TAG]

Parameter	Description
PACKET_TYPE	Packet type configuration (voice/video/best_effort/background)
802.1P_TAG	Default 802.1p value

4) Configure a default DSCP value per packet.
   - dscp-tag [PACKET_TYPE] [DSCP TAG]

Parameter	Description
PACKET_TYPE	Packet type configuration (voice/video/best_effort/background)
DSCP_TAG	Default DSCP value

5) Configure a protocol to distinguish packet types.
   - protocol [PROTOCOL]

Parameter	Description
PROTOCOL	Protocol configuration (none/dot1p/dscp) - none: Determine the type of every incoming packet with best effort. - dot1p: Judge the packet type by checking the 802.1p field of an incoming packet. - dscp: Judge the packet type by checking the DSCP field of an incoming packet.

The packet judgment criteria are as follows: For example, if the packet type is voice, the 802.1p input value is 6 or 7 and the input range of DSCP value is 46-63.
Also, if the packet type is video, the 802.1p input value is 4 or 5 and the input range of DSCP value is 24-45.

802.1p	DSCP	Packet type
6, 7	46~63	voice
4, 5	24~45	video
0, 3	0~7, 16~23	best effort
1, 2	8~15	background

6) To check the configured policy and QoS parameter information per packet, use the ‘show 80211a[|80211bg] qos policy’ command.

Configuration using Web UI

In the menu bar of **<WEC Main window>**, select **<Configuration>** and then select the **<Radio>** → **<802.11a/n>** or **<802.11b/g/n>** → **<QoS>** menu in the sub-menus.

1) Select one out of None/Default/User Priority in the 802.1P POLICY drop-down list of Tagging Policy.
2) To disable a DSCP policy in the DSCP POLICY, select Disable.
3) To enable a DSCP policy in the DSCP POLICY, select Enable.
   a) Select one out of Inner Packet/Default Value in the OUTER DSCP drop-down list.
   b) Select one out of No Mark/Default Value in the INNER DSCP drop-down list.
4) Select one out of None/802.1p/DSCP in the PROTOCOL drop-down list.
5) Enter 802.1p or a DSCP value into the QoS Default Values.
6) Click the **<Apply>** button to apply.

6.2.2.2 Wireless Section

The system can provide QoS service in a wireless section for each AP downward packet type (voice, video, best effort, background). You can configure 802.1p and DSCP tag which are the criteria used to select access category.

Configuration using CLI

1) Go to configure → QoS mode of a wireless section of CLI.

```
APC# configure terminal
APC/configure# [80211a/80211bg] qos
APC/configure/80211a/qos#
```

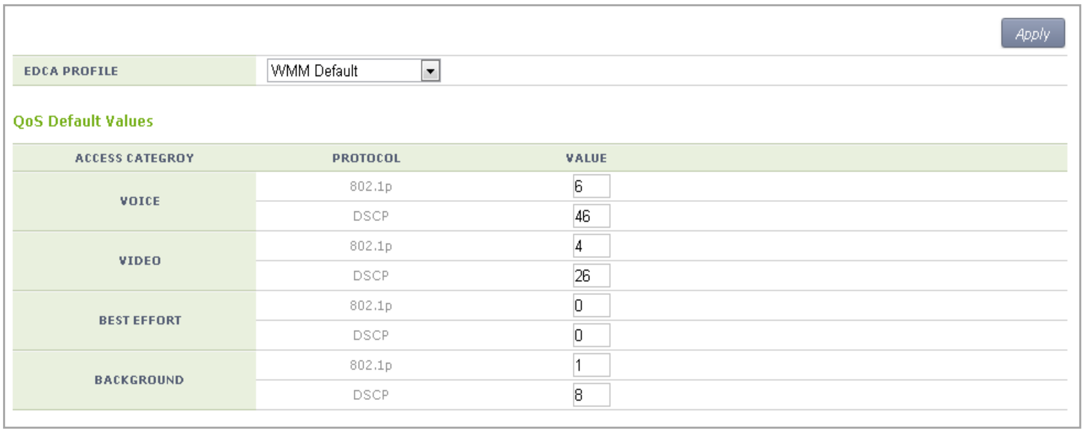
2) Configure 802.1p or DSCP tag value to use for a packet type.
   - ap-tags [PACKET_TYPE] [802.1P TAG] [DSCP TAG]

Parameter	Description
PACKET_TYPE	Packet type configuration (voice/video/best_effort/background)
802.1P_TAG	802.1p configuration
DSCP_TAG	DSCP tag configuration

3) To check the QoS parameter information of a configured AP, use the 'show 80211a [80211bg] qos ac-profile [PACKET_TYPE]' command.

Configuration using Web UI

In the menu bar of **<WEC Main window>**, select **<Configuration>** and then select the **<Radio>** → **<802.11a/n>** or **<802.11b/g/n>** → **<QoS>** menu in the sub-menus.



EDCA PROFILE: WMM Default

QoS Default Values

ACCESS CATEGROY	PROTOCOL	VALUE
VOICE	802.1p	6
	DSCP	46
VIDEO	802.1p	4
	DSCP	26
BEST EFFORT	802.1p	0
	DSCP	0
BACKGROUND	802.1p	1
	DSCP	8

Figure 125. QoS configuration of AP (wireless section)

In the Access Point tab, enter 802.1p or a DSCP value into the QoS Default Values. Click the **<Apply>** button to apply.

6.2.3 Configuring QoS Profile of a Specific Terminal

You can configure a QoS profile that is applied to a specific wireless terminal.
This QoS profile is applied from the RADIUS server of a wireless terminal during authentication.

Configuration using CLI

1) Go to configure → QoS profile configuration mode of CLI.

```
APC# configure terminal
APC/configure# qos <profile name>
APC/configure/qos Samsung #
```

2) Configure 802.1p and a DSCP value that will be used for each access category.
   - ac [AC] [802.1P_TAG] [DSCP_TAG]

Parameter	Description
AC	Access Category(AC_VO/AC_VI/AC_BE/AC_BK)
802.1P_TAG	802.1p configuration (range: 0-7)
DSCP_TAG	DSCP tag configuration (range: 0-63)

3) Configure the brief information of a profile.
   - description [DESCRIPTION]

Parameter	Description
DESCRIPTION	Profile description

4) Configure maximum allowed 802.1p priority value used in the Traffic Identifier (TID) field of AP QoS packet.
   - max-dot1p <802.1p tag>

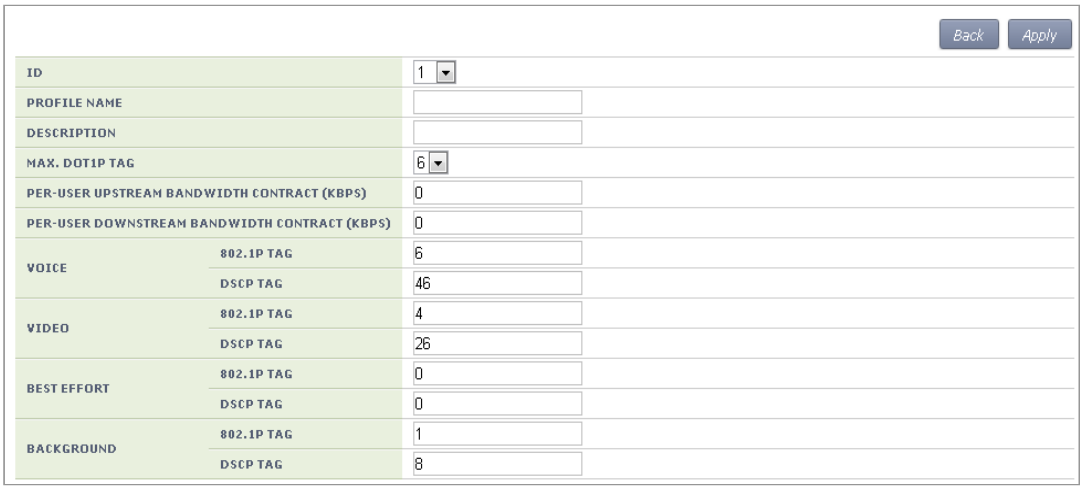
Parameter	Description
802.1P_TAG	Maximum allowed 802.1p configuration (range: 0-7)

5) To check the configured QoS profile information, use the ‘show qos profile’ command.

Configuration using Web UI

In the menu bar of **<WEC Main window>,** select **<Configuration>** and then select the **<User QoS>** menu in the sub-menus. To create a QoS profile to apply to a terminal, click the **<Add>** button in the initial window.

The QoS addition window consists of the following QoS parameters. By entering each QoS parameter, you can configure the QoS profile of a specific terminal or configure the usage control function for each user.



ID		1 ▾
PROFILE NAME		
DESCRIPTION		
MAX. DOT1P TAG		6 ▾
PER-USER UPSTREAM BANDWIDTH CONTRACT (KBPS)		0
PER-USER DOWNSTREAM BANDWIDTH CONTRACT (KBPS)		0
VOICE	802.1P TAG	6
	DSCP TAG	46
VIDEO	802.1P TAG	4
	DSCP TAG	26
BEST EFFORT	802.1P TAG	0
	DSCP TAG	0
BACKGROUND	802.1P TAG	1
	DSCP TAG	8

Figure 126. Configuring QoS profile of a specific terminal

- ID: ID (range: 1-16)
- PROFILE NAME: Profile name
- DESCRIPTION: Profile description
- MAX. DOT1P TAG: Maximum allowed 802.1p tag (range: 0-7)
- PER-USER UPSTREAM BANDWIDTH CONTRACT: Maximum upward usage (range: 0-450000)
- PER-USER DOWNSTREAM BANDWIDTH CONTRACT: Maximum downward usage (range: 0-450000)
- VOICE/VIDEO/BEST EFFORT/BACKGROUND: Enter 802.1P TAG (range: 0-7) and DSCP TAG (range: 0-64) for each item.

6.2.4 Voice Optimization Configuration

The APC configures an EDCA parameter value that is optimized for voice service to an AP in real-time.

Configuration using CLI

1) Go to configure → radio cvo mode to configure of CLI.

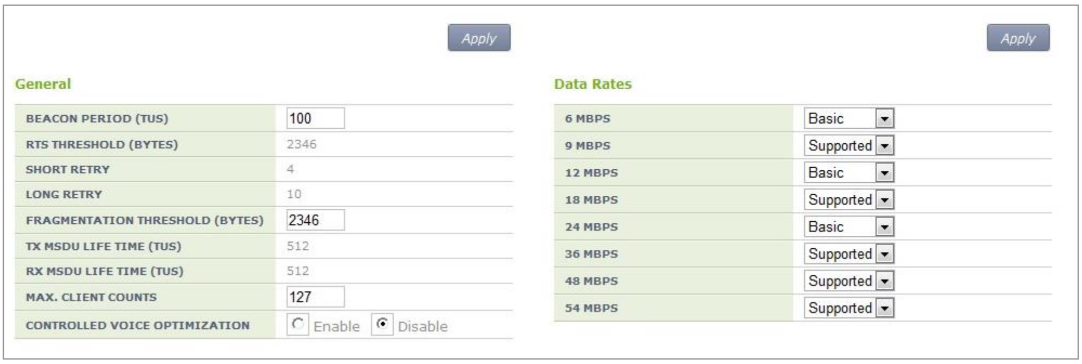
```
APC# configure terminal
APC/configure# [80211a|80211bg] cvo
APC/configure/80211a/cvo#
```

2) Enable or disable the function.
   - [no] enable

3) To check the configured information, use the 'show 80211a cvo config' command.

Configuration using Web UI

In the menu bar of **<WEC Main window>**, select **<Configuration>** and then select the **<Radio>** → **<802.11a/n>** or **<802.11b/g/n>** → **<General>** menu in the sub-menus.



General

BEACON PERIOD (TUS)	100
RTS THRESHOLD (BYTES)	2346
SHORT RETRY	4
LONG RETRY	10
FRAGMENTATION THRESHOLD (BYTES)	2346
TX MSDU LIFE TIME (TUS)	512
RX MSDU LIFE TIME (TUS)	512
MAX. CLIENT COUNTS	127
CONTROLLED VOICE OPTIMIZATION	○ Enable ● Disable

Data Rates

6 MBPS	Basic
9 MBPS	Supported
12 MBPS	Basic
18 MBPS	Supported
24 MBPS	Basic
36 MBPS	Supported
48 MBPS	Supported
54 MBPS	Supported

Figure 127. Configuring voice optimization

To enable Controlled Voice Optimization (CVO), select Enable in the CONTROLLED VOICE OPTIMIZATION. To disable it, select Disable.

6.3 802.11h Configuration

The APC supports the configuration and transmission power limitation for the Dynamic Frequency Selection (DFS) function in an AP. When the AP detects radar, an event is sent to the WEM and a detouring channel can be configured in the AP.

Configuration using CLI

For channel switching announcement related configuration and power constraint value configuration in an AP, execute the command as follows:

1) Go to configure → 80211h configuration mode of CLI.

```
APC# configure terminal
APC/configure# 80211h
APC/configure/80211h#
```

2) Configure the 802.11h information.
   - channel-switch [MODE] [RESTRICTION] [SWITCH COUNT]

Parameter	Description
MODE	Whether the switching announcement function is enabled/disabled
RESTRICTION	Whether the channel packet transmission restriction mode is enabled (disable/enable)
SWITCH COUNT	Waiting time until channel switching announcement

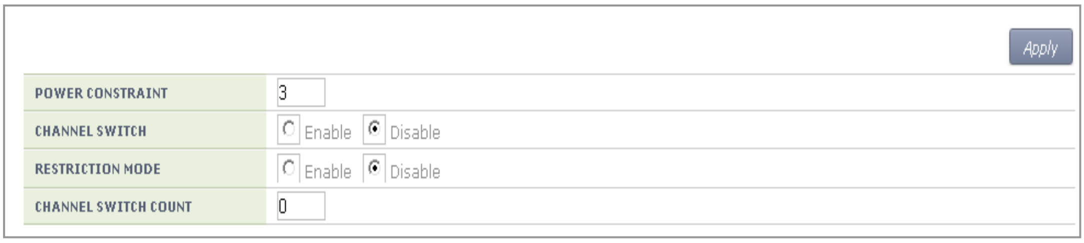
3) Configure the transmission power of a wireless terminal.
   - power-constraint [VALUE]

Parameter	Description
VALUE	Transmission power(0-31 dB)

4) To check the configuration information, use the ‘show 80211h configuration’ command.

Configuration using Web UI

In the menu bar of **<WEC Main window>**, select **<Configuration>** and then select the **<Radio>** → **<802.11a/n>** → **<802.11h>** menu in the sub-menus.



POWER CONSTRAINT	3
CHANNEL SWITCH	○ Enable ● Disable
RESTRICTION MODE	○ Enable ● Disable
CHANNEL SWITCH COUNT	0

Figure 128. Configuring 802.11h

- POWER CONSTRAINT: Power constraint value (0-100)
- CHANNEL SWITCH: Enables channel switch announcement.
- RESTRICTION MODE: Configures transmission restriction.
- CHANNEL SWTICH COUNT: Enter a waiting time until channel switching announcement. Target Beacon Transmission Times (TBTT)

6.4 Country Code

You can use a country code to restrict the number of channels that can be used in an AP and the maximum transmission power of each channel.

Configuration using CLI

To configure the country code function, go to country mode first by executing the following command.

```
APC# configure terminal
APC/configure# country
APC/configure/country#
```

[Global Country Code Configuration]

If you configure a global country code, the country code can be specified to all the connected APs at the same time. The command is shown below.

- set-global [COUNTRY_CODE] [VALUE]

Parameter	Description
COUNTRY_CODE	Country code to configure
VALUE	Environment configuration (both/outdoor/indoor/none)

To check the configuration information, use the ‘show country global-config’ command.

[AP Country Code Configuration]

To configure a country code, execute the command as follows:

- set-ap [AP_ID] [COUNTRY_CODE] [VALUE]

Parameter	Description
AP_ID	AP ID (range: 1-500)
COUNTRY_CODE	Country code to configure
VALUE	Environment configuration (both/outdoor/indoor/none)

To check the configuration information, use the ‘show country ap-config [AP_ID]’ command.

[Editing Country Code]

You can add or delete an operation channel per country and change maximum transmission power per channel.

The command used to add or delete a channel per country is shown below.

- add-channel [COUNTRY_CODE] [CHANNEL_NUMBER] [MAX_TX_POWER]: Adds a channel.
- del-channel [COUNTRY_CODE] [CHANNEL_NUMBER]: Deletes a channel.

Parameter	Description
COUNTRY_CODE	Country code to configure
CHANNEL_NUMBER	Channel to configure.
MAX _TX_POWER	Maximum transmission power per channel.

The command used to change maximum transmission power value of a channel for a specific country code is shown below.

- max-tx-power [COUNTRY_CODE] [CHANNEL_NUMBER] [MAX_TX_POWER]

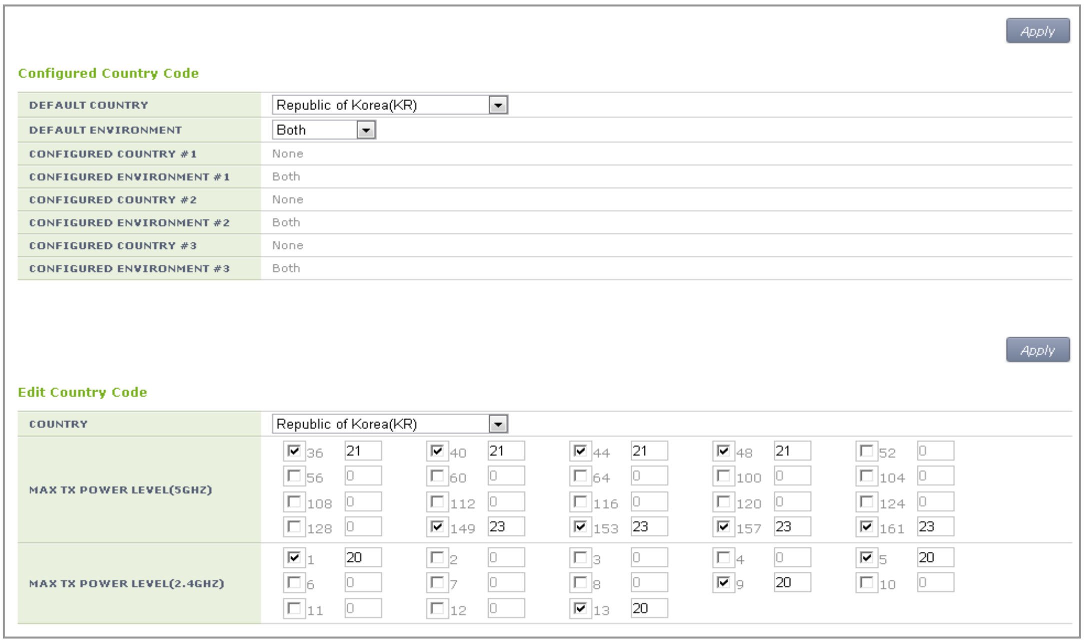
Parameter	Description
COUNTRY_CODE	Country code to configure
CHANNEL_NUMBER	Channel to configure.
MAX _TX_POWER	Maximum transmission power per channel.

To check the configuration information, use the ‘show country information [COUNTRY_ CODE]’ command.

Parameter	Description
COUNTRY_CODE	Country code to configure

Configuration using Web UI

In the menu bar of <**WEC Main window**>, select <**Configuration**> and then select the <**Controller**> → <**Country**> menu in the sub-menus.



Configured Country Code

DEFAULT COUNTRY	Republic of Korea(KR)
DEFAULT ENVIRONMENT	Both
CONFIGURED COUNTRY #1	None
CONFIGURED ENVIRONMENT #1	Both
CONFIGURED COUNTRY #2	None
CONFIGURED ENVIRONMENT #2	Both
CONFIGURED COUNTRY #3	None
CONFIGURED ENVIRONMENT #3	Both

Edit Country Code

COUNTRY	Republic of Korea(KR)									
MAX TX POWER LEVEL(5GHZ)	☑ 36	21	☑ 40	21	☑ 44	21	☑ 48	21	□ 52	0
	□ 56	0	□ 60	0	□ 64	0	□ 100	0	□ 104	0
	□ 108	0	□ 112	0	□ 116	0	□ 120	0	□ 124	0
	□ 128	0	☑ 149	23	☑ 153	23	☑ 157	23	☑ 161	23
MAX TX POWER LEVEL(2.4GHZ)	☑ 1	20	□ 2	0	□ 3	0	□ 4	0	☑ 5	20
	□ 6	0	□ 7	0	□ 8	0	☑ 9	20	□ 10	0
	□ 11	0	□ 12	0	☑ 13	20				

Figure 129. Country code window (1)

[Global Country Code Configuration]

1) Select a country in the DEFAULT COUNTRY drop-down list of Configured Country Code item. (Only an authenticated country code is supported.)
2) Select an environment in the DEFAULT ENVIRONMENT drop-down list.
   - Both: The terminal operation environment includes all the environments.
   - Outdoor: The terminal operation environment is outdoor.
   - Indoor: The terminal operation environment is indoor.
   - Non-country: A terminal is operating under non-country entity.
3) Click the <**Apply**> button to apply.

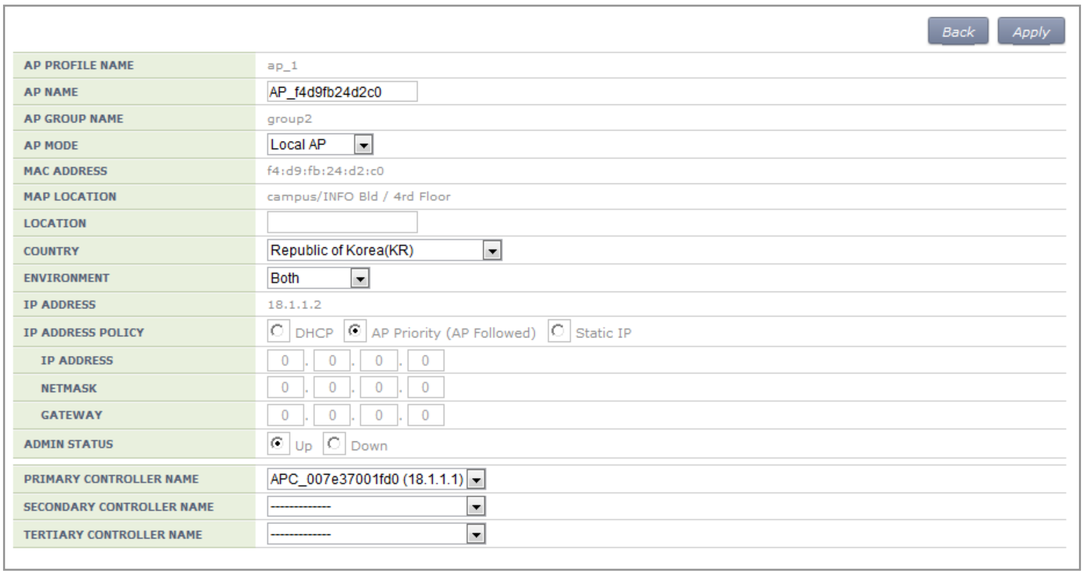
[Editing Country Code]

In the Edit Country Code item, you can add or delete an operation channel per country or change maximum transmission power per channel.

1) Select a country in the COUNTRY drop-down list of Edit Country Code item. (Only an authenticated country code is supported.)
2) Select a channel to add in the MAX TX POWER LEVEL (5 GHZ/2.4 GHZ) and enter maximum transmission power level (0-30).
3) In the MAX TX POWER LEVEL (5 GHZ/2.4 GHZ), unselect a channel to delete.
4) Click the <**Apply**> button to apply.

[AP Country Code Configuration]

In the menu bar of **<WEC Main window>**, select **<Configuration>** and then select the **<Access Points>** → **<General>** menu in the sub-menus.



AP PROFILE NAME	ap_1
AP NAME	AP_f4d9fb24d2c0
AP GROUP NAME	group2
AP MODE	Local AP
MAC ADDRESS	f4:d9:fb:24:d2:c0
MAP LOCATION	campus/INFO Bld / 4rd Floor
LOCATION	
COUNTRY	Republic of Korea(KR)
ENVIRONMENT	Both
IP ADDRESS	18.1.1.2
IP ADDRESS POLICY	○ DHCP ● AP Priority (AP Followed) ○ Static IP
IP ADDRESS	0 . 0 . 0 . 0
NETMASK	0 . 0 . 0 . 0
GATEWAY	0 . 0 . 0 . 0
ADMIN STATUS	● Up ○ Down
PRIMARY CONTROLLER NAME	APC_007e37001fd0 (18.1.1.1)
SECONDARY CONTROLLER NAME	-------------
TERTIARY CONTROLLER NAME	-------------

Figure 130. Country code window (2)

After selecting COUNTRY and ENVIRONMENT, click the **<Apply>** button.

CHAPTER 7. WLAN Additional Services

In this chapter, how to configure WLAN additional services such as wireless terminal management, spectrum analysis, Call Admission Control (CAC) and Radio Resource Management (RRM), etc. is described.

7.1 Managing Wireless Terminal

7.1.1 Information Retrieval Functions

Configuration using CLI

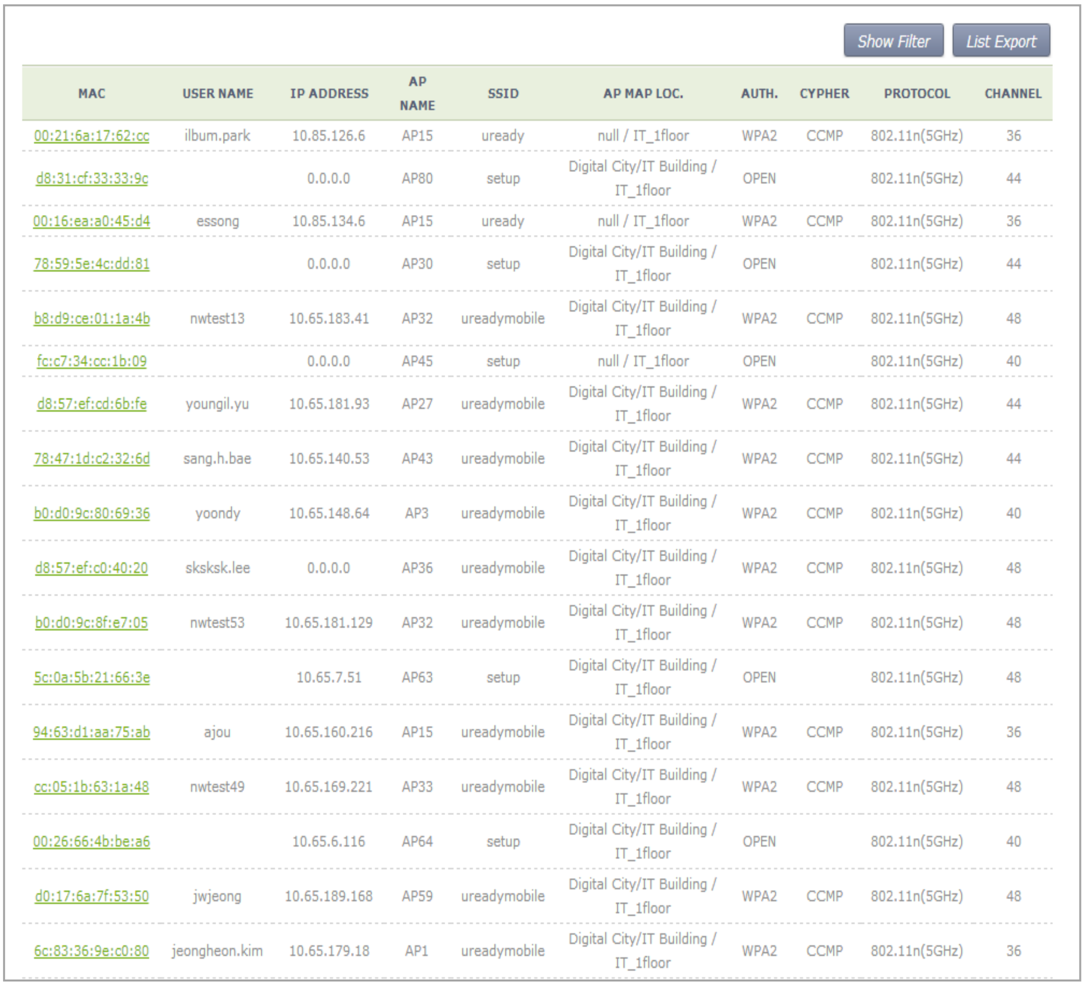
Using the following command, you can retrieve the information of a wireless terminal being serviced by the APC.

- show station summary: When you enter this command, the summary information of all the wireless terminals connected to the APC is retrieved.
- show station summary ap [AP_ID]: The information of wireless terminals of each AP is retrieved.
- show station summary bssid [BSSID_ID]: The information of wireless terminals of each BSSID is retrieved.
- show station summary wlan [WLAN_ID]: The information of wireless terminals of each WLAN is retrieved.
- show station detail [MAC_ADDRESS]: The detail information of a wireless terminal that has a specific MAC address is retrieved.
- show station stats ap-80211-stats [MAC_ADDRESS]: The WI-FI statistics information of a wireless terminal is retrieved.
- show station association history [MAC_ADDRESS]: The connection history of a wireless terminal is retrieved.
- show station stats debug all: The debug statistics information of a wireless terminal is retrieved.
- show station stats management_frame all: The debug statistics information of a wireless terminal is retrieved.

Configuration using Web UI

In the menu bar of **<WEC Main window>**, select **<Monitor>** and then select the **<Stations>** menu in the sub-menus. The brief information of each station is displayed in the window.

To check the detail information of a specific station, click the MAC information of the specific station in the Stations window list.



MAC	USER NAME	IP ADDRESS	AP NAME	SSID	AP MAP LOC.	AUTH.	CYPHER	PROTOCOL	CHANNEL
00:21:6a:17:62:cc	ilbum.park	10.85.126.6	AP15	uready	null / IT_1floor	WPA2	CCMP	802.11n(5GHz)	36
d8:31:cf:33:33:9c		0.0.0.0	AP80	setup	Digital City/IT Building / IT_1floor	OPEN		802.11n(5GHz)	44
00:16:ea:a0:45:d4	essong	10.85.134.6	AP15	uready	null / IT_1floor	WPA2	CCMP	802.11n(5GHz)	36
78:59:5e:4c:dd:81		0.0.0.0	AP30	setup	Digital City/IT Building / IT_1floor	OPEN		802.11n(5GHz)	44
b8:d9:ce:01:1a:4b	nwtest13	10.65.183.41	AP32	ureadymobile	Digital City/IT Building / IT_1floor	WPA2	CCMP	802.11n(5GHz)	48
fc:c7:34:cc:1b:09		0.0.0.0	AP45	setup	null / IT_1floor	OPEN		802.11n(5GHz)	40
d8:57:ef:cd:6b:fe	youngil.yu	10.65.181.93	AP27	ureadymobile	Digital City/IT Building / IT_1floor	WPA2	CCMP	802.11n(5GHz)	44
78:47:1d:c2:32:6d	sang.h.bae	10.65.140.53	AP43	ureadymobile	Digital City/IT Building / IT_1floor	WPA2	CCMP	802.11n(5GHz)	44
b0:d0:9c:80:69:36	yoondy	10.65.148.64	AP3	ureadymobile	Digital City/IT Building / IT_1floor	WPA2	CCMP	802.11n(5GHz)	40
d8:57:ef:c0:40:20	sksksk.lee	0.0.0.0	AP36	ureadymobile	Digital City/IT Building / IT_1floor	WPA2	CCMP	802.11n(5GHz)	48
b0:d0:9c:8f:e7:05	nwtest53	10.65.181.129	AP32	ureadymobile	Digital City/IT Building / IT_1floor	WPA2	CCMP	802.11n(5GHz)	48
5c:0a:5b:21:66:3e		10.65.7.51	AP63	setup	Digital City/IT Building / IT_1floor	OPEN		802.11n(5GHz)	48
94:63:d1:aa:75:ab	ajou	10.65.160.216	AP15	ureadymobile	Digital City/IT Building / IT_1floor	WPA2	CCMP	802.11n(5GHz)	36
cc:05:1b:63:1a:48	nwtest49	10.65.169.221	AP33	ureadymobile	Digital City/IT Building / IT_1floor	WPA2	CCMP	802.11n(5GHz)	48
00:26:66:4b:be:a6		10.65.6.116	AP64	setup	Digital City/IT Building / IT_1floor	OPEN		802.11n(5GHz)	40
d0:17:6a:7f:53:50	jwjeong	10.65.189.168	AP59	ureadymobile	Digital City/IT Building / IT_1floor	WPA2	CCMP	802.11n(5GHz)	48
6c:83:36:9e:c0:80	jeongheon.kim	10.65.179.18	AP1	ureadymobile	Digital City/IT Building / IT_1floor	WPA2	CCMP	802.11n(5GHz)	36

Figure 131. Information viewing window

7.1.2 Connection History related Configuration

You can configure maximum value for the connection history of a wireless terminal that will be managed in the APC.

- station number-of-assoc-tracking [COUNT]

Parameter	Description
COUNT	Maximum number of association tracking

7.2 Handover Management

The handover releases a connection with an existing AP and connects to a new AP.
It provides seamless wireless LAN connection to a wireless terminal. The APC provides both 802.11 standard handover and Samsung’s unique AirMove (Network Controlled Handover) handover.

7.2.1 Connection History Information

Use the ‘show station association history [MAC_ADDRESS]’ command to check the handover history information of a specific wireless terminal connected to the APC.

7.2.2 AirMove Configuration

Unlike the 802.11 standard handover where a wireless terminal performs the handover function by itself, the AirMove handover is performed by the collaboration between wireless terminals compatible with the APC. Therefore, the packet loss or handover time is optimized. Some Samsung smartphones such as Galaxy S2 or S3, etc. provide the AirMove function.

Configuration using CLI

To configure the AirMove related function, execute the following command to go to the handover configuration mode.

```
WEC8500# configure terminal
WEC8500/configure# handover
```

[Handover Option Configuration]

- handover [OPTION] [OPTION_DETAIL]

AirMove Configuration Item	Description
operation mode	Operation mode configuration - OPTION: opmode - OPTION_DETAIL: Each mode (VoIP/STA)
buffered-forwarding mode	Configures whether to use the buffered forwarding function. - OPTION: fwd-buffering - OPTION_DETAIL: Enable/Disable
decision delta	Configures the threshold of RSSI difference between a serving AP and a target AP. - OPTION: decision-delta - OPTION_DETAIL: Threshold (dBm)
scan time on channel	Configures scanning time of a wireless terminal per channel. - option: scan-time-channel - OPTION_DETAIL: Time (ms)

AirMove Configuration Item	Description
scan interleaving time	Configures the scanning interval of a wireless terminal. - OPTION: scan-time-interleave - OPTION_DETAIL: Time (ms)
Service time in scanning period	Configures a period when an wireless terminal transmits/receives an actual data traffic after scanning. - OPTION: scan-time-service - OPTION_DETAIL: Time (ms)
scan report level	Configures the threshold of a scan report that will be transmitted from an AP to the APC. - OPTION: scan-report-level - OPTION_DETAIL: scan report level (dBm)
Numbers of handover scan attempts per channel	Configures the scanning times of a wireless terminal per channel. - OPTION: number-of-proreq - OPTION_DETAIL: Number of times
Number of channels for which scan is attempted	Configures the number of channels a wireless terminal will scan at a time. - OPTION: number-of-channel - OPTION_DETAIL: Number of channels
scan trigger level	RSSI intensity at which a wireless terminal starts channel scanning - OPTION -trigger-level - OPTION_DETAIL: RSSI (dBm)
station decision delta	Configures the threshold of RSSI difference, measured in a wireless terminal, between a serving AP and a target AP. If the threshold is exceeded, a wireless terminal performs its handover. - OPTION: station-decision-delta - OPTION_DETAIL: Threshold (dBm)

An example of using the command for each configuration item is as follows:

```
WEC8500/configure# handover opmode APP
WEC8500/configure# handover buffered-forwarding enable
WEC8500/configure# handover decision-delta 10
WEC8500/configure# handover scan-time-channel 10
WEC8500/configure# handover scan-time-interleave 1000
WEC8500/configure# handover scan-time-service 200
WEC8500/configure# handover scan-report-level -90
WEC8500/configure# handover number-of-proreq 3
WEC8500/configure# handover number-of-channel 4
WEC8500/configure# handover scan-trigger-level -65
WEC8500/configure# handover station-decision-delta 10
```

To check the configuration information, use the ‘show handover configuration’ command.

[AirMove Enable/Disable Configuration]

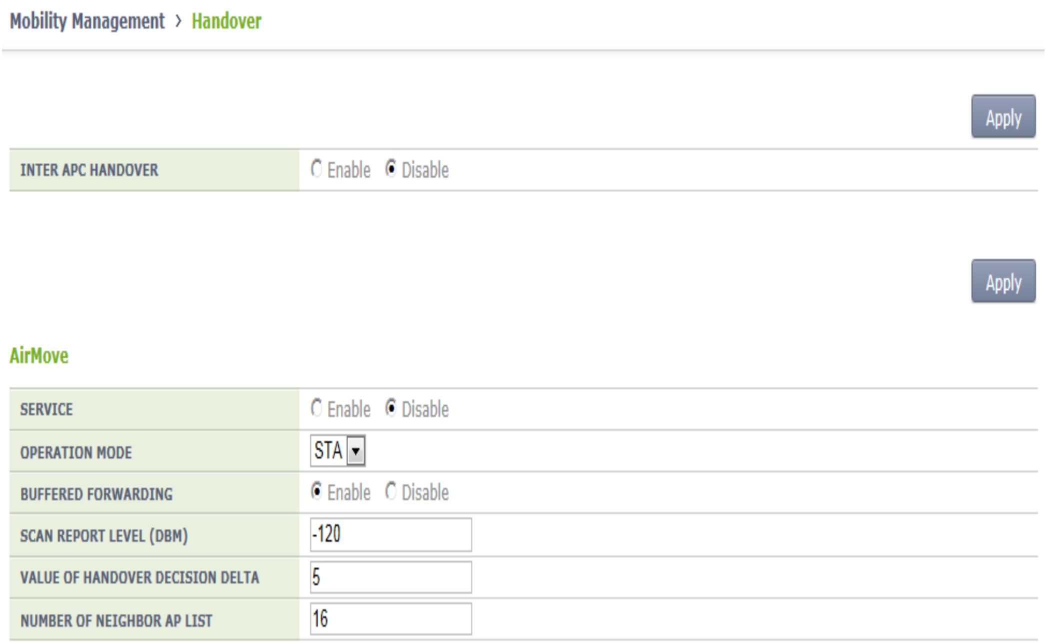
The AirMove is enabled by default, so use the following command to disable it.

- no handover mode NCHO

To check the configuration information, use the 'show handover configuration' command.

Configuration using Web UI

In the menu bar of <**WEC Main window**>, select <**Configuration**> and then select the <**Mobility Management**> → <**Handover**> menu in the sub-menus.



INTER APC HANDOVER	○ Enable ● Disable

AirMove

SERVICE	○ Enable ● Disable
OPERATION MODE	STA
BUFFERED FORWARDING	● Enable ○ Disable
SCAN REPORT LEVEL (DBM)	-120
VALUE OF HANDOVER DECISION DELTA	5
NUMBER OF NEIGHBOR AP LIST	16

Figure 132. Handover window

You can enable or disable the intra handover function by selecting Enable/Disable in the INTER APC HAND-OVER item. After configuring a value, click the <**Apply**> button to apply.

7.2.3 Inter APC Handover Configuration

The Inter APC handover is a technology that supports handover among several APC systems. Depending on network configuration, the Inter APC L3 handover and Inter APC L2 handover services are provided.
By using the clustering service, you can configure several APC systems into a single group.

Configures whether to use the Inter APC handover.

The default value of Inter APC handover is not configured.

- handover inter-apc enable

To check the configuration information, use the 'show handover configuration' command.

7.3 Call Admission Control (CAC) Configuration

The CAC function is provided to protect existing calls from the calls incoming to a wireless LAN. The APC does not allow an additional call when maximum allowed number of calls per radio is reached.

7.3.1 SIP ALG Configuration

To make Call Admission Control (CAC) working, the Session Initiation Protocol (SIP) Application Layer Gateway (ALG) function must be enabled. The SIP ALG analyzes a SIP packet and forwards VoIP communication status to the CAC.

Configuration using CLI

The SIP ALG related commands are as follows:

- sipalg enable: Configures whether to enable the SIP ALG function.
- sipalg sip-error-resp-enable(SIP ERROR RESPONSE): Configures how to reject a received call when maximum allowed number of calls is exceeded.
  - Disable (default): No response for a received call connection request message. The received message is not forwarded to the called side.
  - Enable: Rejects by transmitting 503 Service Unavailable SIP response for a received call connection request message. The received message is not forwarded to a called side.
- sipalg sip-detect-long-call-enable (SIP DETECT LONG DURATION CALL): Configures whether to delete an internal resource by detecting abnormal remaining calls. The values configured in the below two timers are used to judge an abnormal remaining call.
  - SIP No Answer Timeout (SIP Long Call Setuptimer): Maximum allowed time of the status before call connection (range: 300-3600, default: 600)
  - SIP Connect Timeout (SIP Long Call EstblshTimer): Maximum allowed time for a connected call (range: 3600-86400, default: 7200)
- sipalg sip-long-call-timeout (SIP NO ANSWER TIMEOUT, SIP CONNECT TIMEOUT): Configures a time required to judge an abnormal remaining call and enter SIP No Answer Timeout and SIP Connect Timeout in order.

To enable SIP ALG, execute the command as follows:

1) Go to configure mode of CLI.

```
APC# configure terminal
```

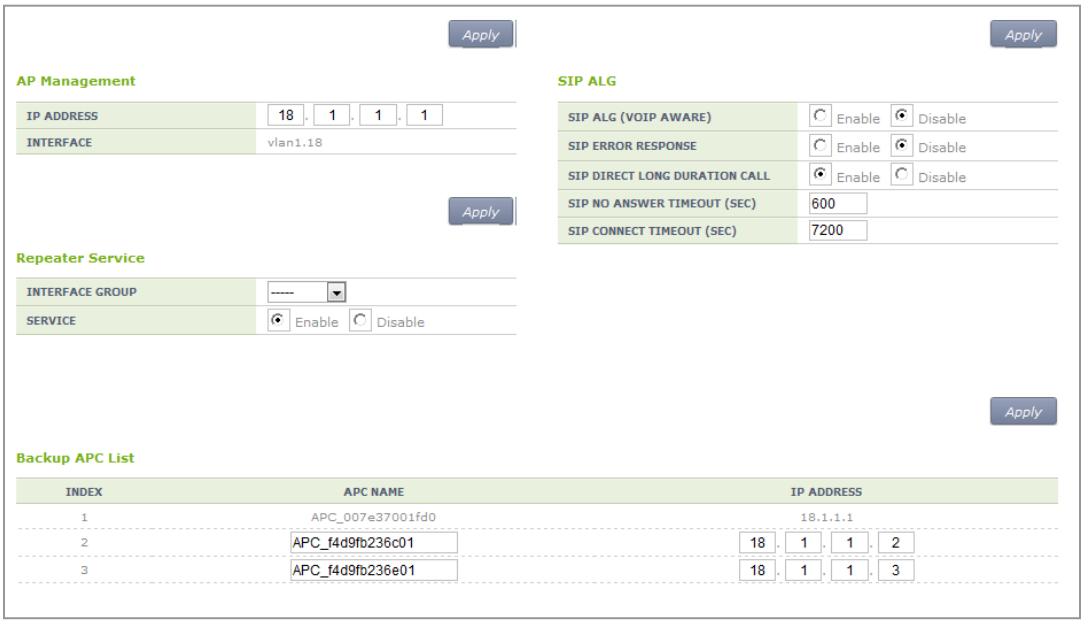
2) Enable the SIP ALG.

```
APC/configure# sipalg enable
```

3) To check the configuration information, use the ‘show sipalg configuration’ command.

Configuration using Web UI

In the menu bar of **<WEC Main window>**, select **<Configuration>** and then select the **<Controller>** → **<General>** menu in the sub-menus.



AP Management

IP ADDRESS	18 . 1 . 1 . 1
INTERFACE	vlan1.18

Repeater Service

INTERFACE GROUP	-----
SERVICE	● Enable ○ Disable

SIP ALG

SIP ALG (VOIP AWARE)	○ Enable ● Disable
SIP ERROR RESPONSE	○ Enable ● Disable
SIP DIRECT LONG DURATION CALL	● Enable ○ Disable
SIP NO ANSWER TIMEOUT (SEC)	600
SIP CONNECT TIMEOUT (SEC)	7200

Backup APC List

INDEX	APC NAME	IP ADDRESS
1	APC_007e37001fd0	18.1.1.1
2	APC_f4d9fb236c01	18 . 1 . 1 . 2
3	APC_f4d9fb236e01	18 . 1 . 1 . 3

Figure 133. SIP ALG configuration window

After configuring SIP ALG that is a voice CAC related configuration in the SIP ALG, click the **<Apply>** button.

7.3.2 Voice CAC Configuration

To protect existing calls, the voice CAC function configures maximum allowed number of calls and rejects any call request when the maximum number is exceeded. You can configure the number of marginal voice calls for handover.

Configuration using CLI

For voice CAC configuration, execute the command as follows:

1) Go to configure → voice CAC mode of a wireless section of CLI.

```
APC# configure terminal
APC/configure# [80211a/80211bg] cac voice
APC/configure/80211a/cac/voice#
```

2) Enable or disable the voice CAC function.
   - acm [MODE]

Parameter	Description
MODE	Enables or disables the voice CAC function - enable: Enable - disable: Disable

3) Configure maximum allowed number of voice calls.
   - max-calls [VALUE]

Parameter	Description
VALUE	Maximum allowed number of voice calls.

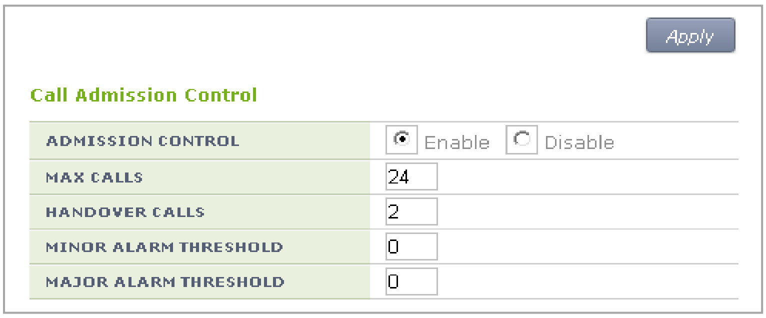
4) Configure the number of marginal voice calls considering the handover.
   - reserved-ho-calls [VALUE]

Parameter	Description
VALUE	Number of marginal voice calls considering the handover

5) To check the configured voice CAC information, use the ‘show [80211a | 80211bg] cac voice configuration’ command.

Configuration using Web UI

In the menu bar of **<WEC Main window>**, select **<Configuration>** and then select the **<Radio>** →**<802.11a/n>** or **<802.11b/g/n>** → **<Admission Control>** menu in the sub-menus.



Call Admission Control

ADMISSION CONTROL	● Enable ○ Disable
MAX CALLS	24
HANDOVER CALLS	2
MINOR ALARM THRESHOLD	0
MAJOR ALARM THRESHOLD	0

Figure 134. Admission control configuration of 802.11a/n

After configuring the below item in the Call Admission Control, click the **<Apply>** button.

- ADMISSION CONTROL: Configures the CAC function.
- MAX CALLS: Maximum number of allowed calls (range: 2-30)
- HANDOVER CALLS: Number of marginal calls considering handover (range: 0-10)
  The number of allowed calls is MAX CALLS-HANDOVER CALLS.
- MINOR ALARM THRESHOLD: Configures a threshold that generates a Minor alarm (range: 0-15)
  Enter ‘0’ to prevent the alarm.
- MAJOR ALARM THRESHOLD: Configures a threshold that generates a Major alarm (range: 0-30)
  Enter ‘0’ to prevent the alarm.

7.3.3 Video CAC Configuration

To protect existing video calls, the video CAC function configures the maximum allowed number of video calls and rejects any call request when the maximum number is exceeded. You can configure the number of marginal calls for handover.

Configuration using CLI

For video CAC configuration, execute the command as follows:

1) Go to configure → video CAC mode of a wireless section of CLI.

```
APC# configure terminal
APC/configure# [80211a/80211bg] cac video
APC/configure/80211a/cac/video#
```

2) Enable or disable the video CAC function.
   - acm [MODE]

Parameter	Description
Mode	Enables or disables the CAC function - enable: Enable - disable: Disable

3) Select a video CAC method.
   - method [method]

Parameter	Description
method	Select a video CAC method (static/chan_util) - static: Based on video calls - chan_util: Based on channel usage

4) Configure the maximum allowed number of calls.
   - max-calls [VALUE]

Parameter	Description
VALUE	Maximum allowed number of video calls

5) Configure the number of marginal calls with consideration for handover.
   - reserved-ho-calls [VALUE]

Parameter	Description
VALUE	Number of marginal calls with consideration for handover

6) Configure the maximum allowed usage of channels.
   - max-chan-util [VALUE]

Parameter	Description
VALUE	Maximum allowed usage of channels

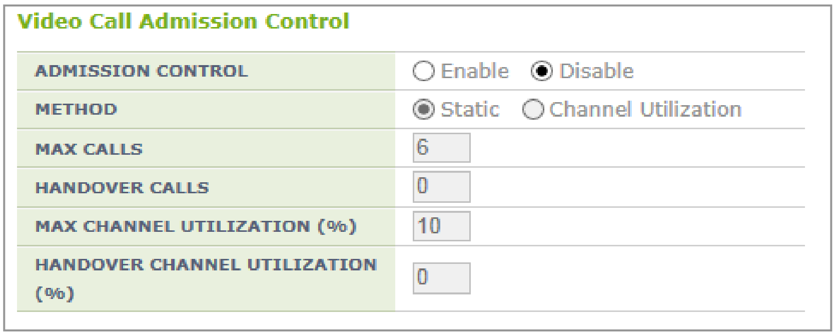
7) Configure the usage of marginal channels with consideration for handover.
   - reserved-ho-chan-util [VALUE]

Parameter	Description
VALUE	Usage of marginal channels with consideration for handover

8) You can view the video CAC information you configured by executing the 'show [80211a | 80211bg] cac video configuration' command.

Configuration using Web UI

From the menu bar of **<WEC Main Window>,** select **<Configuration>** and then select **<Radio>**→ **<802.11a/n>** or **<802.11b/g/n>** → **<Admission Control>** in the submenus.



Video Call Admission Control

ADMISSION CONTROL	○ Enable ● Disable
METHOD	● Static ○ Channel Utilization
MAX CALLS	6
HANDOVER CALLS	0
MAX CHANNEL UTILIZATION (%)	10
HANDOVER CHANNEL UTILIZATION (%)	0

Figure 135. 802.11a/n Admission Control Configuration Window

After configuring the items below in the Call Admission Control, click the **<Apply>** button.

- ADMISSION CONTROL: Configure the video CAC function
- METHOD: Select a video CAC method (static/chan_util)
- MAX CALLS: Maximum allowed number of calls (range: 2-30)
- HANDOVER CALLS: Number of marginal calls with consideration for handover (range: 0-8)
  The maximum allowed number of calls becomes MAX CALLS-HANDOVER CALLS.
- MAX CHANNEL UTILIZATION (%): Maximum allowed usage of channels (range: 5-85)
- HANDOVER CHANNEL UTILIZATION (%): Usage of marginal channels with consideration for handover (range: 0-25)

7.4 Radio Resource Management (RRM)

RRM performs automatic setup function for AP’s channel and Tx Power. RRM is functionally divided into Dynamic Channel Selection (DCS), Dynamic Power control (DPC), and Coverage Hole Detection and Control (CHDC). The DCS automatically sets the channels of the APs. The DPC DCS automatically sets the Tx Power of the AP. The CHDC adjusts the Tx Power when Coverage Hole occurs.

7.4.1 RRM Configuration

This section describes the settings for using the RRM function and the cluster configuration.

Configuration using CLI

To configure each function, execute the command as follows:

1) Go to configure → rrm configuration mode of CLI.

```
WEC8500# configure terminal
WEC8500/configure# rrm
```

2) Enable RRM. The ‘no’ parameter is used to disable RRM. DCS, DPC and CHDC, which are functions of RRM, can run only if the RRM is enabled.

```
WEC8500/configure/rrm# enable
```

3) In the cluster environment, set the same RF Group Name to all the connected APCs. A name must consist of up to 15 characters.

```
WEC8500/configure/rrm# rf-group-name [Name]
```

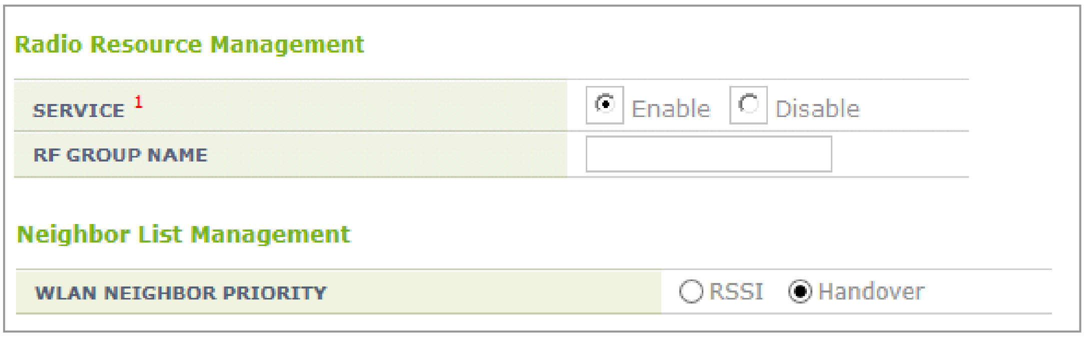
4) Configure priorities between the neighbor list of each Wlan. Go to the wireless section the configuration of which you want to change and then enter neighbor-list setup mode. You can select between rssi and handover, and the default value is rssi.

```
WEC8500/configure/rrm# 80211a
WEC8500/configure/rrm/80211a# neighbor-list
WEC8500/configure/rrm/80211a/neighbor-list# wlan-neighbor-priority
rssi/handover
```

5) To check the configured information, use the ‘show rrm config-summary’ command.

Configuration using Web UI

In the menu bar of **<WEC Main window>**, select **<Configuration>** and then select the **<Radio>** → **<802.11a/n/ac>** or **<802.11b/g/n>** → **<RRM>** menu in the sub-menus. Enable or disable the RRM service at the top of the menu. The RRM can be set in either 802.11a/n/ac screen or 802.11b/g/n screens. Configure priorities between the neighbor list of each Wlan at the bottom of the menu.



Radio Resource Management

SERVICE [1] ● Enable ○ Disable

RF GROUP NAME

Neighbor List Management

WLAN NEIGHBOR PRIORITY ○ RSSI ● Handover

Figure 136. RRM configuration window

7.4.2 DPC Configuration

This section describes the setting options of the DPC function which automatically sets the Tx Power of the AP.

Configuration using CLI

1) Go to configure → rrm configuration mode of CLI.

```
WEC8500# configure terminal
WEC8500/configure# rrm
```

2) Go to the wireless section where you want to change the settings.

```
WEC8500/configure/rrm# 80211a
```

3) Set the DPC function. Enter the dpc setting mode and set it to ‘enable’. Use the ‘no’ parameter to disable the mode. The function operates only when the RRM is set to Enable.

```
WEC8500/configure/rrm/80211a# dpc
WEC8500/configure/rrm/80211a/dpc# enable
```

4) Execute the following command to change the Received Signal Strength Indication (RSSI) threshold for neighbor AP. The default value is -70 (dBm).

```
WEC8500/configure/rrm/80211a/dpc# rssi-threshold [value]
```

5) If you need to change the RSSI threshold for the station, execute the following command. The default value is -70 (dBm). This parameter is used only in the DCS-DPC joint algorithm.

```
WEC8500/configure/rrm/80211a/dpc# rssi-threshold-for-stn [value]
```

6) Execute the following command to change the execution interval. The default value is 600 (seconds).

```
WEC8500/configure/rrm/80211a/dpc# periodic-interval [value]
```

7) Execute the following command to change the Tx Power range which is automatically set by DPC. The default minimum is 16 for 80211a and 12 for 80211b.
The default maximum is 20 for both 80211a and 80211b.

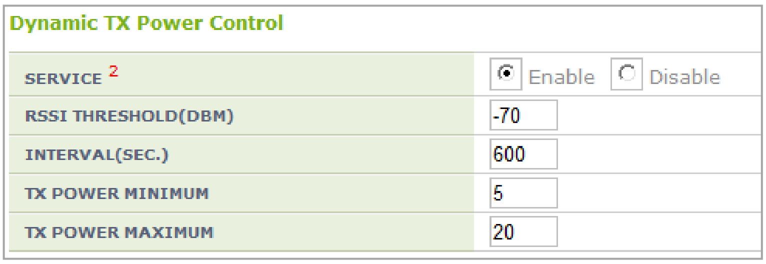
```
WEC8500/configure/rrm/80211a/dpc# txPower min [value] max [value]
```

8) Check the settings using the ‘show rrm config-summary’ command.

Configuration using Web UI

In the menu bar of **<WEC Main window>**, select **<Configuration>** and then select the **<Radio>** → **<802.11a/n/ac>** or **<802.11b/g/n>** → **<RRM>** menu in the sub-menus.

Enable or disable the DPC in the SERVICE field in Dynamic TX Power Control.



Dynamic TX Power Control

SERVICE [2]	● Enable ○ Disable
RSSI THRESHOLD(DBM)	-70
INTERVAL(SEC.)	600
TX POWER MINIMUM	5
TX POWER MAXIMUM	20

Figure 137. DPC settings

7.4.3 DCS Configuration

This section describes the setting options of the DCS function which automatically sets the channel of the AP.

Configuration using CLI

1) Go to configure → rrm configuration mode of CLI.

```
WEC8500# configure terminal
WEC8500/configure# rrm
```

2) Go to the wireless section where you want to change the settings.

```
WEC8500/configure/rrm# 80211a
```

3) Set the DCS function. Enter the dcs setting mode and set it to ‘enable’. Use the ‘no’ parameter to disable the mode. The function operates only when the RRM is set to Enable.

```
WEC8500/configure/rrm/80211a# dcs
WEC8500/configure/rrm/80211a/dcs# enable
```

4) Configure whether to apply the DCS-DPC joint algorithm. If the ‘no’ parameter is selected, the configuration is cleared.

```
WEC8500/configure/rrm/80211a/dcs# joint-algo-enable
```

5) Execute the following command to change the execution interval. The default value is 120 (seconds).

```
WEC8500/configure/rrm/80211a/dcs# periodic-interval [value]
```

6) Execute the following command to change the Channel Utilization threshold. The default value is 80 (%).

```
WEC8500/configure/rrm/80211a/dcs# channel-utilization-threshold [value]
```

7) Execute the following command to change the My Utilization threshold. The default is 10 (%) for 802.11a and 40 (%) for 802.11b.

```
WEC8500/configure/rrm/80211a/dcs# my-utilization-threshold [value]
```

8) Execute the following command to set the anchor time. The default value is start time 4, end time 5. If both start time and end time are set to the same time, Anchor Run function is disabled.

```
WEC8500/configure/rrm/80211a/dcs# anchor-time start [value] end [value]
```

9) Execute the following command to change the channels that is automatically set by the DCS. Use the 'no' parameter to disable the mode.

```
WEC8500/configure/rrm/80211a/dcs# channel [value]
```

10) Execute the following command to use the Delayed Channel Change function.
To disable the configuration, enter the 'no' parameter. The default is Disable.
The Delayed Channel Change function delays channel change instead of changing it immediately when a channel becomes busy due to channel utilization. If the anchor time is not configured, the default value is used at 4 o'clock.

```
WEC8500/configure/rrm/80211a/dcs# delayed-channel-change
```

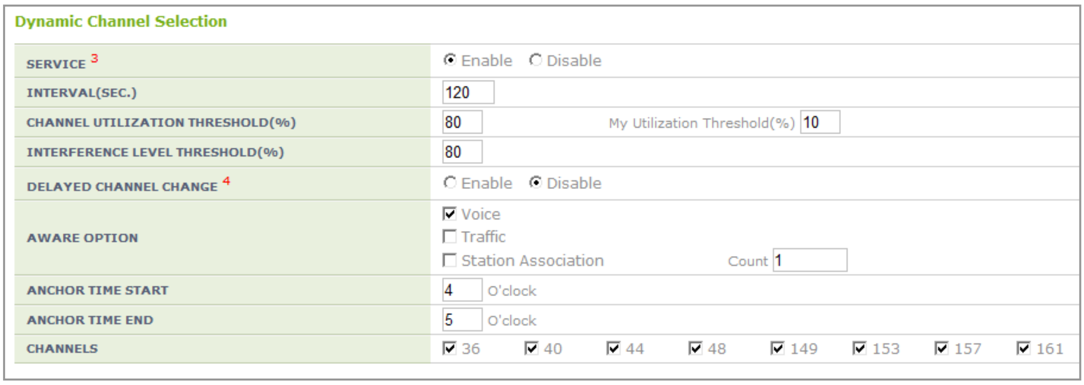
11) To use the Aware Option function, execute the following command. To disable the configuration, enter the 'no' parameter. The Aware Option does not change a channel if there is a specific condition. Therefore, three functions are provided based on whether there is a voice, the association of a station, or traffic in a station. The default is that only the Voice Aware function is enabled. The Station Aware function specifies the number of stations at the same time.

```
WEC8500/configure/rrm/80211a/dcs# aware-option voice
WEC8500/configure/rrm/80211a/dcs# aware-option station [station count]
WEC8500/configure/rrm/80211a/dcs# aware-option traffic
```

12) Check the settings using the 'show rrm config-summary' command.

Configuration using Web UI

In the menu bar of **<WEC Main window>**, select **<Configuration>** and then select the **<Radio>** → **<802.11a/n/ac>** or **<802.11b/g/n>** → **<RRM>** menu in the sub-menus. Enable or disable the DCS in the SERVICE field in Dynamic Channel Selection.



Dynamic Channel Selection

SERVICE [3]	● Enable ○ Disable
INTERVAL(SEC.)	120
CHANNEL UTILIZATION THRESHOLD(%)	80 My Utilization Threshold(%) 10
INTERFERENCE LEVEL THRESHOLD(%)	80
DELAYED CHANNEL CHANGE [4]	○ Enable ● Disable
AWARE OPTION	☑ Voice □ Traffic □ Station Association Count 1
ANCHOR TIME START	4 O'clock
ANCHOR TIME END	5 O'clock
CHANNELS	☑ 36 ☑ 40 ☑ 44 ☑ 48 ☑ 149 ☑ 153 ☑ 157 ☑ 161

Figure 138. DCS settings

7.4.4 CHDC Configuration

This section describes the setting options of the CHDC function which adjusts the Tx Power when Coverage Hole occurs.

Configuration using CLI

1) Go to configure → rrm configuration mode of CLI.

```
WEC8500# configure terminal
WEC8500/configure# rrm
```

2) Go to the wireless section where you want to change the settings.

```
WEC8500/configure/rrm# 80211a
```

3) Set the CHDC function. Enter the chdc setting mode and enable it Use the ‘no’ parameter to disable the mode. The function operates only when the RRM is enabled.

```
WEC8500/configure/rrm/80211a# chdc
WEC8500/configure/rrm/80211a/chdc# enable
```

4) To use the pre-alarm function, operator can collect the statistics from an AP. After entering into the chdc configuration mode, complete configuration (statsCollectEnable). To disable the configuration, enter the ‘no’ parameter. All the functions for pre-alarm are available only when both RRM and CHDC are enabled.

WEC8500/configure/rrm/80211a/chdc# statsCollectEnable

```
Success: DBI set for DPC 11A Stats collect Enable : 1
```

5) If a coverage hole is estimated from the statistics for the pre-alarm function, a warning can be transmitted. After entering into the chdc configuration mode, complete configuration (statsWarningEnable). To disable the configuration, enter the ‘no’ parameter.

```
WEC8500/configure/rrm/80211a/chdc# statsWarningEnable
Success: DBI set for DPC 11A Stats Warning Enable : 1
```

6) If a coverage hole is estimated from the statistics for the pre-alarm function, CHDC can be executed. After entering into the chdc configuration mode, complete configuration (statsActionEnable). To disable the configuration, enter the ‘no’ parameter.

```
WEC8500/configure/rrm/80211a/chdc# statsActionEnable
Success: DBI set for DPC 11A Stats Action Enable : 1
```

7) Configure the minimum value of statistics Failed Client Count for the pre-alarm function. It can be 1~75.

```
WEC8500/configure/rrm/80211a/chdc# min-failed-client-count 70
CHDC 802.11a : Set Minimum Failed Client Count Success
```

8) Configure the percentage of statistics Failed Client Count for the pre-alarm function. It can be 10~35.

```
WEC8500/configure/rrm/80211a/chdc# percent-failed-client-count 20
Success: CHDC 802.11a : Set Percentage of Failed Client Count Success
```

9) Configure the threshold of RSSI that will be added to the statistics Failed Client Count for the pre-alarm function. Configure it for Voice Frame and Data Frame. It can be -90~-20 (dB).

```
WEC8500/configure/rrm/80211a/chdc# rssi-threshold data -75
Success: CHDC 802.11a : Set RSSI THRESHOLD(-75)  Successful

WEC8500/configure/rrm/80211a/chdc# rssi-threshold voice -75
Success: CHDC 802.11a : Set RSSI THRESHOLD(-75)  Successful
```

10) Configure a value that requests an interval to an AP to collect statistics for the pre-alarm function. The default is 120 seconds and it can be 30~3600 seconds.

```
WEC8500/configure/rrm/80211a/chdc# statsCollectInterval 60
This Value: 60 is already set
```

11) Configure the minimum value of the idle time-out count of statistics for the pre-alarm function. This parameter can have a value ranging from 0 to 1,000.

```
WEC8500/configure/rrm/80211a/chdc# min-idle-timeout-count 10
CHDC : Set Minimum IdleTimeOutCnt Success
```

12) To check the configured information, execute the ‘show rrm config-summary’ command. In the ‘Coverage Hole Detection and Control’, operator can check the current status of all the configured values.

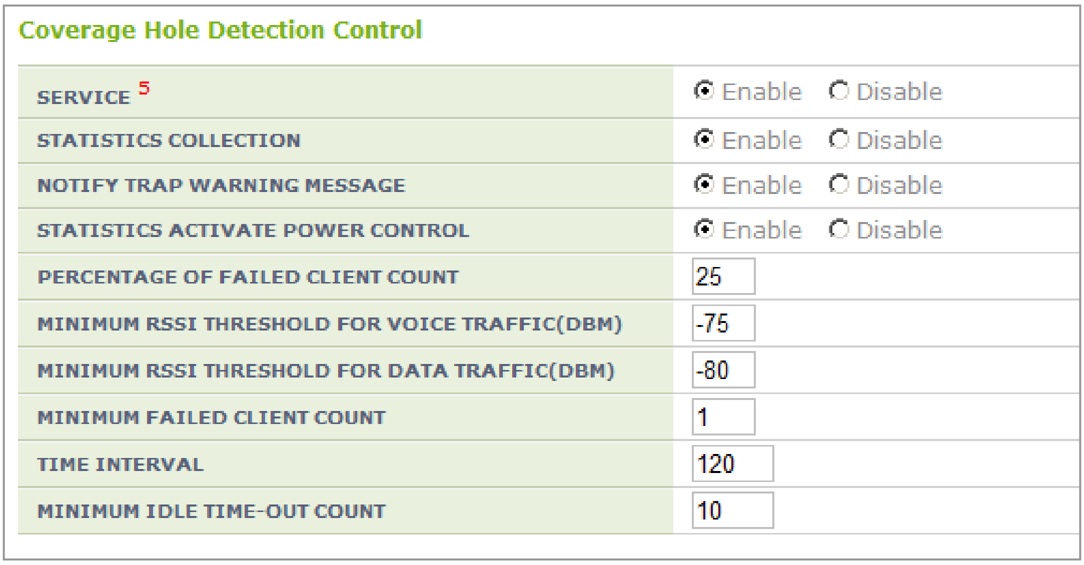
```
WEC8500/configure/rrm/80211a/chdc# show rrm config-summary

RRM Status  .....   Enabled
  Rf Group Name ...   Group
                                       80211a/n         80211b/g/n
  Dynamic Power Control ----------------------- -----------------
   DPC Enable                      ..  Enabled          Enabled
   Periodic Interval               ..  follow DCS       follow DCS
   RSSI Threshold for Neighbor AP  ..  -70              -70
   RSSI Threshold for Station      ..  -70              -70
   TX Power Min. - Max.            ..  17 - 20          14 - 20
   Minimum Number of AP            ..  2                2
   Elapsed Time After Last Run     ..  36               7
  Dynamic Channel Selection ------------------- -----------------
   DCS Enable                      ..  Enabled          Enabled
   DCS-DPC Joint Algorithm Enable  ..  Enabled          Enabled
   Periodic Interval               ..  60               60
   Anchor Time Start               ..  0                0
   Anchor Time Stop                ..  23               23
   Interference Level Threshold    ..  80               80
   Channel Utilization Threshold   ..  99               99
   My Utilization Threshold        ..  10               40
   Delayed Channel Change          ..  Enabled          Enabled
   Aware-Option: Voice Call        ..  Enabled          Enabled
   Aware-Option: Traffic           ..  Enabled          Enabled
   Aware-Option: Station Assoc.    ..  Enabled          Enabled
   Station Count for Station Aware ..  1                1
   Elapsed Time After Last Run     ..  36               7
  Coverage Hole Detection and Control --------- -----------------
   CHDC Enable                     ..  Enabled          Enabled
   Statistics Collect Enable       ..  Enabled          Enabled
   Statistics Warning Enable       ..  Enabled          Enabled
```

```
      Statistics Action Enable         ..  Enabled          Enabled
      RSSI Voice Threshold             ..  -75              -75
      RSSI  Data Threshold             ..  80               -30
      Minimum Failed Client Count      ..  1                1
      Percentage Min. Failed Count     ..  25               25
      Minimum Idle time-out Count      ..  10               10
      Statistics Collect Interval      ..  120              60
     Neighbor List Management -------------------- -----------------
      WLAN Neighbor Priority           ..  Handover         Handover
```

Configuration using Web UI

In the menu bar of **<WEC Main window>**, select **<Configuration>** and then select the **<Radio>** → **<802.11a/n/ac>** or **<802.11b/g/n>** → **<RRM>** menu in the sub-menus.

In the Coverage Hole Detection Control window, operator can enable or disable the CHDC and configure the values using the same functions as the CLI.



Coverage Hole Detection Control

SERVICE [5]	● Enable ○ Disable
STATISTICS COLLECTION	● Enable ○ Disable
NOTIFY TRAP WARNING MESSAGE	● Enable ○ Disable
STATISTICS ACTIVATE POWER CONTROL	● Enable ○ Disable
PERCENTAGE OF FAILED CLIENT COUNT	25
MINIMUM RSSI THRESHOLD FOR VOICE TRAFFIC(DBM)	-75
MINIMUM RSSI THRESHOLD FOR DATA TRAFFIC(DBM)	-80
MINIMUM FAILED CLIENT COUNT	1
TIME INTERVAL	120
MINIMUM IDLE TIME-OUT COUNT	10

Figure 139. CHDC settings

7.4.5 Sleeping Cell Detection

This is a function that allows the APC to detect the statuses of APs that are not performing basic functions and transmit an alarm/warning.

Configuration using CLI

1) Enable/Disable: Configure whether the silent alarm detection function will be performed. (Enable: function performing, Disable: function not performing)

```
WEC8500/configure/rrm# sleep-cell-detect
WEC8500/configure/rrm/sleep-cell-detect# enable
```

2) APC Threshold: Minimum number of connected users throughout the whole APC for sleeping cell detection.
If the total number of STA associations is equal to or smaller than the APC threshold, the day is judged as a holiday and consequently the sleeping cell detection is not performed.

```
WEC8500/configure/rrm/sleep-cell-detect# apc-threshold
```

3) AP Threshold: Minimum number of users connected to an AP for sleeping cell detection.
If the number of STA associations of an AP is equal to or smaller than the AP threshold, a silent alarm occurs.

```
WEC8500/configure/rrm/sleep-cell-detect# ap-threshold
```

4) PERIOD_1ST: Start and end times of sleeping cell detection for Specific Period 1. (For a full day, set the start and end times as the same time.)

```
WEC8500/configure/rrm/sleep-cell-detect# period_1st
```

5) PERIOD_2ND: Start and end times of sleeping cell detection start for Specific Period 2. (For a full day, set the start and end times as the same time.)

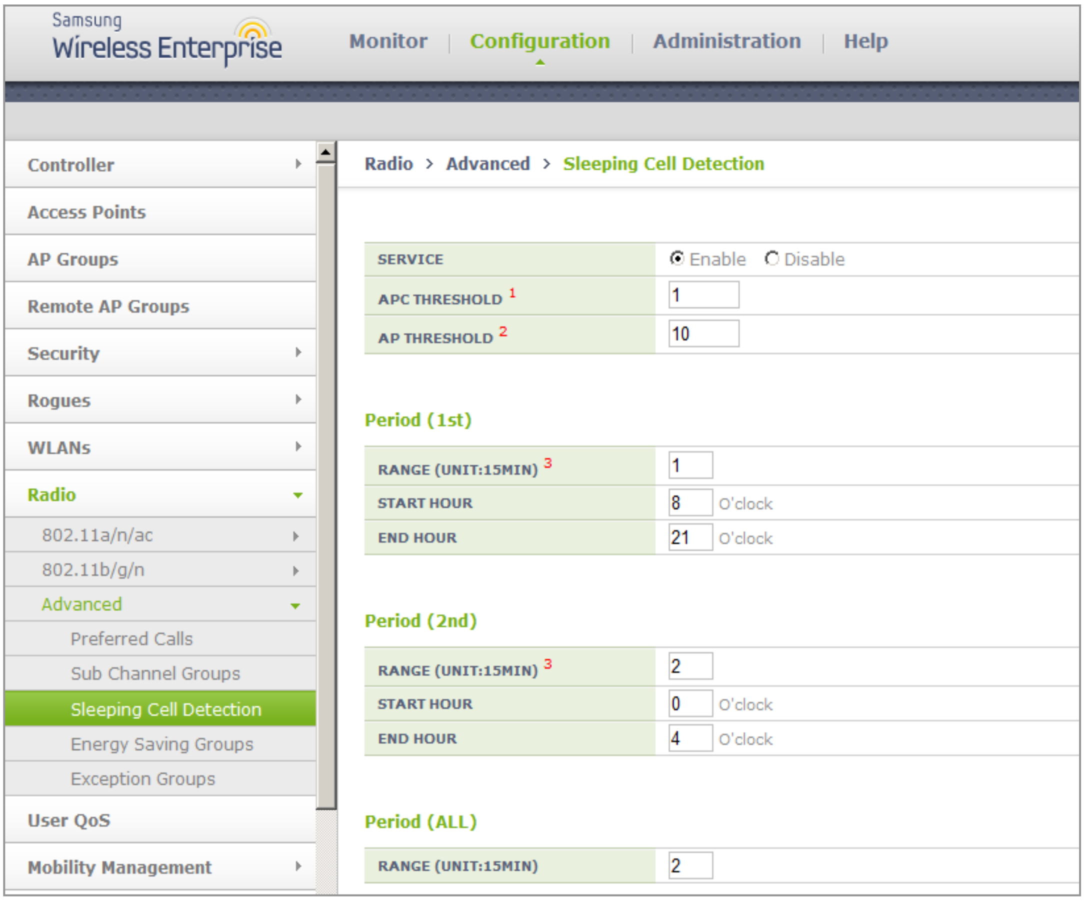
```
WEC8500/configure/rrm/sleep-cell-detect# period_2nd
```

6) PERIOD_ALL: Start and end times of sleeping cell detection for periods other than Specific Periods 1 and 2.

```
WEC8500/configure/rrm/sleep-cell-detect# period_all
```

Configuration using Web UI

From the menu bar of **<WEC Main Window>**, select **<Configuration>** and then select **<Radio>** → **<Advanced>** → **<Sleeping Cell Detection>** in the submenus.



SERVICE	● Enable ○ Disable
APC THRESHOLD [1]	1
AP THRESHOLD [2]	10

Period (1st)

RANGE (UNIT:15MIN) [3]	1
START HOUR	8 O'clock
END HOUR	21 O'clock

Period (2nd)

RANGE (UNIT:15MIN) [3]	2
START HOUR	0 O'clock
END HOUR	4 O'clock

Period (ALL)

RANGE (UNIT:15MIN)	2

7.4.6 Energy Saving

- The purpose is to reduce the power consumption of the APC by turning off the RF radios of APs without any connected STA at a specific time when the number of STAs connected to the APC drops drastically.
- The APs of the APC are divided into the active group in which APs are always in operation and the standby group in which the RF radios of APs are turned off.
  When the standby group (energy saving group) is defined, the APC recognizes the remaining APs as the active group. You can define up to 10 groups.

Configuration using CLI

1) Enable/Disable: Configure whether the energy saving function will be performed.
(Enable: function performing, Disable: function not performing)

```
WEC8500/configure/rrm# energy-saving-group 1
WEC8500/configure/rrm/energy-saving-group 1# enable
```

2) APC Threshold: Maximum number of connected users throughout the whole APC for energy saving detection.
If the total number of STA associations is equal to or smaller than the APC threshold, the day is judged as a holiday and the energy saving function is performed according to the times set for weekends.

```
WEC8500/configure/rrm/energy-saving-group 1# apc-threshold
```

3) WEEKDAY: Start and end times of energy saving for weekdays.
(For a full day, set the start and end times as the same time.)

```
WEC8500/configure/rrm/energy-saving-group 1# weekday
```

4) WEEKDEND: Start and end times of energy saving for weekends.
(For a full day, set the start and end times as the same time.)

```
WEC8500/configure/rrm/energy-saving-group 1# weekend
```

5) ADD-AP: Add AP members to the energy saving group.

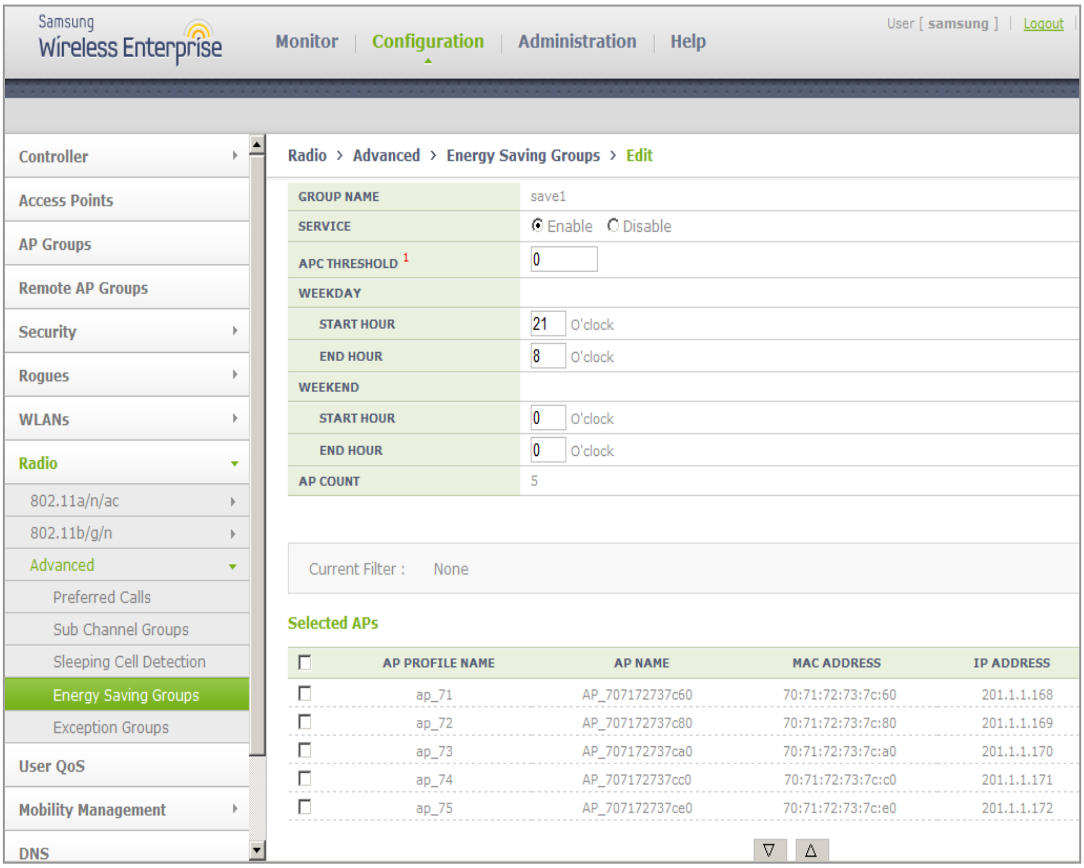
```
WEC8500/configure/rrm/energy-saving-group 1# add-ap
```

6) DEL-AP: Delete AP members from the energy saving group.

```
WEC8500/configure/rrm/energy-saving-group 1# del-ap
```

Configuration using Web UI

From the menu bar of <WEC Main Window>, select **<Configuration>** and then select **<Radio>** → **<Advanced>** → **<Energy Saving Groups>** → **<GROUP NAME>** in the submenus.



GROUP NAME	save1
SERVICE	● Enable ○ Disable
APC THRESHOLD [1]	0
WEEKDAY	
START HOUR	21 O'clock
END HOUR	8 O'clock
WEEKEND	
START HOUR	0 O'clock
END HOUR	0 O'clock
AP COUNT	5

Current Filter : None

Selected APs

□	AP PROFILE NAME	AP NAME	MAC ADDRESS	IP ADDRESS
□	ap_71	AP_707172737c60	70:71:72:73:7c:60	201.1.1.168
□	ap_72	AP_707172737c80	70:71:72:73:7c:80	201.1.1.169
□	ap_73	AP_707172737ca0	70:71:72:73:7c:a0	201.1.1.170
□	ap_74	AP_707172737cc0	70:71:72:73:7c:c0	201.1.1.171
□	ap_75	AP_707172737ce0	70:71:72:73:7c:e0	201.1.1.172

7.5 Location Tracking

The APC tracks the location information of several terminals in a wireless LAN network based on the wireless data collected from W-EP wireless LAN APs.

To configure the location tracking function, execute the command as follows:

1) Go to configure → locationtrack configuration mode of CLI.

```
WEC8500# configure terminal
WEC8500/configure # locationtrack
WEC8500/configure/locationtrack #
```

2) Configure the location tracking function.

```
WEC8500/configure/locationtrack # enable
```

3) To check the configured information, execute the ‘show locationtrack config’ command.

```
WEC8500/configure/locationtrack # show locationtrack config
Location tracking enable....: Enabled
Algorithm type..............: 4
Expiry date of history files: 0
```

4) Configure the MAC address of a wireless terminal for which the tracking function will be executed.
   - station [MAC_ADDRESS]

5) To check the location information of a wireless terminal to track, execute the ‘show locationtrack station’ command.

```
WEC8500/configure/locationtrack # show locationtrack station
No.  stationId station_MAC_Addr  ap_MAC_Addr       (staX,staY)
lastTime(+)
---- --------- ----------------- ----------------- ----------------- -
-------------------
1            1 f4:d9:fb:34:20:60 f4:d9:fb:34:20:60 (2432,1947)
0(1374022070)
```

7.6 Spectrum Analysis

A non-802.11 device such as microwave oven, bluetooth, or Closed Circuit Television (CCTV), etc. deteriorates data transmitting/receiving performance because it causes interference in a wireless LAN environment. As a function that measures surrounding interference, the spectrum analysis analyzes wireless or Radio Frequency (RF) signals to resolve interference problem instantly.

7.6.1 Retrieving Spectrum Analysis Data

The spectrum analysis function of APC provides the following data.

- Sample report: Wireless capture data converted into Fast Fourier Transform (FFT)
- Duty cycle report: Channel utilization rate
- Interference report: Interference signal information

The FFT report provides the information of an AP and maximum 13 available channels and also maximum/minimum values of Received Signal Strength Indicator (RSSI) for each channel. The duty cycle report provides AP information and affected channel information. In addition, it provides duty cycle transmission data that indirectly provides channel utilization rate.
The interference report provides AP information, affected channel, or configuration information of an interferer and also interference information (RSSI or maximum/minimum frequency of an interference signal) in real-time.

Configuration using CLI

By using the following command, you can check each data.

- show spectrum-analysis report [DATA] ap [AP_ID]

Parameter	Description
DATA	Spectrum analysis data type (sample/duty_cycle/interference)
AP_ID	AP ID (range: 1-500)

An example of command execution and its execution result are as follows:

- FFT report

```
APC# show spectrum-analysis report sample ap 1

FFT (Fast Fourier Transform) Reporting Enabled
AP ID 1 Description:
   MAC Address.................................... 00:11:22:33:44:55
   Name........................................... AP_ 01122334455
   IP Address..................................... 100.100.100.220
   Mode........................................... General
   Operational Status.............................. Up
   Map Location....................................
Channel Information:
   Channel Interval................................ 2000 ms
   Channel......................................... 1 2 3 4 5 6 7 8
9 10 11 12 13

Channel ID........................................ 1
-----------------------------
Num  Maximum RSSI  Average RSSI
--- ------------ ------------
  1   -120        -120
  2   -120        -120
  3   -120        -120
  4   -120        -120
  5   -120        -120
  6   -120        -120
  7   -120        -120
  8   -120        -120
  9   -120        -120
 10   -120        -120
 11   -120        -120
 12   -120        -120
 13   -120        -120
 14   -120        -120
 15   -120        -120
 16   -120        -120
 17   -120        -120
 18   -120        -120
 19   -120        -120
 20   -120        -120
 21   -120        -120
 22   -120        -120
 23   -120        -120
 24   -120        -120
 25   -120        -120
 26   -120        -120
 27   -120        -120
 28   -120        -120
 29   -120        -120
 30   -120        -120
Press any key to continue (q : quit | enter : next line) :
```

- Duty cycle report

```
APC# show spectrum-analysis report duty_cycle ap 1

Duty Cycle Reporting Enabled
AP ID  1 Description:
   MAC Address..................................... 00:11:22:33:44:55
   Name............................................ AP_ 01122334455
   IP Address..................................... 100.100.100.220
   Mode........................................... General
   Operational Status............................. Up
   Map Location...................................
Affected Channels:
   Channel Interval............................... 2000 ms
   Channel........................................ 1 2 3 4 5 6 7 8 9
10 11 12 13
Real Time Duty Cycle Report:
Current Time : 2012-06-29 00:40:13
--------------------------------------------------------------------
   Channel:  1......................................... D:  100  %
   Channel:  2......................................... D:  100  %
   Channel:  3......................................... D:  100  %
   Channel:  4......................................... D:  100  %
   Channel:  5......................................... D:   30  %
   Channel:  6......................................... D:  100  %
   Channel:  7......................................... D:  100  %
   Channel:  8......................................... D:  100  %
   Channel:  9......................................... D:  100  %
   Channel: 10......................................... D:   50  %
   Channel: 11......................................... D:   97  %
   Channel: 12......................................... D:   70  %
   Channel: 13......................................... D:  100  %
--------------------------------------------------------------------
```

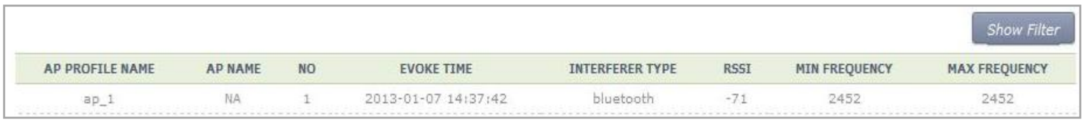
- Interference report

```
APC# show spectrum-analysis report interference ap 1
Interference Reporting Enabled
AP ID  1 Description:
   MAC Address.........................................
00:11:22:33:44:55
   Name................................................ AP_
01122334455
   IP Address..........................................
100.100.100.220
   Mode................................................ General
   Operational Status.................................. Up
   Map Location........................................

Affected Channels:
   Channel Interval.................................... 2000 ms
   Channel............................................. 1 2 3 4 5 6 7
8 9 10 11 12 13

Affected Interferers:
      BlueTooth........................................ Enabled
      Microwave Oven................................... Enabled
      802.11bgn Continuous Transmitter................. Enabled
      802.11bgn DECT-like Phone........................ Enabled
```

```
        802.11bgn Video Camera.......................... Enabled
        ZigBee.......................................... Enabled
        802.11an Continuous Transmitter................. Enabled
        802.11an DECT-like Phone........................ Enabled
        802.11an Video Camera........................... Enabled

Real Time Interference Report:
   Number of Interferers............................... 1
Num Evoke   Time Interferer Type   RSSI Minimum Frequency Maximum
Frequency
--- ------------------- ------------------------------ ---- --------
--------- -----------------
1   2012-06-29 08:52:47 802.11bgn Video Camera -80 2401   2401
```

Configuration using Web UI

In the menu bar of **<WEC Main window>,** select **<Monitor>** and then select the **<Interference Device>** menu in the sub-menus. You can retrieve the interference report.



AP PROFILE NAME	AP NAME	NO	EVOKE TIME	INTERFERER TYPE	RSSI	MIN FREQUENCY	MAX FREQUENCY
ap_1	NA	1	2013-01-07 14:37:42	bluetooth	-71	2452	2452

Figure 140. Spectrum Analysis Data

7.6.2 Spectrum Analysis Configuration

You can configure the spectrum analysis function and also a spectrum analysis channel that will be applied to each spectrum report. The channel information is as follows:

Radio	Channel
2.4 GHz	All, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13
5 GHz Low	All, 36, 40, 44, 48, 52, 56, 60, 64
5 GHz Mid	All, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136,140
5 GHz High	All, 149, 153, 157, 161, 165

To configure the spectrum analysis related function, you must go to the configuration mode of an AP for which the spectrum analysis function will be configured by executing the command as follows:

```
APC# configure terminal
APC/configure# spectrum-analysis ap 1
APC/configure/spectrum-analysis/ap 1#
```

[Enable/Disable Spectrum]

The command that enables or disables the spectrum analysis function is shown below.

- service [MODE]

Parameter	Description
MODE	Enables or disables spectrum analysis - enable: Enable (default) - disable: Disable

[Spectrum Analysis Report Configuration]

The command used to enable or disable each spectrum analysis data item is shown below.

- configuration-request [DATA] [MODE]

Parameter	Description
DATA	Type of a report to configure (sample/duty-cycle/interference) - sample: FFT report (default: disabled) - duty-cycle: Duty cycle report (default: disabled) - interference: Interference report (default: enable)
MODE	Enables or disables each report function. - enable: Enable - disable: Disable

[Channel Report Interval Configuration]

The command is shown below.

- channel-interval [INTERVAL]

Parameter	Description
INTERVAL	Channel report interval (range: 1000-60000 ms, default: 1000)

[Changing Channel]

By using the following command, you can change a channel for which the spectrum analysis will be executed.
(The default is ‘All’ channels.)

- dot11b: 2.4 GHz wireless bandwidth
- dot11aLow: 5 GHz low wireless bandwidth
- dot11aMid: 5 GHz mid wireless bandwidth
- dot11aHigh: 5 GHz high wireless bandwidth

7.6.3 Interference Type Configuration

The interference type of 2.4 GHz or 5 GHz that can be detected by the W-EP wireless LAN is shown below.

Wireless bandwidth	Interference type
2.4 GHz	continuous_transmitter, cordless_phone, video_camera
5 GHz	bluetooth, continuous_transmitter, cordless_phone, microwave_oven, video_camera, zigbee

To configure an interference type, execute the command as follows:

1) Go to configure mode of CLI.

```
APC# configure terminal
APC/configure#
```

2) Configure an interference type. The default value of all the interference types is ‘enabled’.
   - interferer 80211b zigbee: 2.4 GHz configuration
   - interferer 80211a cordless_phone: 5 GHz configuration

7.7 Controlling Usage per User

A wireless terminal can control traffic usage per user by receiving a QoS profile that specifies traffic usage (bandwidth) from the RADIUS server at the authentication stage. You can configure upward and downward usage per wireless terminal.

Configuration using CLI

The procedure of configuring a usage to a profile is as follows:

1) Go to configure mode of CLI.

```
APC# configure terminal
```

2) Create a QoS profile.

```
APC/configure# qos [PROFILE_NAME]
APC/configure/qos samsung#
```

Parameter	Description
PROFILE_NAME	Name of a QoS profile to create

3) Configure the downward usage in kbps.
   - bw-contract-downstream [VALUE]

Parameter	Description
VALUE	Downward usage

4) Configure the upward usage in kbps.
   - bw-contract-upstream [VALUE]

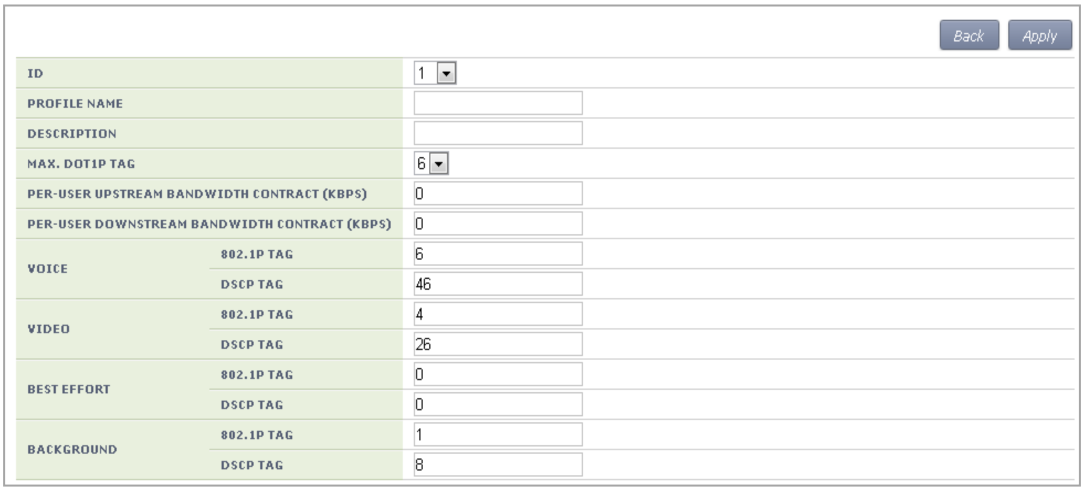
Parameter	Description
VALUE	Upward usage

5) To check the configured profile information, use the ‘show qos profile’ command.

Configuration using Web UI

In the menu bar of **<WEC Main window>,** select **<Configuration>** and then select the **<QoS>** menu in the sub-menus. To create a QoS profile to apply to a terminal, click the **<Add>** button in the initial window.

The QoS addition window consists of the following QoS parameters. By entering each QoS parameter, you can configure the QoS profile of a specific terminal or configure the usage control function for each user.



ID		1
PROFILE NAME		
DESCRIPTION		
MAX. DOT1P TAG		6
PER-USER UPSTREAM BANDWIDTH CONTRACT (KBPS)		0
PER-USER DOWNSTREAM BANDWIDTH CONTRACT (KBPS)		0
VOICE	802.1P TAG	6
	DSCP TAG	46
VIDEO	802.1P TAG	4
	DSCP TAG	26
BEST EFFORT	802.1P TAG	0
	DSCP TAG	0
BACKGROUND	802.1P TAG	1
	DSCP TAG	8

Figure 141. Controlling Usage per User

- ID: ID (range: 1-16)
- PROFILE NAME: Profile name
- DESCRIPTION: Profile description
- MAX. DOT1P TAG: Maximum allowed 802.1p tag (range: 0-7)
- PER-USER UPSTREAM BANDWIDTH CONTRACT: Maximum upward usage (range: 0-450000)
- PER-USER DOWNSTREAM BANDWIDTH CONTRACT: Maximum downward usage (range: 0-450000)
- VOICE/VIDEO/BEST EFFORT/BACKGROUND: Enter 802.1P TAG (range: 0-7) and DSCP TAG (range: 0-64) for each item.

7.8 Remote Packet Capture

APC can capture a packet exchanged between the wireless terminals on a remote PC in real-time by using the remote packet capture protocol.
To configure the remote packet capture function, you must go to the pcap mode by executing the command as follows:

```
APC# configure terminal
APC/configure# pcap
```

Configuring the MAC address of a wireless terminal

Configure the MAC address of a wireless terminal whose packets will be captured.

```
APC/configure/pcap# config-filter
APC/configure/pcap/config-filter# station-mac [MAC_ADDRESS]
APC/configure/pcap/config-filter# enable-station-mac [INDEX]
```

Parameter	Description
MAC_ADDRESS	MAC address (11:22:33:44:55:66 format)
INDEX	Index number of MAC address (range: 1-10)

Configuring AP MAC address

Configure the MAC address of an AP whose packets will be captured.

```
APC/configure/pcap# config-filter
APC/configure/pcap/config-filter# ap-mac [MAC_ADDRESS]
APC/configure/pcap/config-filter# enable-ap-mac [INDEX]
```

Parameter	Description
MAC_ADDRESS	MAC address (11:22:33:44:55:66 format)
INDEX	Index number of MAC address (range: 1-10)

Configuring Filtering Mode

Capture target can be specified by configuring the filtering mode

```
APC/configure/pcap# filtering-mode [FILTERING MODE]
```

Parameter	Description
FILTERING MODE	Filtering mode - station-only: Use only the configured station MAC information. - ap-only: Use only the configured AP MAC information.

Starting Service

You must start the remote packet capture service to connect to a device using a program that supports the remote packet capture protocol on a remote PC.

The related commands are given below.

```
APC/configure/pcap# start-service
```

Retrieving Configuration Information

Use the ‘show pcap current-config’ command to retrieve the remote packet capture configuration information.

```
APC# show pcap current-config detail

 - Current status : Idle
 - Filtering mode : station-only

 - Configured AP’s MAC Information
  No.      MAC Addr.       Filtering         Matched Count
Inbound Rate    Outbound Rate
 ===== ===================== =========== =============================
================ ================
  1   F4:D9:FB:23:66:00   --------> ON             0
0.0             0.0
       ID       Prf.            AP Name             IPv4 Addr
      ------ ----------- ----------------------- ---------------
        2      ap_2          AP_f4d9fb236600       10.10.10.20

 - Configured Station’s MAC Information
  No.      MAC Addr.       Filtering         Matched Count
Inbound Rate    Outbound Rate
 ===== ===================== =========== =============================
================ ================
  1   78:47:1D:C5:4C:85   OFF <-------             0
0.0             0.0
            AP   WN             SSID                IPv4 Addr
            ---- ---- --------------------------- ---------------
             2    2          Ajay_2_2_4G            20.20.20.30
  2   FC:A1:3E:47:59:E7   OFF <-------             0
0.0             0.0
            AP   WN             SSID                IPv4 Addr
            ---- ---- --------------------------- ---------------
             2    2          Ajay_2_2_4G            20.20.20.25

WEC8500#
```

7.9 Clustering

The clustering function comprehensively manages several APC systems in a single wireless LAN when several APC systems are used to manage a wireless LAN that cannot be managed by a single APC. The inter-APC handover function is provided by using clustering. In other words, it can provide the handover function between wireless LANs managed by different APC systems.
However, if a model is different, it is not interoperated through clustering.

Configuration using CLI

[Cluster Setting]
To use the clustering function, you must configure each APC according to the following procedure. Maximum 12 WEC8500 can be grouped in a cluster. Maximum 2 WEC8050 can be grouped in a cluster.

1) Go to configure mode of CLI.

```
WEC8500# configure terminal
WEC8500/configure#
```

2) Set the interval and the number of retries to transmit the Keep-alive messages between APCs in the cluster.
   - cluster keep-alive-interval [INTERVAL]
   - cluster keep-alive-retry-count [RETRY_COUNT]

Parameter	Description
INTERVAL	Interval to transmit the Keep-alive message (Unit: s, range: 1-30, default: 10)
RETRY_COUNT	Maximum number of the transmission retries when there is no response to the Keep-alive message (range: 3-20, default: 3)

3) Enable the cluster
   - cluster enable: Enable
   - no cluster enable: Disable

4) To check the configuration information, use the ‘show cluster config’ command.

```
WEC8500# show cluster config
========================================================
         CLUSTER CONFIGURATION INFORMATION
========================================================
  KEEP-ALIVE-INTERVAL      :  10
  KEEP-ALIVE-RETRY-COUNT   :  3
  ENABLE                        :  YES
  OWN-APC-INDEX                 :  1
========================================================
```

[Adding APC to APC List]

To add an APC to the cluster, the APC must be added to the APC list first. APC information is automatically added to the APC list.

1) Go to apc-list configure mode of CLI.

```
WEC8500# configure terminal
WEC8500/configure# apc apc-list
WEC8500/configure/apc/apc-list#
```

2) Add the APC to the APC list.
   - add-apc [APC_NAME] [MAC_ADDRESS]

Parameter	Description
APC_NAME	APC name to be added to the APC list
MAC_ADDRESS	MAC address of the APC to be added to the APC list (system mac address output parameter value of the ‘show system info’ command in the APC)

[Adding APC to cluster]

After adding APC to the APC list, the APC must be added to a cluster.

1) Go to configure mode of CLI.

```
WEC8500# configure terminal
WEC8500/configure#
```

2) Add the APC to a cluster.
   - cluster add-apc [INDEX] [APC_NAME] [IPV4_ADDRESS] [DB_REFRESH_INTERVAL]

Parameter	Description
INDEX	Index in cluster (range: 1-12)
APC_NAME	APC name (maximum 18 characters)
IPV4_ADDRESS	IPv4 address
DB_REFRESH_INTERVAL	Database update interval (Unit: s, range: 60-5000, default: 120)

[Deleting APC from cluster]

Delete the APC added in cluster. To delete an APC from a cluster, you must delete the APC from the cluster configuration of all the APCs in the cluster.

1) Go to configure mode of CLI.

```
WEC8500# configure terminal
WEC8500/configure#
```

2) Delete an APC from the cluster. To delete all the APC systems in a cluster, enter the ‘cluster del-apc-all’ command.
   - cluster del-apc [INDEX]
   - cluster del-apc-all

Parameter	Description
INDEX	Index in cluster (range: 1-12)

[Retrieving APC information added in cluster]

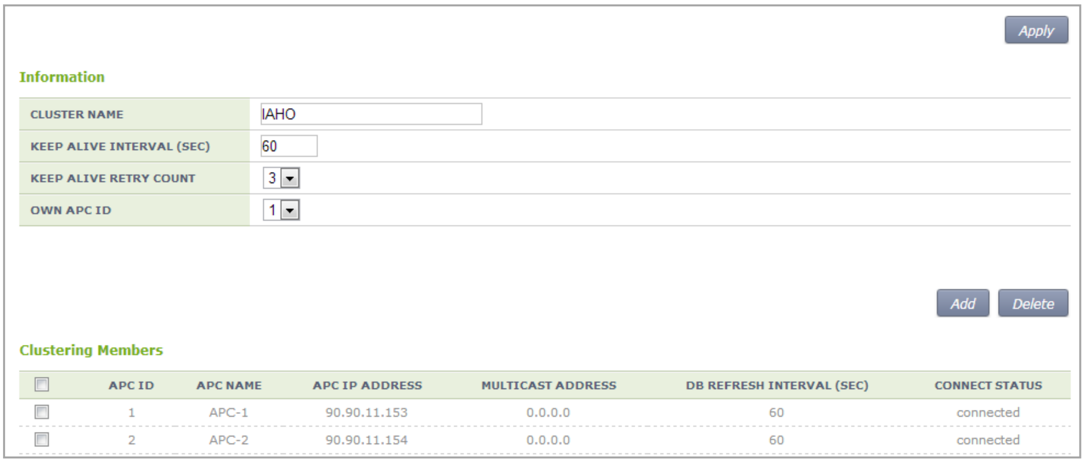
You can check the added APC information using the ‘show cluster list-apc’ command.

```
WEC8500# show cluster list-apc
======================================================================
INDEX  APC-NAME     IPv4-ADDRESS   DB-REF-INT CONNECT-STATUS
======================================================================
 1     APC-1       192.168.87.146 120        CONNECTED[1]
 2     APC-2       192.168.87.217 120        CONNECTED[1]
======================================================================
```

Configuration using Web UI

In the menu bar of <**WEC Main window**>, select <**Configuration**> and then select the <**Mobility Management**> → <**Clustering**> menu in the sub-menus.

The Clustering window is shown below.



Information

CLUSTER NAME	IAHO
KEEP ALIVE INTERVAL (SEC)	60
KEEP ALIVE RETRY COUNT	3
OWN APC ID	1

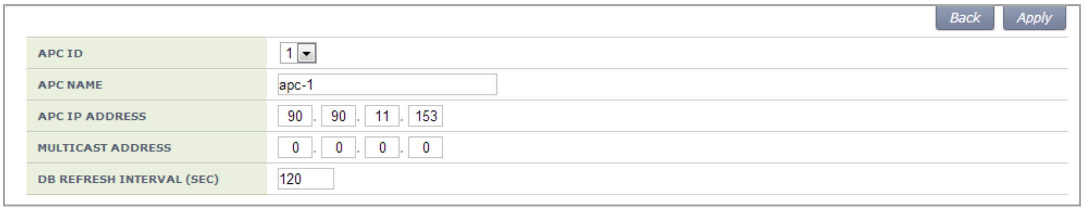
Clustering Members

□	APC ID	APC NAME	APC IP ADDRESS	MULTICAST ADDRESS	DB REFRESH INTERVAL (SEC)	CONNECT STATUS
□	1	APC-1	90.90.11.153	0.0.0.0	60	connected
□	2	APC-2	90.90.11.154	0.0.0.0	60	connected

Figure 142. Clustering window

Configure a clustering configuration value in the <**Information**> item and then click the <**Apply**> button to apply. The Clustering Members item shows all the clustering members. Click the <**Add**> or <**Delete**> button to add or delete a clustering member.

The clustering addition window is shown below.



APC ID	1
APC NAME	apc-1
APC IP ADDRESS	90 . 90 . 11 . 153
MULTICAST ADDRESS	0 . 0 . 0 . 0
DB REFRESH INTERVAL (SEC)	120

Figure 143. Clustering addition window

7.10 Limiting the Number of Connected Users

The W-EP wireless LAN system limits the number of wireless terminals connected to each AP. The limitation is per radio (2.4/5 GHz bandwidth) or WLAN for each AP.

7.10.1 Limiting Connections per Radio

Configuration using CLI

1) Go to configure mode of CLI.

```
APC# configure terminal
APC/configure#
```

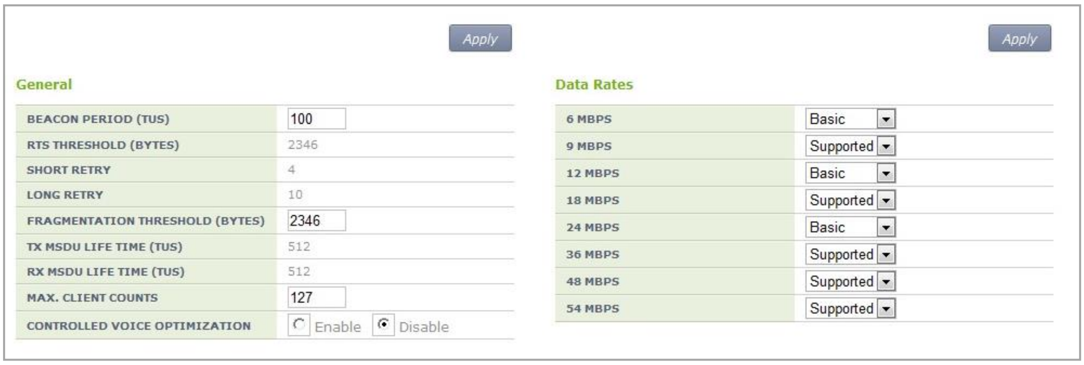
2) Configure connection limitation.
   - [RADIO] max-associated-stations [MAX_STATION] global: Configures connection limitation per wireless bandwidth. When you enter the ‘global’ parameter at the end, connection limitation is applied to all the APs.
   - [RADIO] max-associated-stations [MAX_STATION] [TARGET] [AP_ID]: Configures connection limitation to a specific AP.

Parameter	Description
RADIO	Wireless area to configure [80211bg/80211a] - 80211bg: 2.4 GHz area - 80211a: 5 GHz area
MAX-STATION	Maximum number of wireless terminals that can be connected (default: 127)
TARGET	Configuration range - AP: Index of an AP to configure - Global: All APs connected to an APC
AP_ID	AP ID (range: 1-500)

3) To check the configuration information, use the ‘show 80211bg radio-config global’ command.

Configuration using Web UI

In the menu bar of **<WEC Main window>**, select **<Configuration>** and then select the **<Radio>** → **<802.11a/n>** or **<802.11b/g/n>** → **<General>** menu in the sub-menus.



General

BEACON PERIOD (TUS)	100
RTS THRESHOLD (BYTES)	2346
SHORT RETRY	4
LONG RETRY	10
FRAGMENTATION THRESHOLD (BYTES)	2346
TX MSDU LIFE TIME (TUS)	512
RX MSDU LIFE TIME (TUS)	512
MAX. CLIENT COUNTS	127
CONTROLLED VOICE OPTIMIZATION	○ Enable ● Disable

Data Rates

6 MBPS	Basic
9 MBPS	Supported
12 MBPS	Basic
18 MBPS	Supported
24 MBPS	Basic
36 MBPS	Supported
48 MBPS	Supported
54 MBPS	Supported

Figure 144. Configuring connection limitation per radio

After configuring MAX CLIENT COUNTS, click the **<Apply>** button.

7.10.2 Connection Limitation per WLAN

Configuration using CLI

To configure connection limitation per WLAN, execute the command as follows:

1) Go to configure → wlan configuration mode of CLI.

```
APC# configure terminal
APC/configure# wlan 1
APC/configure/wlan 1#
```

2) Disable the WLAN.

```
APC/configure/wlan 1# no enable
```

3) Configure connection limitation.

```
max-associated-stations [MAX-STATION]
```

Parameter	Description
MAX-STATION	Maximum number of wireless terminals that can be connected (default: 127)

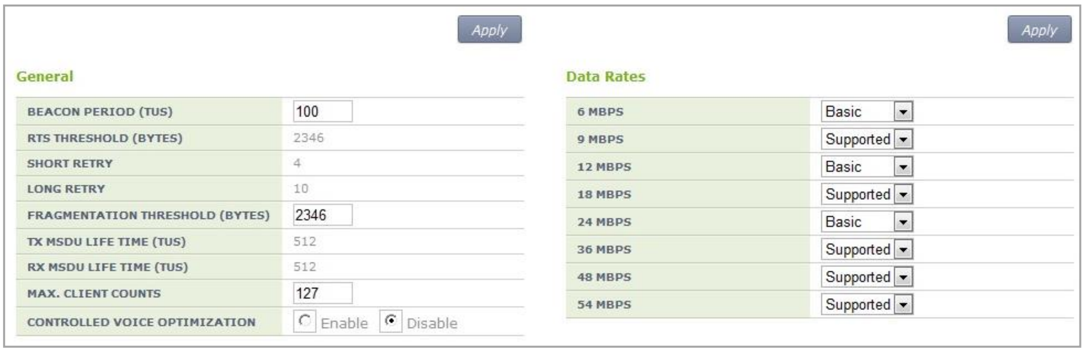
4) Enable the WLAN.

```
APC/configure/wlan 1# enable
```

5) To check the configured connection limitation, use the ‘show wlan detail’ command.

Configuration using Web UI

In the menu bar of **<WEC Main window>**, select **<Configuration>** and then select the **<Radio>** → **<802.11a/n>** or **<802.11b/g/n>** → **<General>** menu in the sub-menus.



General

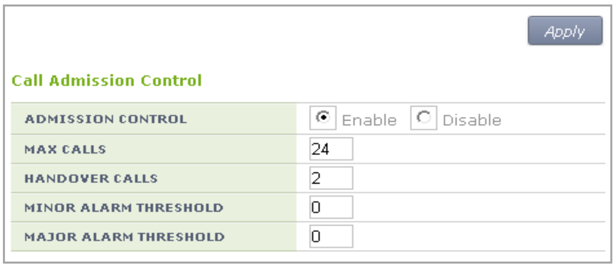
BEACON PERIOD (TUS)	100
RTS THRESHOLD (BYTES)	2346
SHORT RETRY	4
LONG RETRY	10
FRAGMENTATION THRESHOLD (BYTES)	2346
TX MSDU LIFE TIME (TUS)	512
RX MSDU LIFE TIME (TUS)	512
MAX. CLIENT COUNTS	127
CONTROLLED VOICE OPTIMIZATION	○ Enable ● Disable

Data Rates

6 MBPS	Basic
9 MBPS	Supported
12 MBPS	Basic
18 MBPS	Supported
24 MBPS	Basic
36 MBPS	Supported
48 MBPS	Supported
54 MBPS	Supported

Figure 145. Configuring connection limitation per WLAN

After configuring MAXIMUM CONNECTIONS, click the **<Apply>** button.



Call Admission Control

ADMISSION CONTROL	● Enable ○ Disable
MAX CALLS	24
HANDOVER CALLS	2
MINOR ALARM THRESHOLD	0
MAJOR ALARM THRESHOLD	0

7.11 Voice Statistics and Communication Failure Detection

Because APC provides voice statistics and the WLAN-based communication failure detection function, you can easily know communication failure reason.

7.11.1 Voice Statistics Function

It provides the number of successful voice communication and call time.
When the CAC function is enabled, the CAC statistics is also provided.

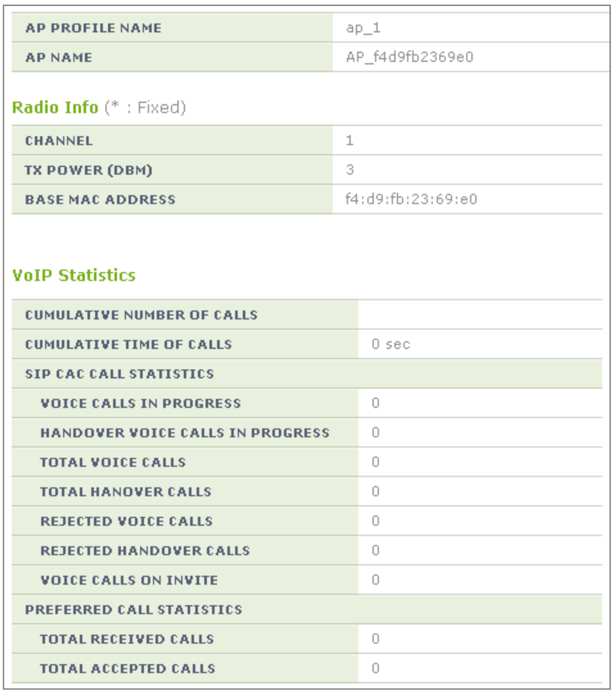
Configuration using CLI

Use the following command to check voice statistics.

```
APC# show 80211bg voip-stats ap 2
 VoIP Stats
  Cumulative Number of Calls ................ 4
  Cumulative Time of Calls .................. 0:0:23
  Number of Active Calls ................... 2
 CAC Stats
  Calls In Progress ........................ 2
  Handover Calls In Progress ............... 0
  Calls Since AP Joined .................... 4
  Handover Calls Since AP Joined ........... 0
  Calls Rejected Since AP Joined ........... 0
  Handover Calls Rejected Since AP Joined ... 0
  Calls On Invite .......................... 0
  Preferred Calls Received ................. 0
  Preferred Calls Accepted ................. 0
```

Configuration using Web UI

In the menu bar of **<WEC Main window>**, select **<Monitor>** and then select the **<Access Points>** → **<Radio>** → **<802.11a/n>** or **<802.11b/g/n>** → AP menu in the sub-menus.



AP PROFILE NAME	ap_1
AP NAME	AP_f4d9fb2369e0

Radio Info (* : Fixed)

CHANNEL	1
TX POWER (DBM)	3
BASE MAC ADDRESS	f4:d9:fb:23:69:e0

VoIP Statistics

CUMULATIVE NUMBER OF CALLS	
CUMULATIVE TIME OF CALLS	0 sec
SIP CAC CALL STATISTICS	
VOICE CALLS IN PROGRESS	0
HANDOVER VOICE CALLS IN PROGRESS	0
TOTAL VOICE CALLS	0
TOTAL HANOVER CALLS	0
REJECTED VOICE CALLS	0
REJECTED HANDOVER CALLS	0
VOICE CALLS ON INVITE	0
PREFERRED CALL STATISTICS	
TOTAL RECEIVED CALLS	0
TOTAL ACCEPTED CALLS	0

Figure 146. Voice statistics

7.11.2 Detecting WLAN-based Communication Failure

You can configure whether to detect WLAN-based communication failure.

Configuration using CLI

1) Go to configure mode of CLI.

```
APC# configure terminal
APC/configure#
```

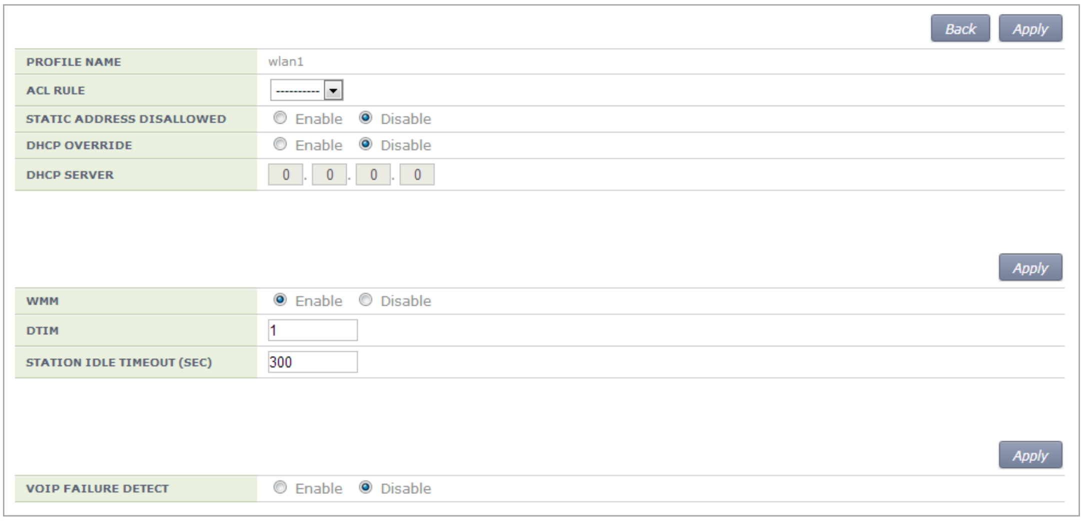
2) Enable or disable communication failure detection.
   - [no] call-fail-detect [WLAN_ID]

Parameter	Description
WLAN_ID	WLAN ID (range: 1-240)

3) To check the configured connection limitation information, use the ‘show voip config [WLAN_ID]’ command.

Configuration using Web UI

In the menu bar of <**WEC Main window**>, select <**Configuration**> and then select the <**WLANs**> menu in the sub-menus. Select a WLAN ID to change in the WLANs screen and go to the <**Advanced**> tab.



PROFILE NAME	wlan1
ACL RULE	----------
STATIC ADDRESS DISALLOWED	○ Enable ● Disable
DHCP OVERRIDE	○ Enable ● Disable
DHCP SERVER	0 . 0 . 0 . 0
WMM	● Enable ○ Disable
DTIM	1
STATION IDLE TIMEOUT (SEC)	300
VOIP FAILURE DETECT	○ Enable ● Disable

Figure 147. Detecting WLAN-based communication failure

After configuring the VOIP FAILURE DETECT item, click the <**Apply**> button.

7.12 Voice Signal and Media Monitoring

For voice call fault analysis, the APC provides VoIP wireless terminal, call information, event and RTP media voice quality statistics.

7.12.1 Checking Voice Related Wireless Information

Configuration using CLI

Execute the following command to check voice related fault analysis statistics.

1) Check the connection status of a voice wireless terminal.

```
WEC8500# show voice station summary
MAC Address       IP Address     Tel-no     AP  BSS               WLAN
Proto  Server IP      Reg         Call
----------------- -------------- --------- --- ----------------- ----
------ ------------- ----------- ----------
50:01:BB:FD:96:E1 10.10.10.5     9922       3    F4:D9:FB:24:C8:C2 1
SIP(UDP)  90.90.1.100  Registered Established
78:47:1D:C2:18:11 10.10.10.10    9907       3    F4:D9:FB:24:C8:D1 1
SIP(UDP)  90.90.1.100  Registered Not calling
WEC8500#
```

2) Check the connection status of an active call.

```
WEC8500# show voice active-call summary
MAC Address       IP Address     Tel-No     AP   BSS              WLAN
Caller      Callee      Dir Status   Dur(sec) Start Time   MOS
----------------- -------------- ---------- --- ---------------- ----
---------- ----------- --- -------- ------ -------- ---
C8:19:F7:70:89:04 10.10.10.65     9961       3    F4:D9:FB:24:C8:C2 1
9907       9961       In  Established 48    05-12 21:16:13 3.95
50:01:BB:FD:96:E1 10.10.10.5      9922       3    F4:D9:FB:24:C8:C2 1
9922       9950       Out Established 336    05-12 21:11:25 3.95
78:47:1D:C2:18:11 10.10.10.10     9907       3    F4:D9:FB:24:C8:D1 1
9907       9961       Out Established 48    05-12 21:16:13 3.77
----------------- -------------- ---------- --- ----------------- ----
---------- ----------- --- -------- ------ -------- ---#
```

3) Check the information of a completed call.

```
WEC8500# show voice complete-call summary
CONN      Start Time      Dur   AP         SSID       MAC Address
Tel-no  IPv4 Address  Port  Rat   MOS LQ/CQ/PQ    Pkt Cnt
==== =================== ==== ==== =============== === ==============
========== =============== ===== ==== ============== ===============
   0 2013/05/11-17:24:23   26    1      uready Caller D4:88:90:1B:3C:E2
10.10.10.194   23143  GOOD 4.01/3.95/3.84       225,664
                                        Callee 3C:8B:FE:2E:6F:6A
10.10.10.193   10617  POOR 2.31/2.17/2.90       221,708
---------------------------------------------------------------------
---------------------------------------------------------------------
   1 2013/05/11-17:25:16   10    1      uready Caller 3C:8B:FE:2E:6F:6A
10.10.10.193   10617  FAIR 3.57/3.11/3.63       90,300
                                        Callee D4:88:90:1B:3C:E2
10.10.10.194   23143  GOOD 4.06/3.91/3.94       85,140
---------------------------------------------------------------------
---------------------------------------------------------------------
   2 2013/05/11-19:02:10   28    1       uready Caller D4:88:90:1B:3C:E2
10.10.10.194   23143  POOR 3.21/2.92/3.44       244,756
                                         Callee 3C:8B:FE:2E:6F:6A
10.10.10.193   10617  POOR 1.97/1.66/2.68       240,800
---------------------------------------------------------------------
---------------------------------------------------------------------
```

4) Check the voice signal related log.

```
WEC8500/configure# show voice sipmsg-log
Time                   MAC Address        Msg Type       Dir
SRC IP       DST IP       AP    BSS              WLAN   Contents
---------------------  ----------------  -------------  -----
-----------  -----------  ----  ----------------  -----  -------------
--------
2013-05-12 21:26:45   c8:19:f7:70:89:04  INVITE         SEND
10.10.10.65  90.90.1.100   3    f4:d9:fb:24:c8:c2  1    F:9922, T:995
0, RTP:10.10.10.65:21120
2013-05-12 21:26:44   c8:19:f7:70:89:04  200(REGISTER)  RECV
90.90.1.100  10.10.10.65   3    f4:d9:fb:24:c8:c2  1    F:9961, T:996
1, Expire:600
2013-05-12 21:26:44   c8:19:f7:70:89:04   REGISTER       SEND
10.10.10.65  90.90.1.100   3    f4:d9:fb:24:c8:c2  1    F:9961, T:996
1, Expire:600
2013-05-12 21:26:44   c8:19:f7:70:89:04   401(REGISTER)   RECV
90.90.1.100  10.10.10.65   3    f4:d9:fb:24:c8:c2  1    F:9961, T:996
1, Expire:0
2013-05-12 21:26:44   c8:19:f7:70:89:04   REGISTER       SEND
10.10.10.65  90.90.1.100   3    f4:d9:fb:24:c8:c2  1    F:9961, T:996
1, Expire:
```

5) Check a WLAN event related to a voice.

```
WEC8500# show voice event
Event Type          MAC Address        AP    BSS               WLAN
Time                 Contents
------------------- ----------------  ---- -----------------  ---
-------------------- ----------------------------
Deassoc During Call 78:47:1D:C2:18:11  3    F4:D9:FB:24:C8:D1 1
2013-05-12 21:22:04  wlan disconncted in AP(3) BSSID(f4:d9:fb:24:c8:d1)
during call caller(9907)          → callee(9950) duration(5)sec
CallStop             C8:19:F7:70:89:04 3    F4:D9:FB:24:C8:C2 1
2013-05-12 21:22:04  caller(9922) → callee(9950) duration(62)sec
CallConnect         78:47:1D:C2:18:11  3    F4:D9:FB:24:C8:D1 1
2013-05-12 21:22:01  caller(9907) → callee(9950)
CallSetup           78:47:1D:C2:18:11  3    F4:D9:FB:24:C8:D1 1
2013-05-12 21:21:59  caller(9907) → callee(9950)
CallStop             78:47:1D:C2:18:11 3    F4:D9:FB:24:C8:D1 1
2013-05-12 21:21:47  caller(9907) → callee(9950) duration(6)sec
CallConnect         78:47:1D:C2:18:11  3    F4:D9:FB:24:C8:D1 1
2013-05-12 21:21:47  caller(9907) → callee(9950)
```

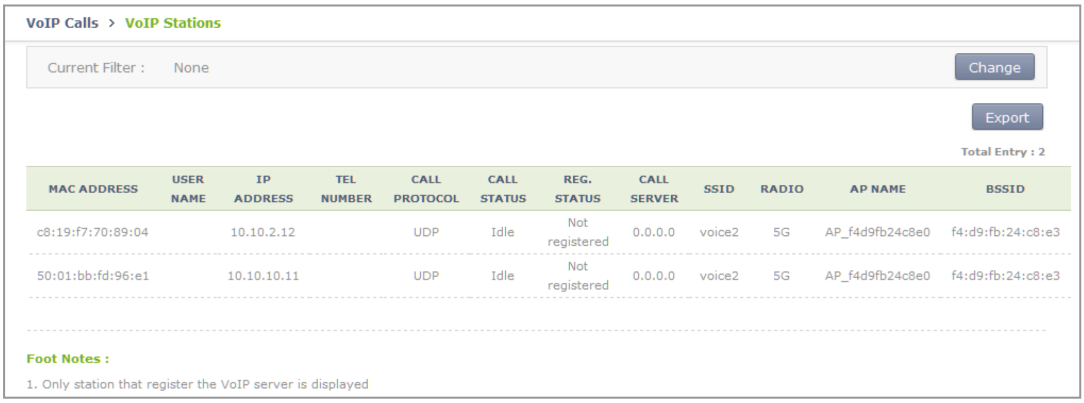
6) Check the voice related statistics.

```
WEC8500# show voice statistics radio

RADIO (5G) Voice Statistis
------ ------ ------- ------ ----- --- ------ ------ --- ------ ------
Type    Total  Success Failed Active    UpstreamTime       Downstream
        Calls  Call     Call   Call   MOS Jitter Delay  MOS Jitter Delay
------ ------ ------- ------ ----- --- ------ ------ --- ------ ------
Total         8      6      0      2 0.0      0      0 0.0      0      0
5 Min         0      0      0      0 0.0      0      0 0.0      0      0
15 Min        0      0      0      0 0.0      0      0 0.0      0      0
1 Hour        0      0      0      0 0.0      0      0 0.0      0      0
1 Day         8      6      0      2 0.0      0      0 0.0      0      0

RADIO (2.4G) Voice Statistis
------ ------ ------- ------ ----- --- ------ ------ --- ------ ------
Type    Total  Success Failed Active    UpstreamTime       Downstream
        Calls  Call     Call   Call   MOS Jitter Delay  MOS Jitter Delay
------ ------ ------ ------ ------ --- ------ ------ --- ------ ------
Total         3      3      0      0 0.0      0      0 0.0      0      0
5 Min         0      0      0      0 0.0      0      0 0.0      0      0
15 Min        0      0      0      0 0.0      0      0 0.0      0      0
1 Hour        0      0      0      0 0.0      0      0 0.0      0      0
1 Day         3      3      0      0 0.0      0      0 0.0      0      0
WEC8500# show voice statistics wlan 1
```

```
WLAN (A_toanyone_1) Voice Statistis
------ ------ ------- ------ ----- --- ------ ------ --- ------ ------
Type    Total  Success Failed Active   UpstreamTime       Downstream
        Calls  Call   Call   Call   MOS Jitter Delay MOS Jitter Delay
------ ------ ----- ------ ------ --- ------ ------ --- ------ ------
Total        11      9      0      2 0.0      0      0 0.0      0      0
5 Min         0      0      0      0 0.0      0      0 0.0      0      0
15 Min        0      0      0      0 0.0      0      0 0.0      0      0
1 Hour        0      0      0      0 0.0      0      0 0.0      0      0
1 Day        11      9      0      2 0.0      0      0 0.0      0      0

WEC8500# show voice statistics device

DEVICE ( Model Name:SHV-E210L, OS Ver:4.1.1 Build Ver:E210LKLJLK1 )
Voice Statistis
---------- ------ ------ ------ ------ --- ------ ------ --- ------ --
----
Type    Total  Success Failed Active   UpstreamTime       Downstream
        Calls  Call   Call   Call   MOS Jitter Delay MOS Jitter Delay
------ ------ ----- ------ ------ --- ------ ------ --- ------ ------
Total         8      6      0      2 0.0      0      0 0.0      0      0
5 Min         0      0      0      0 0.0      0      0 0.0      0      0
15 Min        0      0      0      0 0.0      0      0 0.0      0      0
1 Hour        0      0      0      0 0.0      0      0 0.0      0      0
1 Day         8      6      0      2 0.0      0      0 0.0      0      0
WEC8500#
```

Configuration using Web UI

1) Check the connection status of a voice wireless terminal.
   In the menu bar of **<WEC Main window>**, select **<Monitor>** and then select the **<VoIP Call>** → **<VoIP Stations>** **<Active Calls>** **<Complete Calls>** menu in the sub-menus.



Current Filter : None

Total Entry : 2

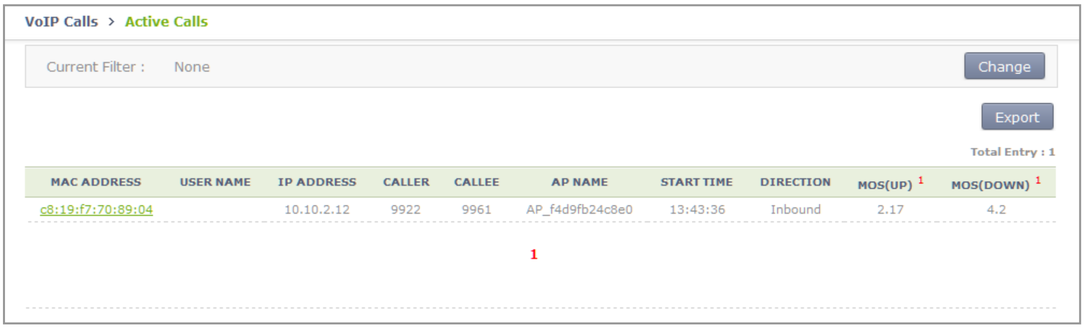
MAC ADDRESS	USER NAME	IP ADDRESS	TEL NUMBER	CALL PROTOCOL	CALL STATUS	REG. STATUS	CALL SERVER	SSID	RADIO	AP NAME	BSSID
c8:19:f7:70:89:04		10.10.2.12		UDP	Idle	Not registered	0.0.0.0	voice2	5G	AP_f4d9fb24c8e0	f4:d9:fb:24:c8:e3
50:01:bb:fd:96:e1		10.10.10.11		UDP	Idle	Not registered	0.0.0.0	voice2	5G	AP_f4d9fb24c8e0	f4:d9:fb:24:c8:e3

Foot Notes :

1. Only station that register the VoIP server is displayed

Figure 148. VoIP Stations Retrieval Screen

2) Check the connection status of an active call.
   In the menu bar of <**WEC Main window**>, select <**Monitor**> and then select the <**VoIP Call**> → <**Active Calls**>menu in the sub-menus.



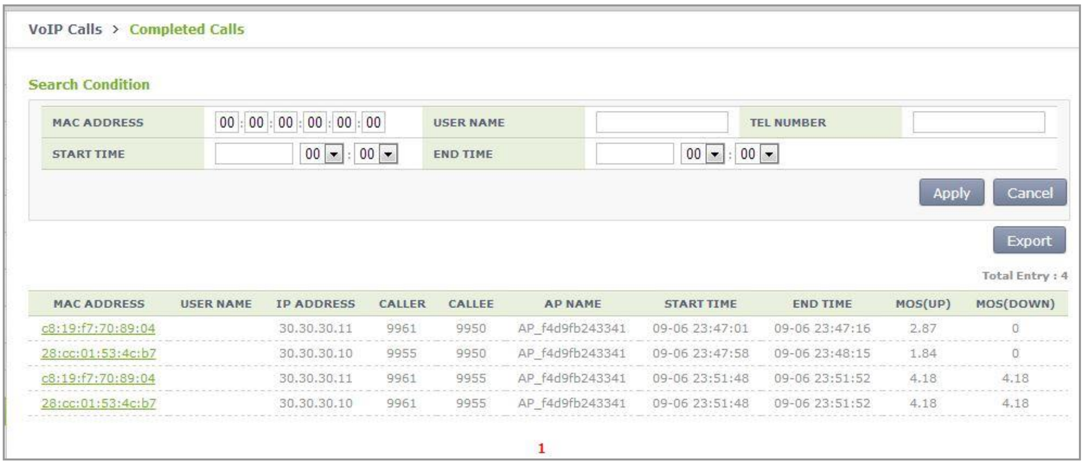
Current Filter : None

Total Entry : 1

MAC ADDRESS	USER NAME	IP ADDRESS	CALLER	CALLEE	AP NAME	START TIME	DIRECTION	MOS(UP) [1]	MOS(DOWN) [1]
c8:19:f7:70:89:04		10.10.2.12	9922	9961	AP_f4d9fb24c8e0	13:43:36	Inbound	2.17	4.2

Figure 149. Active Call Retrieval Screen

3) Check the information of a completed call.
   In the menu bar of <**WEC Main window**>, select <**Monitor**> and then select the <**VoIP Call**> → <**Complete Calls**>menu in the sub-menus.



MAC ADDRESS	00 : 00 : 00 : 00 : 00 : 00	USER NAME	
START TIME	00 : 00	END TIME	00 : 00

TEL NUMBER

Total Entry : 4

MAC ADDRESS	USER NAME	IP ADDRESS	CALLER	CALLEE	AP NAME	START TIME	END TIME	MOS(UP)	MOS(DOWN)
c8:19:f7:70:89:04		30.30.30.11	9961	9950	AP_f4d9fb243341	09-06 23:47:01	09-06 23:47:16	2.87	0
28:cc:01:53:4c:b7		30.30.30.10	9955	9950	AP_f4d9fb243341	09-06 23:47:58	09-06 23:48:15	1.84	0
c8:19:f7:70:89:04		30.30.30.11	9961	9955	AP_f4d9fb243341	09-06 23:51:48	09-06 23:51:52	4.18	4.18
28:cc:01:53:4c:b7		30.30.30.10	9961	9955	AP_f4d9fb243341	09-06 23:51:48	09-06 23:51:52	4.18	4.18

Figure 150. Complete Calls Retrieval Screen

7.12.2 Checking Voice Related Quality Information

Configuration using CLI

Execute the following command to check the voice related quality analysis (Voice Quality Monitoring) information.

1) Operator can check the voice quality analysis information of a wireless terminal that has an active call.

```
WEC8500# show voice vqm current-stats brief
========================================================
[CONN-740 Start Time=2013/7/19.14:47:27, Duration=47 sec(s)
   Call-ID[f03c77b50564418855587192e12b889d <-> ca371fce-6e10-401a-
9a4e-dd53678804c6@ug1.scm.com] Session id :0
   SRC [I/F=ge4 Phone-No=9960, IP=20.20.20.30:22458]
   DST [I/F=ge4 Phone-No=9910, IP=20.20.20.25:25407]
   RTP Flow Quality Metrics:
   [Flow-1] DIR=Forward Quality Ratings=Poor [MOS-LQ=3.06, MOS-
CQ=2.82, MOS-PQ=3.35]
   RTP Flow Quality Metrics:
   [Flow-2] DIR=Reverse Quality Ratings=Good [MOS-LQ=4.04, MOS-
CQ=3.95, MOS-PQ=3.89]

WEC8500#
```

2) Operator can check the voice quality analysis information of a wireless terminal that has a completed call.

```
WEC8500# show voice vqm history-stats brief
========================================================
[CONN-1 Start Time=2013/7/19.14:47:27, Duration=75 sec(s)
Station Mac [78:47:1d:c5:4c:85: ↔fc:a1:3e:47:59:e7:] startBssid
[f4:d9:fb:23:66:10↔f4:d9:fb:23:66:10] endBssid
[f4:d9:fb:23:66:10↔f4:d9:fb:23:66:10]
ssid [Ajay_2_2_4G↔Ajay_2_2_4G]  Direction [1↔2] wlanId [2↔2]
startApId [2↔2]  endApId [2↔2]
Session id :0
SRC [I/F=ge4 Call-ID=f03c77b50564418855587192e12b889d Phone-No=9960,
IP=20.20.20.30:22458]
DST [I/F=ge4 Call-ID=ca371fce-6e10-401a-9a4e-dd53678804c6@ug1.scm.com
Phone-No=9910, IP=20.20.20.25:25407]
RTP Flow Quality Metrics:
[Flow-1] DIR==Forward Quality Ratings=Poor [MOS-LQ=2.21, MOS-CQ=1.33,
MOS-PQ=2.84]
RTP Flow Quality Metrics:
[Flow-2] DIR==Reverse Quality Ratings=Poor [MOS-LQ=2.46, MOS-CQ=1.50,
MOS-PQ=3.00]

========================================================
[CONN-2 Start Time=2013/7/19.14:52:36, Duration=30 sec(s)
Station Mac [fc:a1:3e:47:59:e7: ↔78:47:1d:c5:4c:85:] startBssid
[f4:d9:fb:23:66:10↔f4:d9:fb:23:66:10] endBssid
[f4:d9:fb:23:66:10↔f4:d9:fb:23:66:10]
```

```
ssid [Ajay_2_2_4G↔Ajay_2_2_4G]  Direction [1↔2] wlanId [2↔2]
startApId [2↔2]  endApId [2↔2]
Session id :1
SRC [I/F=ge4 Call-ID=035be38a40032eb8edb0b94e944d58d4 Phone-No=9910,
IP=20.20.20.25:25407]
DST [I/F=ge4 Call-ID=917a913e-83ae-497f-ad84-bf0ee80edf36@ug1.scm.com
Phone-No=9960, IP=20.20.20.30:22458]
RTP Flow Quality Metrics:
[Flow-1] DIR==Forward Quality Ratings=Fair [MOS-LQ=3.73, MOS-CQ=3.65,
MOS-PQ=3.72]
RTP Flow Quality Metrics:
[Flow-2] DIR==Reverse Quality Ratings=Poor [MOS-LQ=3.30, MOS-CQ=3.06,
MOS-PQ=3.49]

========================================================
[CONN-3 Start Time=2013/7/19.14:53:12, Duration=24 sec(s)
Station Mac [78:47:1d:c5:4c:85: ↔fc:a1:3e:47:59:e7:] startBssid
[f4:d9:fb:23:66:10↔f4:d9:fb:23:66:10] endBssid
[f4:d9:fb:23:66:10↔f4:d9:fb:23:66:10]
ssid [Ajay_2_2_4G↔Ajay_2_2_4G]  Direction [1↔2] wlanId [2↔2]
startApId [2↔2]  endApId [2↔2]
Session id :2
SRC [I/F=ge4 Call-ID=a47241e5f5d3d6b7f942d0aaeddbd8ef Phone-No=9960,
IP=20.20.20.30:22458]
DST [I/F=ge4 Call-ID=65031276-a4dd-4b1c-a718-4ed3188e44a5@ug1.scm.com
Phone-No=9910, IP=20.20.20.25:25407]
RTP Flow Quality Metrics:
[Flow-1] DIR==Forward Quality Ratings=Poor [MOS-LQ=3.25, MOS-CQ=2.96,
MOS-PQ=3.47]
RTP Flow Quality Metrics:
[Flow-2] DIR==Reverse Quality Ratings=Fair [MOS-LQ=3.65, MOS-CQ=3.57,
MOS-PQ=3.68]

WEC8500#
```

3) Operator can check the call statistics information.

```
WEC8500# show voice vqm summary-stats
========================================================
VQM Summary Stats for last YEAR:0 MONTH:0 DAY:0 0 HR:26 MN:44 SEC
Calls Active      = 0
Calls Terminated  = 3
Flows Quality Summary (Total/Good/Fair/Poor) = 6/0/2/4
Listening Call Quality (MOS)  min/ave/max = 2.21/3.10/3.73
Conversational Call Quality (MOS)  min/ave/max = 1.33/2.68/3.65
P.862 Raw Quality (MOS)  min/ave/max = 2.84/3.36/3.72
Listening Call Quality (R-factor)  min/ave/max = 45/63/77
Conversational Call Quality (R-factor)  min/ave/max = 24/53/75
Packet Delay Variation (msec) ave/max = 13/25
Packet Received/Processed/Lost/Discarded = 12980/12909/93/1154
Packet Duplicate/OutOfseq = 0/135
Packet Error Stats: Ignored/Errors = 71/1
System Error Stats: Resource Unavail/Filter Mismatch/Limit Exceeded =
0/0/0
Voice Quality Alerts: Low R-factor/Excess Loss/Excess Delay/Upload  =
1/6/5/0
```

```
Upload Count       =  1141
Upload Ok Count    =  0
Upload Fail Count  = 0
Requested Count    = 1141

WEC8500#
```

4) Operator can check the alarm information that occurs during call.

```
WEC8500# show voice vqm alarms brief
========================================================
VQM ActiveRfactor/ActivePktLoss/ActivePktDly/ActiveMos = 1/1/1/1
VQM QualityThresh/LossThresh/DelayThresh/MOSThresh = 50/50/195/35
 ALARMS REPORTED :
 Src Call Id = f03c77b50564418855587192e12b889d  Dst Call Id =
ca371fce-6e10-401a-9a4e-dd53678804c6@ug1.scm.com  Session = 0
 Direction  :Forward  Type : [Low-Quality]      [Excessive Burst]
[Excessive delay]
 Direction  :Reverse  Type : [Excessive Burst]  [Excessive delay]
 ALARMS REPORTED :
 Src Call Id = 035be38a40032eb8edb0b94e944d58d4  Dst Call Id =
917a913e-83ae-497f-ad84-bf0ee80edf36@ug1.scm.com  Session = 1
 Direction  :Forward  Type : [Excessive Burst]
 Direction  :Reverse  Type : [Excessive Burst]  [Excessive delay]
 ALARMS REPORTED :
 Src Call Id = a47241e5f5d3d6b7f942d0aaeddbd8ef  Dst Call Id =
65031276-a4dd-4b1c-a718-4ed3188e44a5@ug1.scm.com  Session = 2
 Direction  :Forward  Type : [Excessive Burst]
 Direction  :Reverse  Type : [Excessive Burst]

WEC8500#
```

7.13 Multicast Stream Admission Control

The multicast stream admission control is provided to protect the currently running multicast streams from new streams that flow into the wireless LAN. When the maximum allowed usage of streams or channels per radio is reached, the APC does not allow any additional streams.

7.13.1 Configuring Admission Control

The multicast stream admission control function configures the maximum number of streams or the maximum usage of channels to protect the currently running multicast streams. It denies multicast streaming requests once the maximum number of streams or the maximum usage of channels is reached. You can set the number of marginal streams or the usage of channels with consideration for handover.

Configuration using CLI

To set multicast stream admission control, execute the following commands:

1) Configuration mode of CLI→ enter the multicast stream admission control mode of the desired wireless section.

```
APC# configure terminal
APC/configure# [80211a/80211bg] msac
APC/configure/80211a/msac#
```

2) Enable or disable the multicast stream admission control function.

- acm [MODE]

Parameter	Description
Mode	Whether or not to use the multicast stream admission control (enable/disable) - enable: Enable - disable: Disable

3) Configure the maximum allowed number of streams.

- max-streams [VALUE]

Parameter	Description
VALUE	Maximum allowed number of streams

4) Set the maximum allowed usage of channels.

- max-chan-util [VALUE]

Parameter	Description
VALUE	Maximum allowed usage of channels

5) Configure the number of marginal streams with consideration for handover.

- reserved-ho-streams [VALUE]

Parameter	Description
VALUE	Number of marginal streams with consideration for handover

6) Configure the usage of marginal channels with consideration for handover.

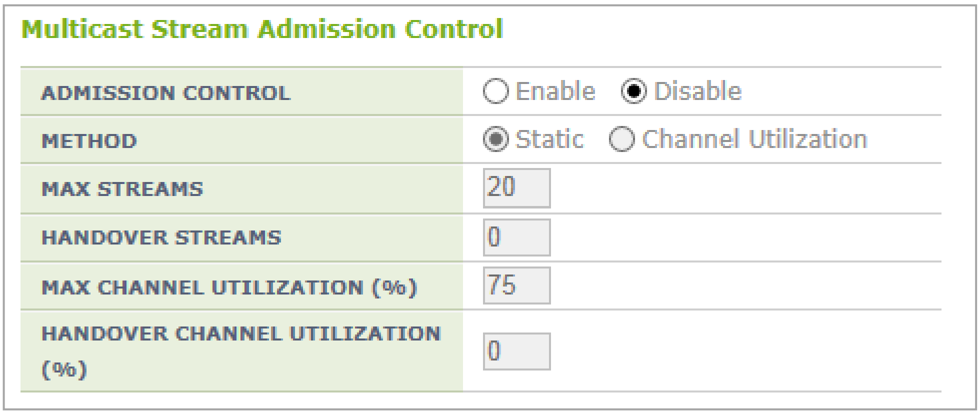
- reserved-ho-chan-util [VALUE]

Parameter	Description
VALUE	Usage of marginal channels with consideration for handover

7) You can view the information you configured by using the ‘show[80211a | 80211bg] msac configuration’ command.

Configuration using Web UI

From the menu bar of **<WEC Main Window>,** select **<Configuration>** and then select **<Radio>** → **<802.11a/n>** or **<802.11b/g/n>** → **<Admission Control>** in the submenus.



Multicast Stream Admission Control

ADMISSION CONTROL	○ Enable ● Disable
METHOD	● Static ○ Channel Utilization
MAX STREAMS	20
HANDOVER STREAMS	0
MAX CHANNEL UTILIZATION (%)	75
HANDOVER CHANNEL UTILIZATION (%)	0

Figure 151. 802.11a/n Admission Control Configuration Window

After configuring the items below in the Multicast Stream Admission Control, click the <**Apply**> button.

- ADMISSION CONTROL: Configure the CAC function
- METHOD: Select the method of admission control
- MAX STREAMS: Maximum allowed number of streams (range: 1-20)
- HANDOVER STREAMS: Number of marginal streams with consideration for handover (range: 0-6)
  The maximum allowed number of streams becomes MAX STREAMS-HANDOVER STREAMS.
- MAX CHANNEL UTILIZATION (%): Maximum allowed usage of channels (range: 5-85)
- HANDOVER CHANNEL UTILIZATION (%): Usage of marginal channels with consideration for handover (range: 0-30)

CHAPTER 8. Security

The W-EP wireless LAN system supports the security function, required in a wire/wireless network environment, such as RADIUS server interoperation function, system user management, guest connection service, unauthorized AP/terminal detection and simple blocking function, firewall, access control (ACL), etc.
In this chapter, how to configure various security functions supported in the system is described.

8.1 RADIUS Server Configuration

The W-EP wireless LAN system provides the security and authentication function by interoperating with an external RADIUS server. The WEC8050 also provides the internal RADIUS server function.

8.1.1 External RADIUS Server

The W-EP wireless LAN system provides the security and authentication function by interoperating with an external RADIUS server. Follow the below procedure to interoperate with a RADIUS server.

8.1.1.1 Basic Settings

The basic steps for configuring a RADIUS server are as follows:

Configuration using CLI

1) Go to configure → security → radius configuration mode of CLI.

```
WEC8500# configure terminal
WEC8500/configure# security
WEC8500/configure/wlan 1/security# radius 1
WEC8500/configure/security/radius 1#
```

2) Configure the IP address of a RADIUS server.

```
WEC8500/configure/security/radius 1# serverIp [IP_ADDRESS]
```

Parameter	Description
IP_ADDRESS	The IP address of a RADIUS server

3) Configure the key of a RADIUS server.

```
WEC8500/configure/security/radius 1# secret [KEY_TYPE] [KEY_STRING]
```

Parameter	Description
KEY_TYPE	RADIUS server key input format - ASCII: ASCII character string - HEX: Hexadecimal value
KEY_STRING	RADIUS server key

4) Enable the accounting function of a RADIUS server and configure the port number.

```
WEC8500/configure/security/radius 1# acct [PORT_NUMBER]
```

Parameter	Description
PORT_NUMBER	Accounting port number of a RADIUS server (range: 1-65535, default: 1813)

5) Configure the authentication port number of a RADIUS server.

```
WEC8500/configure/security/radius 1# auth [PORT_NUMBER]
```

Parameter	Description
PORT_NUMBER	Accounting port number of a RADIUS server (range: 1-65535, default: 1812)

6) Configure the items related to retransmissions in RADIUS communications. You can use default values without changing configuration.

```
WEC8500/configure/security/radius 1# retransmit-interval
[RETRY_INTERVAL]
WEC8500/configure/security/radius 1# retransmit-count [RETRY_COUNT]
```

```
WEC8500/configure/security/radius 1# fo-retransmit-count
[FO_RETRY_COUNT]
```

Parameter	Description
RETRY_INTERVAL	Retransmission interval for a RADIUS message (unit: seconds, range: 1-60, default value: 2)
RETRY_COUNT	Maximum retransmission count of a RADIUS message (range: 1-20, default value: 10)
FO_RETRY_COUNT	Maximum retransmission count of a RADIUS message before a RADIUS server failover is attempted Must smaller than the RETRY_COUNT value (range: 1-10, default value: 3)

7) Exit RADIUS server configuration and security configuration mode.

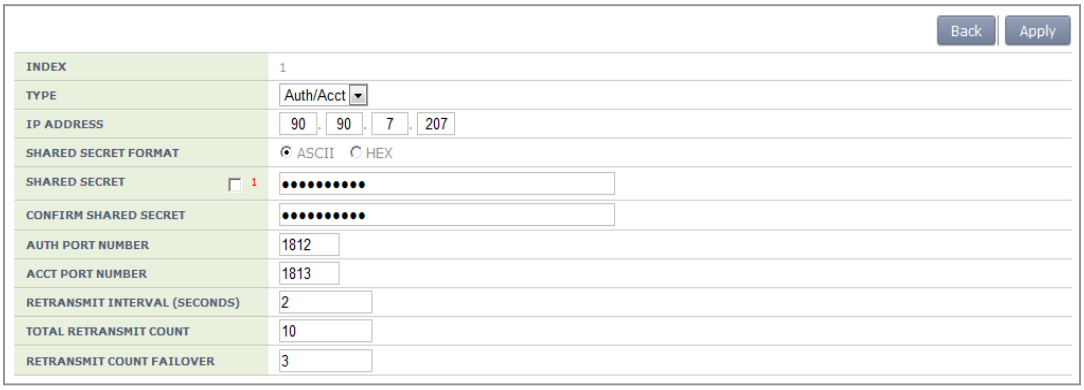
```
WEC8500/configure/security/radius 1# exit
WEC8500/configure/security# exit
```

8) To check the configuration information, use the ‘show security radius-server summary’ command.

Configuration using Web UI

In the menu bar of <**WEC Main window**>, select <**Configuration**> and then select the <**Security**> → <**AAA**> → <**RADIUS**> menu in the sub-menus.

If you click the <**Add**> button in the RADIUS initial window, you can add a RADIUS server.
The server addition window is shown below.



INDEX	1
TYPE	Auth/Acct
IP ADDRESS	90 . 90 . 7 . 207
SHARED SECRET FORMAT	● ASCII ○ HEX
SHARED SECRET □ 1	••••••••••
CONFIRM SHARED SECRET	••••••••••
AUTH PORT NUMBER	1812
ACCT PORT NUMBER	1813
RETRANSMIT INTERVAL (SECONDS)	2
TOTAL RETRANSMIT COUNT	10
RETRANSMIT COUNT FAILOVER	3

Figure 152. RADIUS server configuration

Item	Description
INDEX	ID that distinguishes RADIUS server configurations
TYPE	Selects the type of the RADIUS server - Auth: Performs authentication - Acct: Performs accounting - Auth/Acct: Performs authentication and accounting
IP ADDRESS	IP address of the RADIUS server
SHARED SECRET FORMAT	Key input format for communications with the RADIUS server - ASCII: ASCII strings - HEX: Hexadecimal values
SHARED SECRET	Key for RADIUS server communications
CONFIRM SHARED SECRET	Re-enters the key for RADIUS server communications for confirmation
AUTH PORT NUMBER	Number of the communication port for RADIUS server authentication (range: 1-65,535, default value: 1,812)
ACCT PORT NUMBER	Number of the communication port for RADIUS server accounting (range: 1-65,535, default value: 1,813)
RETRANSMIT INTERVAL	Retransmission interval for a RADIUS message (range: 1-60, default value: 2, unit: seconds)
TOTAL RETRANSMIT COUNT	Maximum retransmission count of a RADIUS message (range: 1-20, default value: 10)
RETRANSMIT COUNT FAILOVER	Maximum retransmission count of a RADIUS message before a RADIUS server failover is attempted (range: 1-10, default value: 3, must be smaller than the TOTAL RETRANSMIT value)

8.1.1.2 Configuring MAC Authentication

The MAC authentication of a RADIUS server is configured as follows:

Configuration using CLI

1) Go to configure → security → radius configuration mode of CLI.

```
WEC8500# configure terminal
WEC8500/configure# security
WEC8500/configure/wlan 1/security# radius 1
WEC8500/configure/security/radius 1#
```

2) Set the password type that will be used for the MAC authentication of the device.

```
WEC8500/configure/security/radius 1# mac-auth-pw-type [PW_TYPE]
```

Parameter	Description
PW_TYPE	Password type (default value: mac) - mac: MAC address of the device. Note: it must be a string whose type must be the same as that of the MAC string which is used as a user ID when the MAC authentication of the device is performed - shared-secret: Key shared between the APC and RADIUS server

3) Set the type of separator of the device's MAC string which is used as a user ID when the MAC authentication of the device is performed.

```
WEC8500/configure/security/radius 1# mac-auth-delimiter
[DELIMITER_TYPE]
```

Parameter	Description
DELIMITER_TYPE	Type of the MAC string separator (default: none) - none: no separator (xxxxxxxxxxxx) - colon: Uses ':' as a separator (xx:xx:xx:xx:xx:xx) - hyphen: Uses '-' as a separator (xx-xx-xx-xx-xx-xx) - single-hyphen: Uses only one '-' in the middle (xxxxxx-xxxxxx)

4) Configure whether to use lowercase characters or uppercase characters for the device's MAC string that will be used as an ID upon the MAC authentication of the device.

```
WEC8500/configure/security/radius 1# mac-auth-case [CASE_TYPE]
```

Parameter	Description
CASE_TYPE	Case type of the device's MAC string (default value: lower) - lower: Uses lowercase - upper: Uses uppercase

5) Exit RADIUS server configuration and then security configuration mode.

```
WEC8500/configure/security/radius 1# exit
WEC8500/configure/security# exit
```

6) You can view configuration information by using the 'show security radius-server detail <server-id>' command.

8.1.2 Internal RADIUS Server

The W-EP wireless LAN system provides the security and authentication function by interoperating with an internal RADIUS server.

To use the internal RADIUS server, operator can add, delete, or edit a user (WEC8500: maximum 2048 users, WEC8050: maximum 512 users).

Configuration using CLI

To configure a local network user related function, enter into the ‘radiuscm’ of configure mode by executing the following command.

```
WEC8050# configure terminal
WEC8050/configure# radiuscm
```

Operator can execute various commands for Local Net Users.

[Adding User]

To add a user to the Local Net Users, execute the following command.

- Add-local-userdb {username} {password} [name] [email] [department] [home_phone] [work_phone] [mobile_phone]

Parameter	Description
Username	Login ID of a user - Character varying (1-63) - MANDATORY - Korean is not allowed. - Special characters {, }, (,), ,, ;, +=, -=,:=, =, !=, >=, >, <=, <, = - , ! - , =*, !*, ==, #, “”, “, ``, *, ?, \, space, & Cannot be used.
Password	User’s password - Character varying (1-63) - MANDATORY - Korean is not allowed. - Special characters {, }, (,), ,, ;, +=, -=,:=, =, !=, >=, >, <=, <, = - , ! - , =*, !*, ==, #, “”, “, ``, *, ?, \, space, & Cannot be used.
Name	Name - Character varying (1-63) - OPTIONAL - Korean is not allowed. - Special characters ‘, *, ?, \, ; cannot be used.
email	email address - Character varying (1-63) - OPTIONAL

Parameter	Description
	- Korean is not allowed. - Special characters ‘, *, ?, \, ; cannot be used.
department	Division information - Character varying (1-63) - OPTIONAL - Korean is not allowed. - Special characters ‘, *, ?, \, ; cannot be used.
Home_phone	Home phone number - Character varying (1-63) - OPTIONAL - Korean is not allowed. - Special characters ‘, *, ?, \, ; cannot be used.
Work_phone	Office phone number - Character varying (1-63) - OPTIONAL - Korean is not allowed. - Special characters ‘, *, ?, \, ; cannot be used.
Mobile_phone	Mobile phone number. - Character varying (1-63) - OPTIONAL - Korean is not allowed. - Special characters ‘, *, ?, \, ; cannot be used.

[Modifying User]

To modify a user from the Local Net Users, execute the following command.

- modify-local-userdb {username} {password} [name] [email] [department] [home_phone] [work_phone] [mobile_phone]

[Deleting User]

To delete one user from the Local Net Users, execute the following command.

- delete-local-userdb {username}

Parameter	Description
Username	User’s ID - Character varying (1-63) - MANDATORY - Korean is not allowed. - Special characters {, }, (,), ,, ;, +=, -=,:=, =, !=, >=, >, <=, <, = - , ! - , =*, !*, ==, #, “”, “, ``, *, ?, \, space, & Cannot be used.

To delete all the users from the Local Net Users, execute the following command.

- Remove-all-local-userdb

[Importing User]

To import the Local Net Users list file, execute the following command.

- Import-local-userdb {filename}

Parameter	Description
Filename	File to import - CSV file format - Filename (1-512)

[Exporting User]

To export the Local Net Users list file, execute the following command.

- Export-local-userdb {filename}

Parameter	Description
Filename	File to export - CSV file format - Filename (1-512)

[Checking User]

To check one local net user, execute the following command.

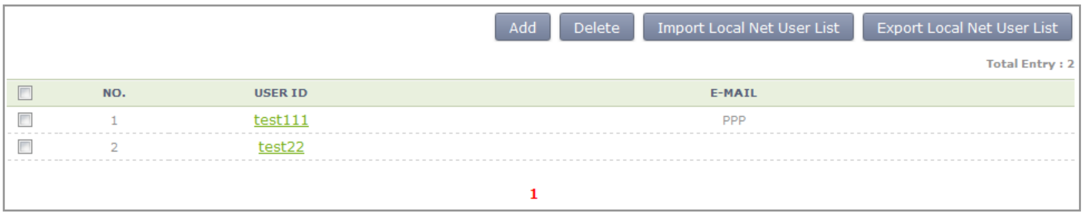
- Show radiuscm username {username}

To check all the local net users, execute the following command.

- Show radiuscm all-user

Configuration using Web UI

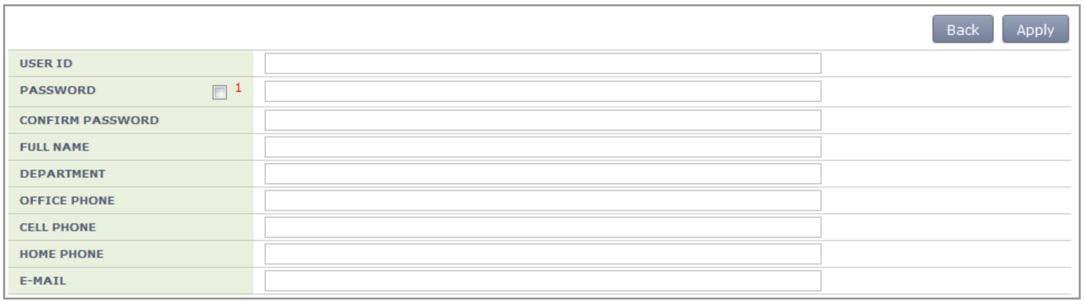
In the menu bar of **<WEC Main window>**, select **<Configuration>** and then select the **<Security>** → **<AAA>** → **<Local User>** menu in the sub-menus.



Total Entry : 2

□	NO.	USER ID	E-MAIL
□	1	test111	PPP
□	2	test22	

To add a user, click the <**Add**> button.



1) Enter an item according to each parameter description, and click the <**Apply**> button.
   - ID: ID of a user to add
   - PASSWORD: User’s initial password
   - CONFIRM PASSWORD: Repeat Password
   - FULL NAME: User’s name (option)
   - DEPARTMENT: User’s department information (option)
   - OFFICE PHONE: Office phone number (option)
   - CELL PHONE: Mobile phone number (option)
   - HOME PHONE: Home phone number (option)
   - E-MAIL: email (option)

2) Importing a local net user list
   Operator can import or export the list of local users. The user list is in the CSV format. An existing data is deleted if there is new importing.

3) Exporting a local net user list
   Operator can export the list of local users in the CSV format file.

8.2 Unauthorized AP/Terminal Detection and Blocking

As the security function, the W-EP wireless LAN device provides the detection service for an unauthorized AP using the Wireless Intrusion Detection System (WIDS)/WES function. This function detects any AP that is illegally installed without an administrator’s approval and also any wireless terminals connected to the AP. If an authorized wireless terminal is connected to an unauthorized AP, some information may be exposed or the wireless LAN may be attacked in some ways. Therefore, it is important to manage the risk.

8.2.1 Enabling Detection Function

The procedure of enabling the unauthorized AP and terminal detection function is shown below.

Configuration using CLI

1) Go to configure mode of CLI.

```
WEC8500# configure terminal
```

2) Enable the detection function.

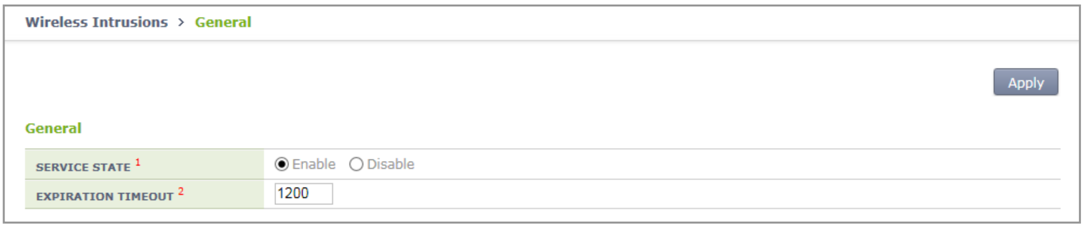
```
WEC8500/configure# wi enable
```

3) To check the configured information, use the following command.

- show wi current-config

Configuration using Web UI

In the menu bar of **<WEC Main window>**, select **<Configuration>** and then select the **<Wireless Intrusion>** → **<General>** menu in the sub-menus.



General

SERVICE STATE [1]	● Enable ○ Disable
EXPIRATION TIMEOUT [2]	1200

Click Apply after selecting Enable or Disable, then operator can configure the Wireless Intrusion service status.

Figure 153. Wireless Intrusion General Configuration Window

Detection

The W-EP wireless LAN system detects all the packets in a wireless LAN network, classifies unauthorized APs and wireless terminals, and creates related alarms and logs. The detected unauthorized APs are classified as follows according to the configured classification policy.

Classification type	Description
Managed AP	AP that is allowed to be used by an administrator among the detected unauthorized APs - Configures the managed AP classification policy. - An administrator can classify a specific AP as a managed AP among the manually detected unauthorized APs.
Unmanaged AP	AP that is not allowed to be used by an administrator among the detected unauthorized APs and AP that can be used maliciously - Configures the unmanaged AP classification policy. - An administrator can classify a specific AP as a unmanaged AP among the manually detected unauthorized APs.

8.2.1.1 Configuring the managed AP classification policy

To configure the managed type authorized AP classification policy, execute the command as follows:

Configuration using CLI

1) Go to configure → wi → device configuration mode of CLI.

```
WEC8500# configure terminal
WEC8500/configure# wi
WEC8500/configure/wi# device
WEC8500/configure/wi/device#
```

2) Configure the managed type authorized AP policy.
   - add-classification-rule- managed [RULE_NAME] enable [PRIORITY] [SSID_TYPE] [SSID]

Parameter	Description
RULE_NAME	Classification policy name
PRIORITY	Priority number
SSID_TYPE	SSID type - managed-ssid: SSID that is used in an authorized AP that is connected to the APC. - user-configured-ssid [SSID]: Entered SSID (An AP that has SSID as SSID_NAME is classified as a friendly type unauthorized AP.)

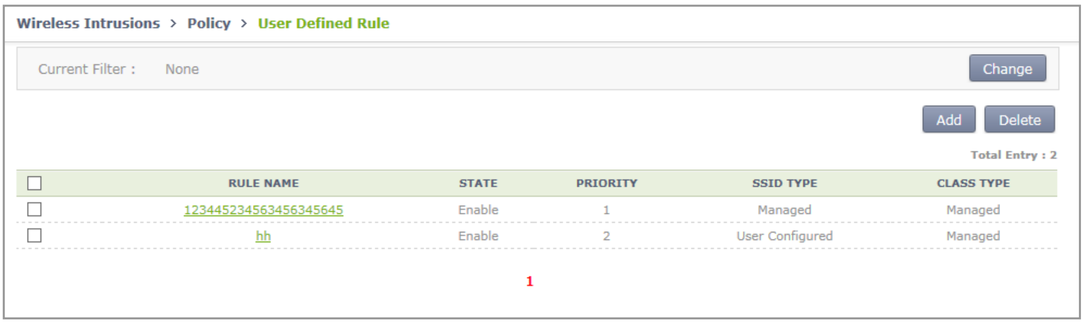
Parameter	Description
SSID_NAME	SSID that is used when the SSID_TYPE is entered as user-configured-ssid

3) To check the configured information, use the ‘show wids device rule managed’ command.

Configuration using Web UI

In the menu bar of <**WEC Main window**>, select <**Configuration**> and then select the <**Wireless Intrusion**> → <**Policy**> → <**User Defined Rule**> menu in the sub-menus. And then, select <**Managed**> at the upper tab.

1) By using Add, Delete, or Change, operator can add, delete, or change user defined rules.



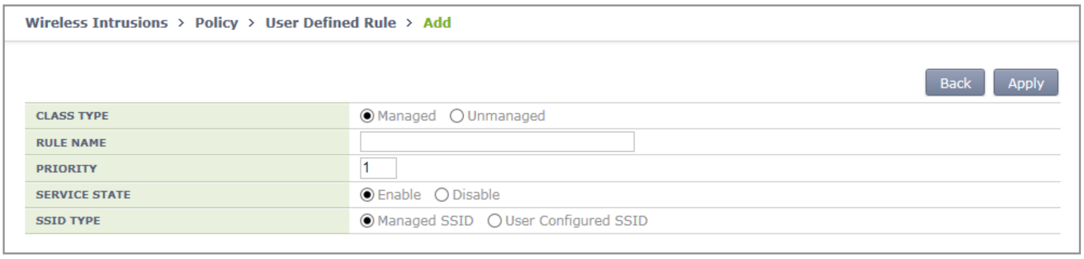
Current Filter : None

Total Entry : 2

□	RULE NAME	STATE	PRIORITY	SSID TYPE	CLASS TYPE
□	123445234563456345645	Enable	1	Managed	Managed
□	hh	Enable	2	User Configured	Managed

Figure 154. Managed Rule Configuration Window

2) In the rule addition screen, operator can add a rule by entering the information and click Apply.



CLASS TYPE	● Managed ○ Unmanaged
RULE NAME	
PRIORITY	1
SERVICE STATE	● Enable ○ Disable
SSID TYPE	● Managed SSID ○ User Configured SSID

Figure 155. Managed Addition Window

8.2.1.2 Configuring the unmanaged AP classification policy

To configure the unmanaged type unauthorized AP classification policy, execute the command as follows:

Configuration using CLI

1) Go to configure → wi → device configuration mode of CLI.

```
WEC8500# configure terminal
WEC8500/configure# wi
WEC8500/configure/wi# device
WEC8500/configure/wi/device#
```

2) Configure the unmanaged type unauthorized AP policy.

   - add-classification-rule-unmanaged [RULE_NAME] enable [PRIORITY] [MATCH_TYPE] [MIN_RSSI] [MIN_DURATION] [NO_OF_MIN_ASSOC CLIENTS] [ENCRYPTION] [SSID_TYPE] [SSID]

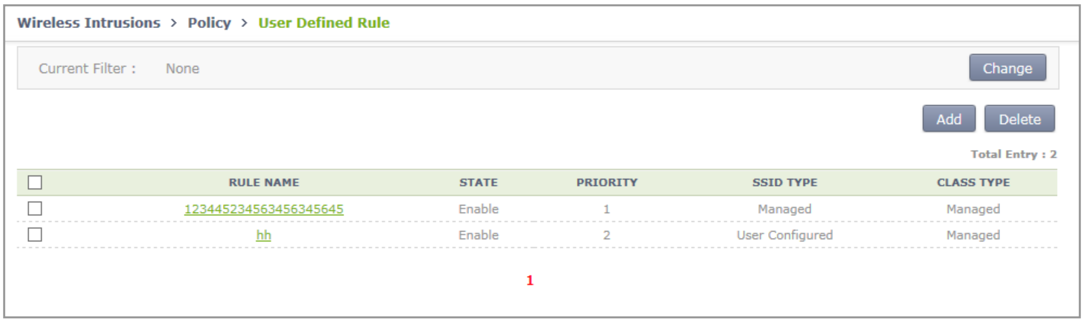
Parameter	Description
RULE_NAME	Classification policy name
PRIORITY	Rule priority number
MATCH_TYPE	Enter either match-all or match-any. - match-all: Classifies as a unmanaged unauthorized AP when the detection criteria entered thereafter are all satisfied. - match-any: Classifies as a unmanaged unauthorized AP when any one of the detection criteria entered thereafter is satisfied.
MIN_RSSI	Minimum RSSI. When the RSSI value is higher than this value, it is classified as a unmanaged unauthorized AP.
MIN_DURATION	Minimum lasting time (unit: s). When the signal lasting time is higher than this value, it is classified as a unmanaged unauthorized AP.
NO_OF_MIN_ASSOCCLIENTS	Minimum number of connected terminals When the number of connected terminals is higher than this value, it is classified as a unmanaged unauthorized AP.
ENCRYPTION	Whether to use encryption - 0: Does not use encryption. If encryption is not used, it is classified as a unmanaged unauthorized AP. - 1: Uses encryption. If encryption is used, it is classified as a malicious unauthorized AP.
SSID TYPE	SSID type - managed-ssid: SSID that is used in an authorized AP that is connected to the APC. - user-configured-ssid [SSID]: Entered SSID (An AP that has SSID as SSID_NAME is classified as a friendly type unauthorized AP.)
SSID_ NAME	SSID that is used when the SSID_TYPE is entered as user-configured-ssid

3) To check the configured information, use the ‘show wids device rule unmanaged’ command.

Configuration using Web UI

In the menu bar of **<WEC Main window>**, select **<Configuration>** and then select the **<Wireless Intrusion>** → **<Policy>** → **<User Defined Rule>** menu in the sub-menus. And then, select **<Unmanaged>** at the upper tab.

1) By using Add, Delete, or Change, operator can add, delete, or change user defined rules.



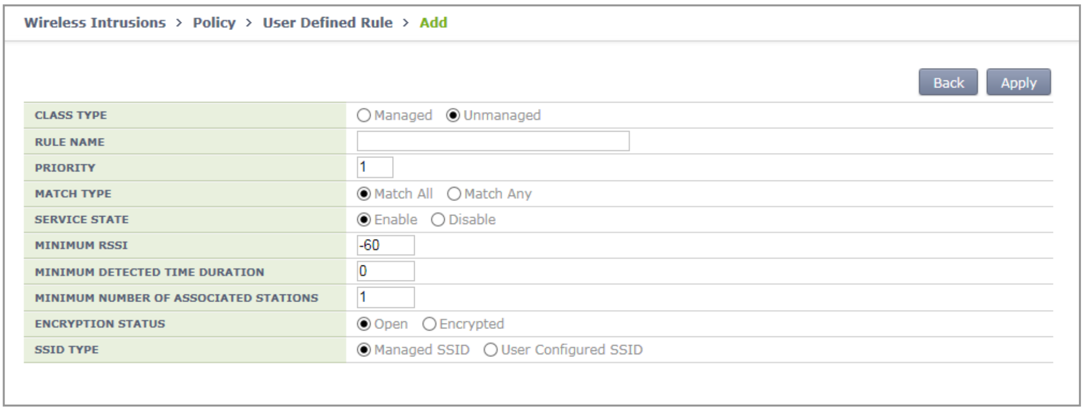
Current Filter : None

Total Entry : 2

□	RULE NAME	STATE	PRIORITY	SSID TYPE	CLASS TYPE
□	12344523456345645645	Enable	1	Managed	Managed
□	hh	Enable	2	User Configured	Managed

Figure 156. Unmanaged Rule Configuration Window

2) In the rule addition screen, operator can add a rule by entering the information and click Apply.



CLASS TYPE	○ Managed ● Unmanaged
RULE NAME	
PRIORITY	1
MATCH TYPE	● Match All ○ Match Any
SERVICE STATE	● Enable ○ Disable
MINIMUM RSSI	-60
MINIMUM DETECTED TIME DURATION	0
MINIMUM NUMBER OF ASSOCIATED STATIONS	1
ENCRYPTION STATUS	● Open ○ Encrypted
SSID TYPE	● Managed SSID ○ User Configured SSID

Figure 157. Unmanaged Rule Addition Window

8.2.1.3 Manual configuration (Move)

A user can change the classification of an unauthorized AP that is detected by the WI or that is classified according to the rule configured by a user.

Configuration using CLI

1) Go to configure → wi → device configuration mode of CLI.

```
WEC8500# configure terminal
WEC8500/configure# wi
WEC8500/configure/wi# device
WEC8500/configure/wi/device#
```

By using the MAC of an unauthorized AP to change, execute the move command.

- move [MAC] [FROM] [TO]

Parameter	Description
MAC	MAC address of a detected AP
FROM	Previous classification of a MAC
TO	Classification to change

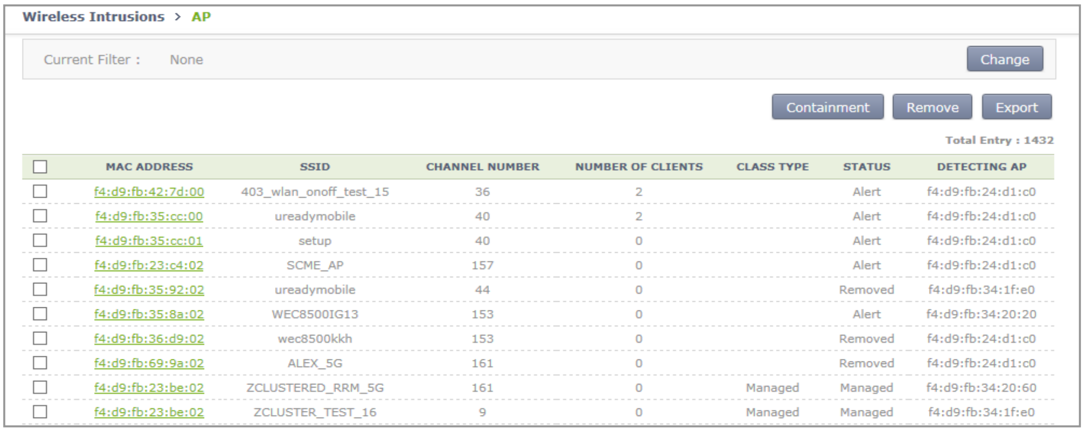
2) To check the changed configuration, use the following command.

- show wi device ap list managed
- show wi device ap list unmanaged

Configuration using Web UI

In the menu bar of <**WEC Main window**>, select <**Monitor**> and then select the <**Wireless Intrusion**> → <**AP**> menu in the sub-menus. And when the AP list is displayed, select one out of the AP list to go to the detail view screen. In the detail view screen, operator can manually change the classification of an AP by using the top down menu of MOVE CLASSIFICATION MANUALLY.

1) In the AP list screen, go to the detail view screen by clicking a MAC address.



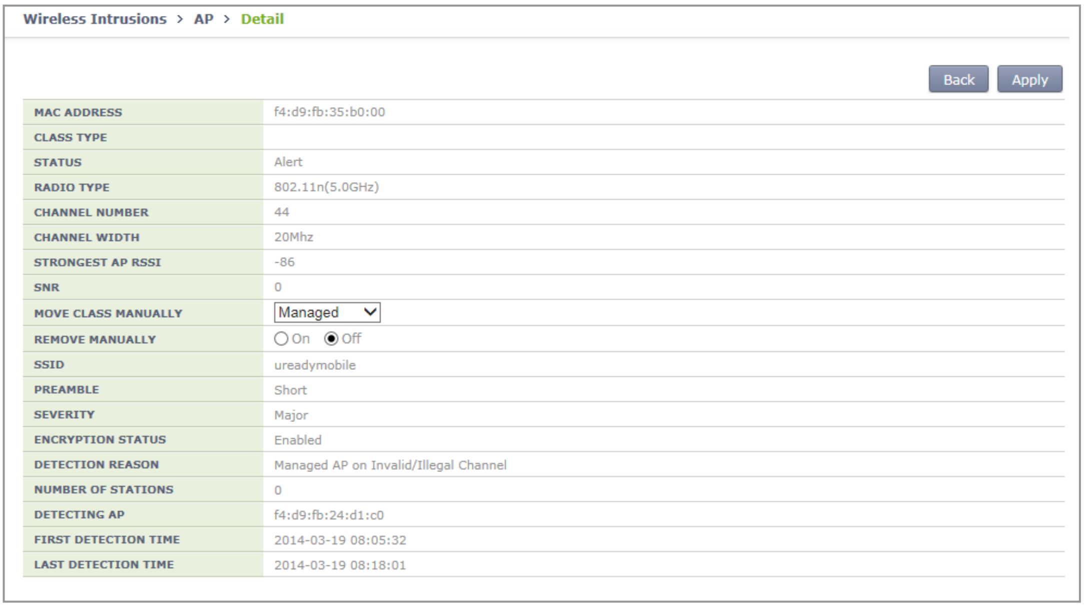
Current Filter : None

Total Entry : 1432

□	MAC ADDRESS	SSID	CHANNEL NUMBER	NUMBER OF CLIENTS	CLASS TYPE	STATUS	DETECTING AP
□	f4:d9:fb:42:7d:00	403_wlan_onoff_test_15	36	2		Alert	f4:d9:fb:24:d1:c0
□	f4:d9:fb:35:cc:00	ureadymobile	40	2		Alert	f4:d9:fb:24:d1:c0
□	f4:d9:fb:35:cc:01	setup	40	0		Alert	f4:d9:fb:24:d1:c0
□	f4:d9:fb:23:c4:02	SCME_AP	157	0		Alert	f4:d9:fb:24:d1:c0
□	f4:d9:fb:35:92:02	ureadymobile	44	0		Removed	f4:d9:fb:34:1f:e0
□	f4:d9:fb:35:8a:02	WEC8500IG13	153	0		Alert	f4:d9:fb:34:20:20
□	f4:d9:fb:36:d9:02	wec8500kkh	153	0		Removed	f4:d9:fb:24:d1:c0
□	f4:d9:fb:69:9a:02	ALEX_5G	161	0		Removed	f4:d9:fb:24:d1:c0
□	f4:d9:fb:23:be:02	ZCLUSTERED_RRM_5G	161	0	Managed	Managed	f4:d9:fb:34:20:60
□	f4:d9:fb:23:be:02	ZCLUSTER_TEST_16	9	0	Managed	Managed	f4:d9:fb:34:1f:e0

Figure 158. List Window to Manually Change Classification

2) In the AP detail screen, change the classification and click Apply, then the configuration is changed.



MAC ADDRESS	f4:d9:fb:35:b0:00
CLASS TYPE	
STATUS	Alert
RADIO TYPE	802.11n(5.0GHz)
CHANNEL NUMBER	44
CHANNEL WIDTH	20Mhz
STRONGEST AP RSSI	-86
SNR	0
MOVE CLASS MANUALLY	Managed
REMOVE MANUALLY	○ On ● Off
SSID	ureadymobile
PREAMBLE	Short
SEVERITY	Major
ENCRYPTION STATUS	Enabled
DETECTION REASON	Managed AP on Invalid/Illegal Channel
NUMBER OF STATIONS	0
DETECTING AP	f4:d9:fb:24:d1:c0
FIRST DETECTION TIME	2014-03-19 08:05:32
LAST DETECTION TIME	2014-03-19 08:18:01

Figure 159. Classification Change Window in AP Detail Screen

8.2.1.4 Manual configuration (Remove)

A user can manually change the status of an unauthorized AP to ‘Removed’, that is detected by the WIDS or that is classified according to the rule configured by a user.

Configuration using CLI

1) Go to configure → wi → device configuration mode of CLI.

```
WEC8500# configure terminal
WEC8500/configure# wi
WEC8500/configure/wi# device
WEC8500/configure/wi/device#
```

2) By using the MAC of an unauthorized AP to change, execute the remove command.
   - remove [MAC]

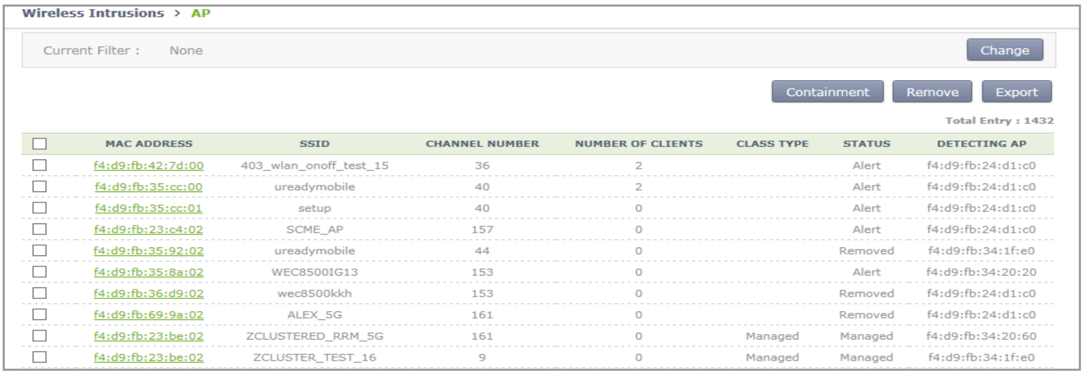
Parameter	Description
MAC	MAC address of an unauthorized AP

3) To check the changed configuration, use the following command.
   - show wi device ap list removed

Configuration using Web UI

In the menu bar of <**WEC Main window**>, select <**Monitor**> and then select the <**Wireless Intrusion**> → <**AP**> menu in the sub-menus. And when the AP list is displayed, check a desired MAC in the list and click the <**Remove**> button to manually remove an AP. In addition, after going into the detail view screen by selecting one out of the AP list, operator can also remove an AP by changing the REMOVE MANUALLY option to On.

1) In the AP list screen, operator can change the status of several APs to ‘Removed’ by clicking <**Remove**> button.



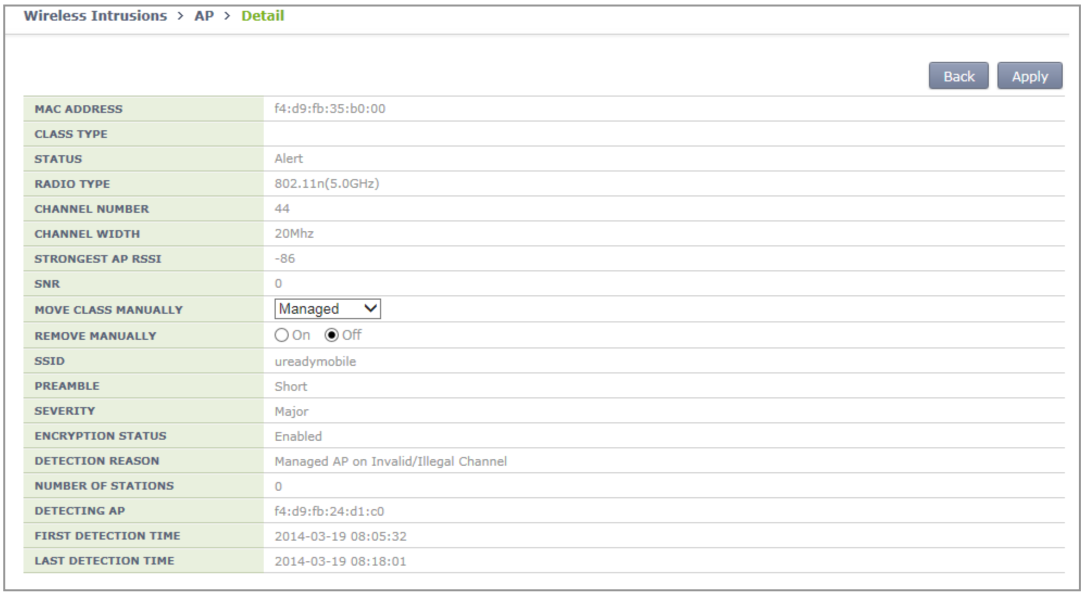
Current Filter : None

Total Entry : 1432

☐	MAC ADDRESS	SSID	CHANNEL NUMBER	NUMBER OF CLIENTS	CLASS TYPE	STATUS	DETECTING AP
☐	f4:d9:fb:42:7d:00	403_wlan_onoff_test_15	36	2		Alert	f4:d9:fb:24:d1:c0
☐	f4:d9:fb:35:cc:00	ureadymobile	40	2		Alert	f4:d9:fb:24:d1:c0
☐	f4:d9:fb:35:cc:01	setup	40	0		Alert	f4:d9:fb:24:d1:c0
☐	f4:d9:fb:23:c4:02	SCME_AP	157	0		Alert	f4:d9:fb:24:d1:c0
☐	f4:d9:fb:35:92:02	ureadymobile	44	0		Removed	f4:d9:fb:34:1f:e0
☐	f4:d9:fb:35:8a:02	WEC8500IG13	153	0		Alert	f4:d9:fb:34:20:20
☐	f4:d9:fb:36:d9:02	wec8500kkh	153	0		Removed	f4:d9:fb:24:d1:c0
☐	f4:d9:fb:69:9a:02	ALEX_5G	161	0		Removed	f4:d9:fb:24:d1:c0
☐	f4:d9:fb:23:be:02	ZCLUSTERED_RRM_5G	161	0	Managed	Managed	f4:d9:fb:34:20:60
☐	f4:d9:fb:23:be:02	ZCLUSTER_TEST_16	9	0	Managed	Managed	f4:d9:fb:34:1f:e0

Figure 160. List Window to Manually Remove

2) If you change the setting of REMOVE MANUALLY to ‘On’ in the AP detail screen and click Apply, the AP status is changed to ‘Removed’.



MAC ADDRESS	f4:d9:fb:35:b0:00
CLASS TYPE	
STATUS	Alert
RADIO TYPE	802.11n(5.0GHz)
CHANNEL NUMBER	44
CHANNEL WIDTH	20Mhz
STRONGEST AP RSSI	-86
SNR	0
MOVE CLASS MANUALLY	Managed
REMOVE MANUALLY	○ On ● Off
SSID	ureadymobile
PREAMBLE	Short
SEVERITY	Major
ENCRYPTION STATUS	Enabled
DETECTION REASON	Managed AP on Invalid/Illegal Channel
NUMBER OF STATIONS	0
DETECTING AP	f4:d9:fb:24:d1:c0
FIRST DETECTION TIME	2014-03-19 08:05:32
LAST DETECTION TIME	2014-03-19 08:18:01

Figure 161. Manual Remove Change Window in AP Detail Screen

8.2.1.5 Unauthorized AP detection option

Operator can enable or disable the AP detection option pre-defined in the system.

Configuration using CLI

1) Go to configure → wi → device → ap configuration mode.

```
WEC8500# configure terminal
WEC8500/configure# wi
WEC8500/configure/wi# device
WEC8500/configure/wi/device# ap
WEC8500/configure/wi/device/ap#
```

2) Using the following command, configure the unauthorized AP detection option.
   - [OPTION] [NOTI_TYPE]

Parameter	Description
OPTION	Unauthorized AP detection option
NOTI_TYPE	Event save option - notify: Notify the state with alarm - detect: Save the state with sys log

The description of OPTION parameter is as follows:

Parameter	Description
ap-blacklist-check	Allocates Rogue ID = 101 by checking a rogue included in the black list.
managed_ssid_invalid_security	Allocates Rogue ID = 102 for an AP that uses a managed SSID and its managed client is in the association status.
fakeap-beacon-on-invalid-channel	Allocates rogue ID = 103 for an AP whose UIC is invalid and that uses a SSID that is not in the ssid white list among the APs that use a managed MAC.
fakeap-beacon-without-ssid	Allocates Rogue ID = 104 for an AP whose UIC is invalid and its SSID is hidden among the APs that use a managed MAC.
fakeap-managed-ssid	Allocates Rogue ID = 105 for an AP whose UIC is invalid and its channel is not in the channel validation list among the APs that use a managed MAC.
illegal-channel	Allocates Rogue ID = 106 if an AP uses a channel that is not in the channel validation list among detected APs.
managedap-invalid-ssid	Allocates Rogue ID = 107 for an AP that uses a SSID that is not in the ssid-whitelist among the APs that use a managed MAC and its UIC is valid.
unknownap-managed-ssid-withauth-client	Allocates Rogue ID = 108 by checking the association status between an unauthorized AP and a managed client.

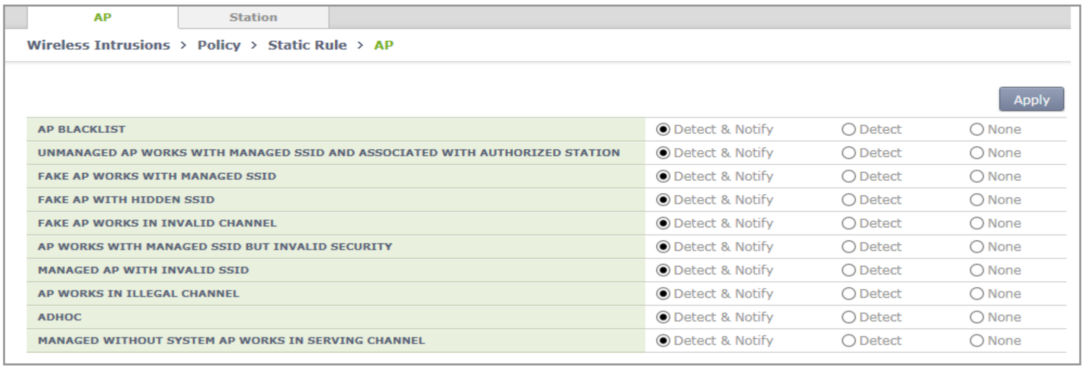
3) To check the changed configuration, use the following command.

- show wi device ap current-config

Configuration using Web UI

In the menu bar of <**WEC Main window**>, select <**Configuration**> and then select the <**Wireless Intrusion**> → <**Policy**> → <**Static Rule**> menu in the sub-menus. And then, operator can change the setting by selecting <AP> at the upper tab and clicking Apply.

In the configuration screen, operator can check Option and click Apply for configuration.



AP BLACKLIST	● Detect & Notify	○ Detect	○ None
UNMANAGED AP WORKS WITH MANAGED SSID AND ASSOCIATED WITH AUTHORIZED STATION	● Detect & Notify	○ Detect	○ None
FAKE AP WORKS WITH MANAGED SSID	● Detect & Notify	○ Detect	○ None
FAKE AP WITH HIDDEN SSID	● Detect & Notify	○ Detect	○ None
FAKE AP WORKS IN INVALID CHANNEL	● Detect & Notify	○ Detect	○ None
AP WORKS WITH MANAGED SSID BUT INVALID SECURITY	● Detect & Notify	○ Detect	○ None
MANAGED AP WITH INVALID SSID	● Detect & Notify	○ Detect	○ None
AP WORKS IN ILLEGAL CHANNEL	● Detect & Notify	○ Detect	○ None
ADHOC	● Detect & Notify	○ Detect	○ None
MANAGED WITHOUT SYSTEM AP WORKS IN SERVING CHANNEL	● Detect & Notify	○ Detect	○ None

Figure 162. Configuration Window for Unauthorized AP Detection Option

8.2.1.6 Unauthorized client detection option

Operator can enable or disable the client detection option pre-defined in the system.

Configuration using CLI

1) Go to configure → wi → device → client configuration mode.

```
WEC8500# configure terminal
WEC8500/configure# wi
WEC8500/configure/wi# rogue
WEC8500/configure/wi/device# client
WEC8500/configure/wi/device /client#
```

2) Configure the unauthorized client detection option by using the following command.
   - [OPTION] [NOTI_TYPE]

Parameter	Description
OPTION	Rogue Client detect option
NOTI_TYPE	Event save option - notify: Notify the state with alarm - detect: Save the state with sys log

The description of OPTION parameter is as follows:

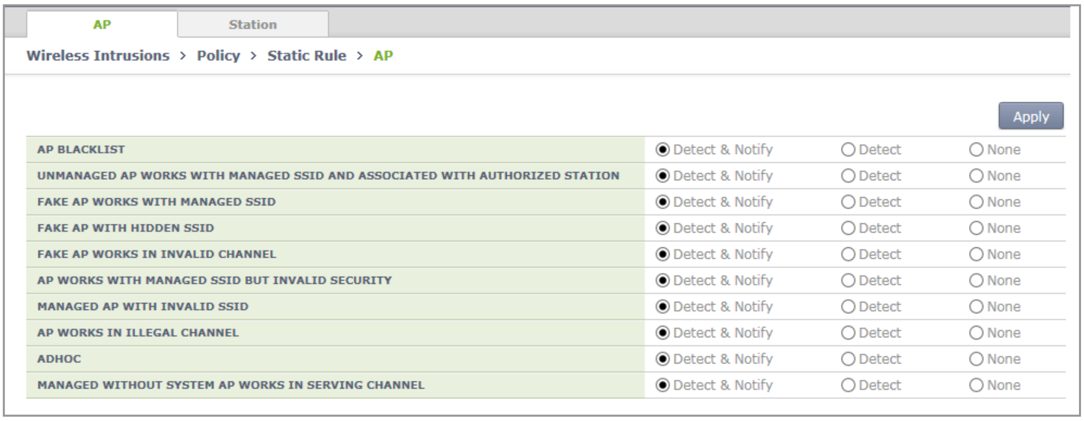
Parameter	Description
assoc-fail-det	Classifies a client that exceeds the association fail threshold as an unauthorized client.
auth-fail-det	Classifies a client that exceeds the authentication fail threshold as an unauthorized client.
auth-request-det	Classifies a client that exceeds the authentication request threshold as an unauthorized client.
deauth-request-det	Classifies a client that exceeds the de-authentication request threshold as an unauthorized client.
exclusion-list-check	Classifies a MAC that does not exist in the client blacklist as an unauthorized client.
oneXauth-fail-det	Classifies a client that exceeds the 802.1X authentication fail threshold as an unauthorized client.
oui-list-check	Classifies an OUI that does not exist in the OUI list white list as an unauthorized client.
probe-request-det	Classifies a client that exceeds the probe request threshold as an unauthorized client.
webauth-fail-det	Classifies a client that exceeds the WEB authentication fail threshold as an unauthorized client.

3) To check the changed configuration, use the following command.
   - show wi device client current-config

Configuration using Web UI

In the menu bar of **<WEC Main window>**, select **<Configuration>** and then select the **<Wireless Intrusion>** → **<Policy>** → **<Static Rule>** menu in the sub-menus. And then, operator can change the setting by selecting <Station> at the upper tab and clicking Apply.

In the configuration screen, operator can check Option and click Apply for configuration.



AP BLACKLIST	● Detect & Notify	○ Detect	○ None
UNMANAGED AP WORKS WITH MANAGED SSID AND ASSOCIATED WITH AUTHORIZED STATION	● Detect & Notify	○ Detect	○ None
FAKE AP WORKS WITH MANAGED SSID	● Detect & Notify	○ Detect	○ None
FAKE AP WITH HIDDEN SSID	● Detect & Notify	○ Detect	○ None
FAKE AP WORKS IN INVALID CHANNEL	● Detect & Notify	○ Detect	○ None
AP WORKS WITH MANAGED SSID BUT INVALID SECURITY	● Detect & Notify	○ Detect	○ None
MANAGED AP WITH INVALID SSID	● Detect & Notify	○ Detect	○ None
AP WORKS IN ILLEGAL CHANNEL	● Detect & Notify	○ Detect	○ None
ADHOC	● Detect & Notify	○ Detect	○ None
MANAGED WITHOUT SYSTEM AP WORKS IN SERVING CHANNEL	● Detect & Notify	○ Detect	○ None

Figure 163. Configuration Window for Unauthorized Station Detection Option

8.2.1.7 Unauthorized Channel Validation Configuration

The unauthorized channel validation function helps an operator detect an AP that uses an unauthorized channel other than configured channels. The configuration procedure is as follows:

Configuration using CLI

1) Go to configure → wi → channel-validation configuration mode of CLI.

```
WEC8500# configure terminal
WEC8500/configure# wi
WEC8500/configure/wi# channel-validation
```

2) Enable the unauthorized channel validation function.

```
WEC8500/configure/wi/channel-validation# enable
```

3) Configure an authorized channel.
   - add [CHANNEL]

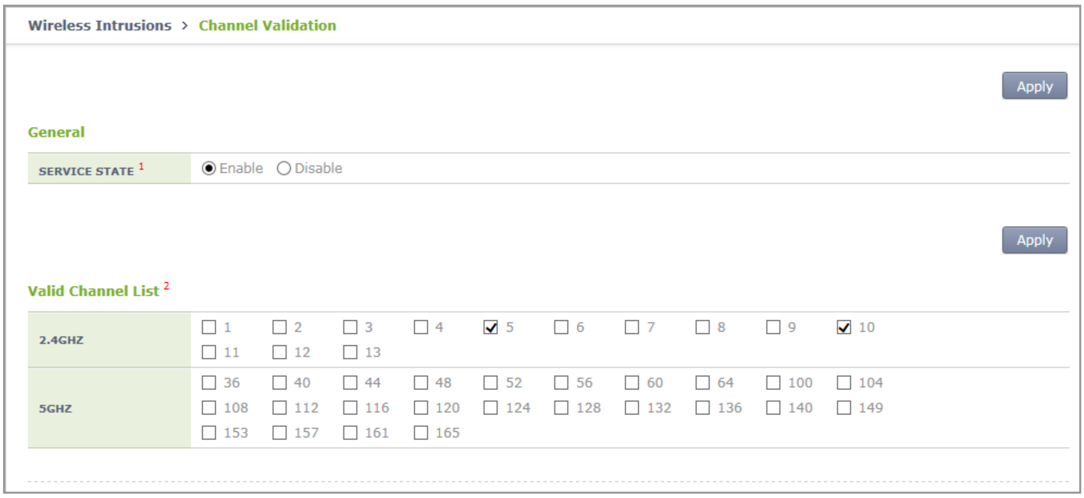
Parameter	Description
CHANNEL	Authorized channel number (e.g. add 2, 3, 4)

4) To check the changed configuration, execute the following command.
   - show wi current-config

Configuration using Web UI

In the menu bar of **<WEC Main window>**, select **<Configuration>** and then select the **<Wireless Intrusion>** → **<Channel Validation>** menu in the sub-menus. And then, operator can configure the SERVICE STATE and Valid Channel List in the screen.

Operator can change configuration after changing the SERVICE STATE and Valid Channel List and clicking Apply.



General

SERVICE STATE [1] ● Enable ○ Disable

Valid Channel List [2]

2.4GHZ	□ 1	□ 2	□ 3	□ 4	☑ 5	□ 6	□ 7	□ 8	□ 9	☑ 10
	□ 11	□ 12	□ 13							
5GHZ	□ 36	□ 40	□ 44	□ 48	□ 52	□ 56	□ 60	□ 64	□ 100	□ 104
	□ 108	□ 112	□ 116	□ 120	□ 124	□ 128	□ 132	□ 136	□ 140	□ 149
	□ 153	□ 157	□ 161	□ 165						

Figure 164. Configuration Window for Channel Validation

8.2.1.8 Configuring and Searching Black/White List

Operator can configure classification to distinguish authorized and unauthorized APs/stations. The administrator configurable lists include <AP black-list, Station black-list, Managed OUI, Managed/Neighbor AP>. The <Managed AP, Managed Station, Managed SSID> are automatically configured and can be used only for search.

Configuration using CLI

1) Go to the configure → wids configuration mode of CLI.

```
WEC8500# configure terminal
WEC8500/configure# wi
```

2) Configure the AP black-list.
   - ap-blacklist [MAC]

Parameter	Description
MAC	MAC address that will be used as AP black-list

3) Configure the station black-list.
   - client-black-list [MAC]

Parameter	Description
MAC	MAC address that will be used as a black-list of the station

4) Configure the Managed Organizationally Unique Identifier (OUI).
   - oui-whitelist [OUI]

Parameter	Description
OUI	First 3 bytes of station MAC address

5) Configure the Managed/Neighbor AP.
   - Managed [MAC] [TYPE]

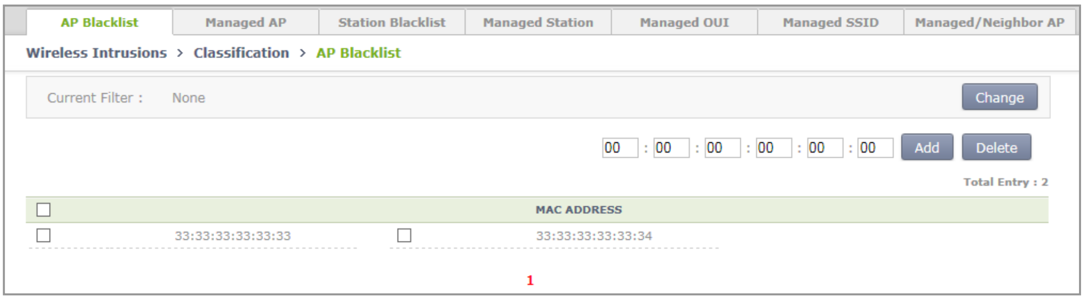
Parameter	Description
MAC	AP MAC address of Managed/Neighbor AP
TYPE	- Managed: Indicates that the address is located internally during configuration - Neighbor: Indicates that the address is located externally during configuration

6) To check the changed configuration, execute the following command.
   - show wi lists managed-ap
   - show wi lists ap-blacklist
   - show wi lists mananged-stat
   - show wi lists client-blacklist
   - show wi lists managed ssid
   - show wi lists oui-list
   - show wi lists neighbor-ap

Configuration using Web UI

In the menu bar of **<WEC Main window>**, select **<Configuration>** and then select the **<Wireless Intrusion>** → **<Classification>** menu in the sub-menus. And then, operator can configure and search by using the upper tab in the screen.

1) In the [AP Blacklist] tab, operator can add an AP blacklist by entering a MAC and click Add. Operator can also delete it by using Delete.



Current Filter : None

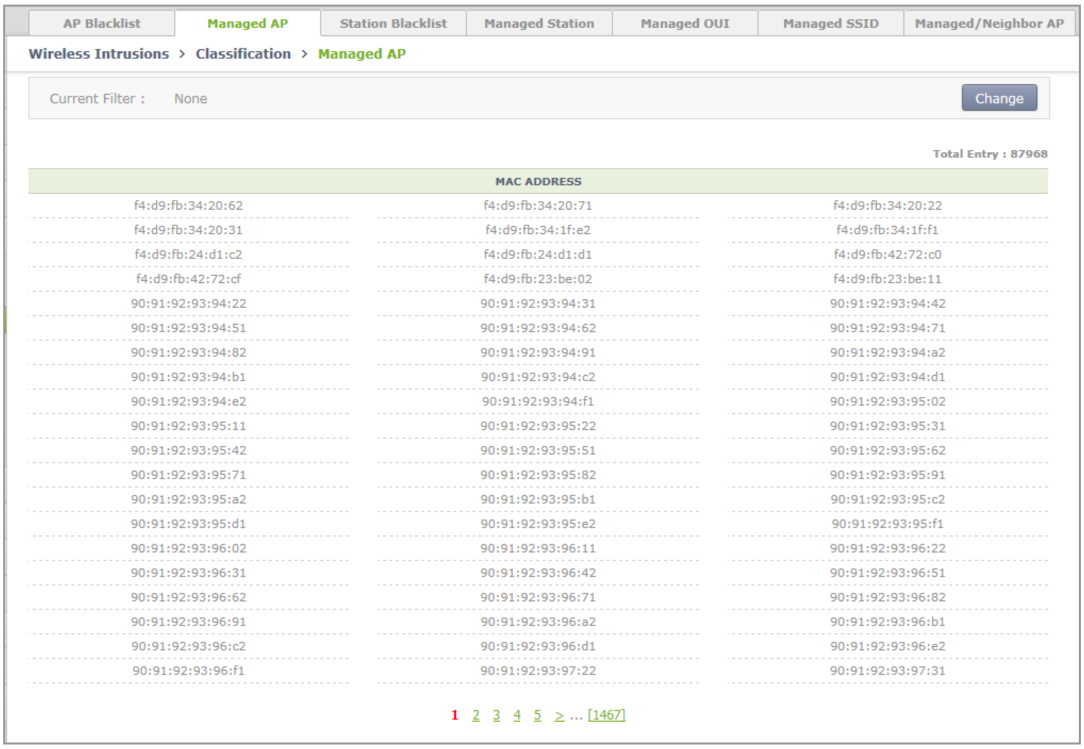
00 : 00 : 00 : 00 : 00 : 00

Total Entry : 2

☐	MAC ADDRESS		
☐	33:33:33:33:33:33	☐	33:33:33:33:33:34

1

Figure 165. AP blacklist Configuration Window



Current Filter : None

Total Entry : 87968

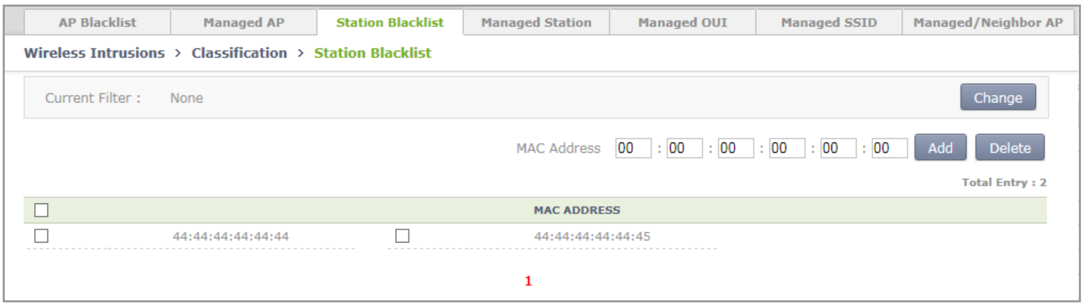
MAC ADDRESS		
f4:d9:fb:34:20:62	f4:d9:fb:34:20:71	f4:d9:fb:34:20:22
f4:d9:fb:34:20:31	f4:d9:fb:34:1f:e2	f4:d9:fb:34:1f:f1
f4:d9:fb:24:d1:c2	f4:d9:fb:24:d1:d1	f4:d9:fb:42:72:c0
f4:d9:fb:42:72:cf	f4:d9:fb:23:be:02	f4:d9:fb:23:be:11
90:91:92:93:94:22	90:91:92:93:94:31	90:91:92:93:94:42
90:91:92:93:94:51	90:91:92:93:94:62	90:91:92:93:94:71
90:91:92:93:94:82	90:91:92:93:94:91	90:91:92:93:94:a2
90:91:92:93:94:b1	90:91:92:93:94:c2	90:91:92:93:94:d1
90:91:92:93:94:e2	90:91:92:93:94:f1	90:91:92:93:95:02
90:91:92:93:95:11	90:91:92:93:95:22	90:91:92:93:95:31
90:91:92:93:95:42	90:91:92:93:95:51	90:91:92:93:95:62
90:91:92:93:95:71	90:91:92:93:95:82	90:91:92:93:95:91
90:91:92:93:95:a2	90:91:92:93:95:b1	90:91:92:93:95:c2
90:91:92:93:95:d1	90:91:92:93:95:e2	90:91:92:93:95:f1
90:91:92:93:96:02	90:91:92:93:96:11	90:91:92:93:96:22
90:91:92:93:96:31	90:91:92:93:96:42	90:91:92:93:96:51
90:91:92:93:96:62	90:91:92:93:96:71	90:91:92:93:96:82
90:91:92:93:96:91	90:91:92:93:96:a2	90:91:92:93:96:b1
90:91:92:93:96:c2	90:91:92:93:96:d1	90:91:92:93:96:e2
90:91:92:93:96:f1	90:91:92:93:97:22	90:91:92:93:97:31

1 2 3 4 5 > ... [1467]

2) In the [Managed AP] tab, operator can search for a Managed AP.

Figure 166. Managed AP Window

3) In the [Station Blacklist] tab, operator can add a station blacklist by entering a MAC and click Add. Operator can also delete it by using Delete.



Current Filter : None

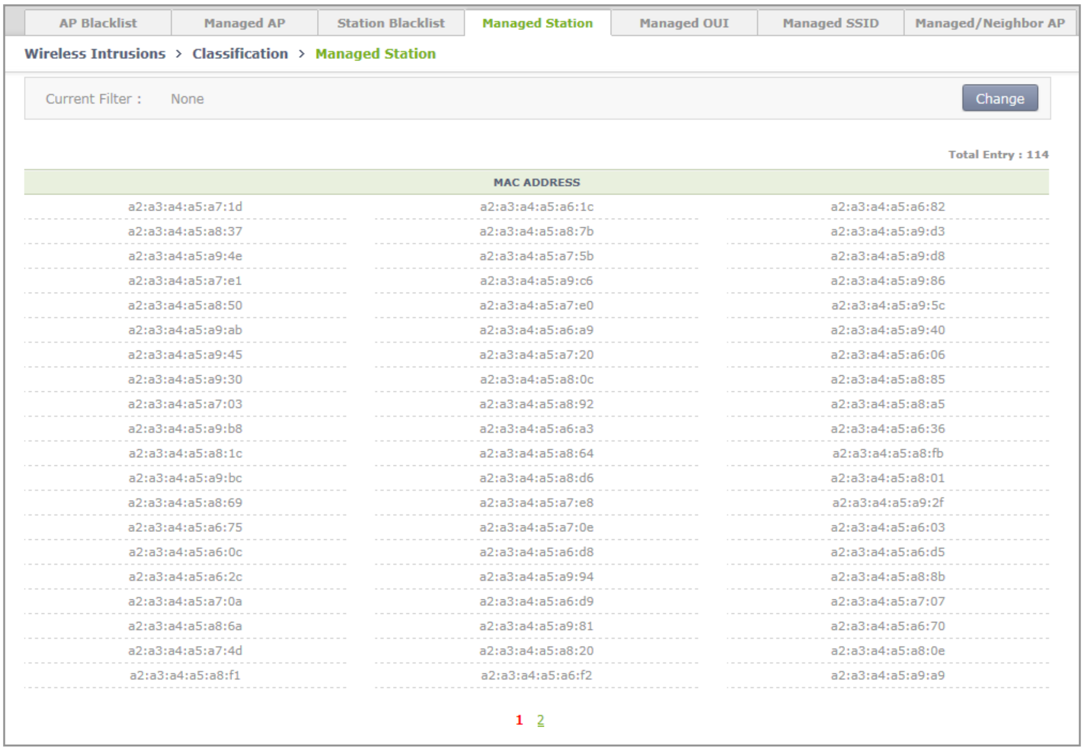
MAC Address 00 : 00 : 00 : 00 : 00 : 00

Total Entry : 2

□	MAC ADDRESS		
□	44:44:44:44:44:44	□	44:44:44:44:44:45

Figure 167. Station blacklist Search/Configuration Window

4) In the [Managed Station] tab, operator can search Managed Station.



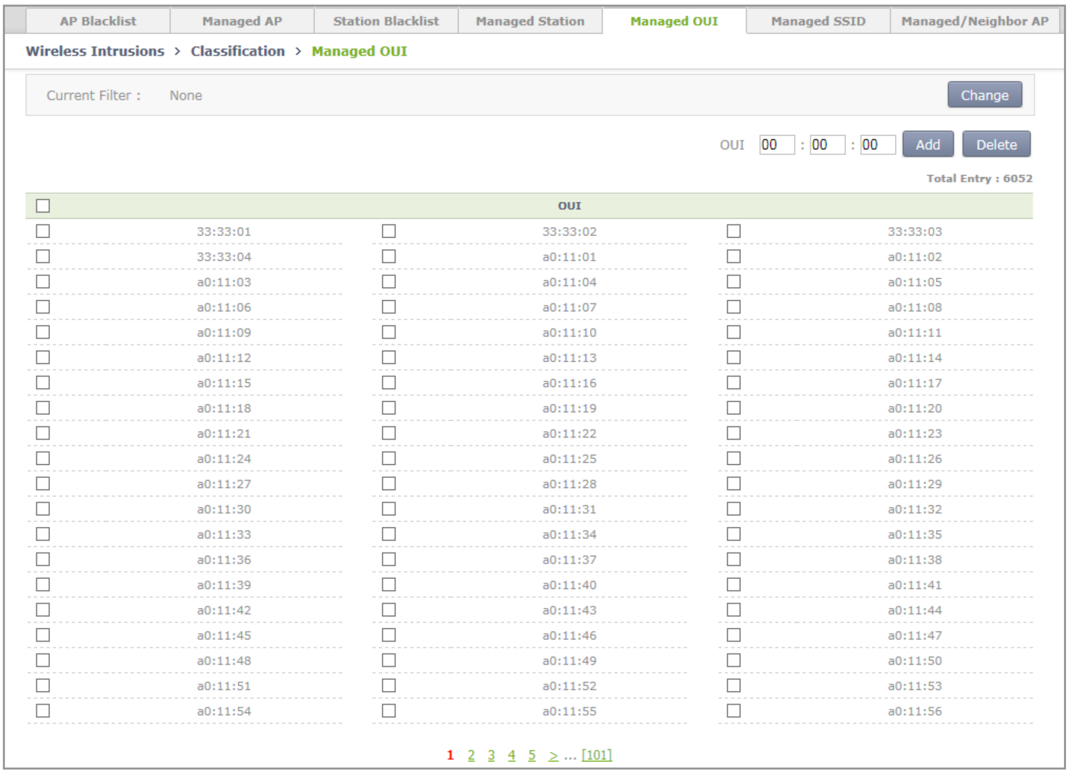
Current Filter : None

Total Entry : 114

	MAC ADDRESS	
a2:a3:a4:a5:a7:1d	a2:a3:a4:a5:a6:1c	a2:a3:a4:a5:a6:82
a2:a3:a4:a5:a8:37	a2:a3:a4:a5:a8:7b	a2:a3:a4:a5:a9:d3
a2:a3:a4:a5:a9:4e	a2:a3:a4:a5:a7:5b	a2:a3:a4:a5:a9:d8
a2:a3:a4:a5:a7:e1	a2:a3:a4:a5:a9:c6	a2:a3:a4:a5:a9:86
a2:a3:a4:a5:a8:50	a2:a3:a4:a5:a7:e0	a2:a3:a4:a5:a9:5c
a2:a3:a4:a5:a9:ab	a2:a3:a4:a5:a6:a9	a2:a3:a4:a5:a9:40
a2:a3:a4:a5:a9:45	a2:a3:a4:a5:a7:20	a2:a3:a4:a5:a6:06
a2:a3:a4:a5:a9:30	a2:a3:a4:a5:a8:0c	a2:a3:a4:a5:a8:85
a2:a3:a4:a5:a7:03	a2:a3:a4:a5:a8:92	a2:a3:a4:a5:a8:a5
a2:a3:a4:a5:a9:b8	a2:a3:a4:a5:a6:a3	a2:a3:a4:a5:a6:36
a2:a3:a4:a5:a8:1c	a2:a3:a4:a5:a8:64	a2:a3:a4:a5:a8:fb
a2:a3:a4:a5:a9:bc	a2:a3:a4:a5:a8:d6	a2:a3:a4:a5:a8:01
a2:a3:a4:a5:a8:69	a2:a3:a4:a5:a7:e8	a2:a3:a4:a5:a9:2f
a2:a3:a4:a5:a6:75	a2:a3:a4:a5:a7:0e	a2:a3:a4:a5:a6:03
a2:a3:a4:a5:a6:0c	a2:a3:a4:a5:a6:d8	a2:a3:a4:a5:a6:d5
a2:a3:a4:a5:a6:2c	a2:a3:a4:a5:a9:94	a2:a3:a4:a5:a8:8b
a2:a3:a4:a5:a7:0a	a2:a3:a4:a5:a6:d9	a2:a3:a4:a5:a7:07
a2:a3:a4:a5:a8:6a	a2:a3:a4:a5:a9:81	a2:a3:a4:a5:a6:70
a2:a3:a4:a5:a7:4d	a2:a3:a4:a5:a8:20	a2:a3:a4:a5:a8:0e
a2:a3:a4:a5:a8:f1	a2:a3:a4:a5:a6:f2	a2:a3:a4:a5:a9:a9

Figure 168. Managed Station Search Window

5) In the [Managed OUI] tab, operator can add a Managed OUI by entering an OUI and click Add. Operator can also delete it by using Delete.



Wireless Intrusions > Classification > Managed OUI

Current Filter : None

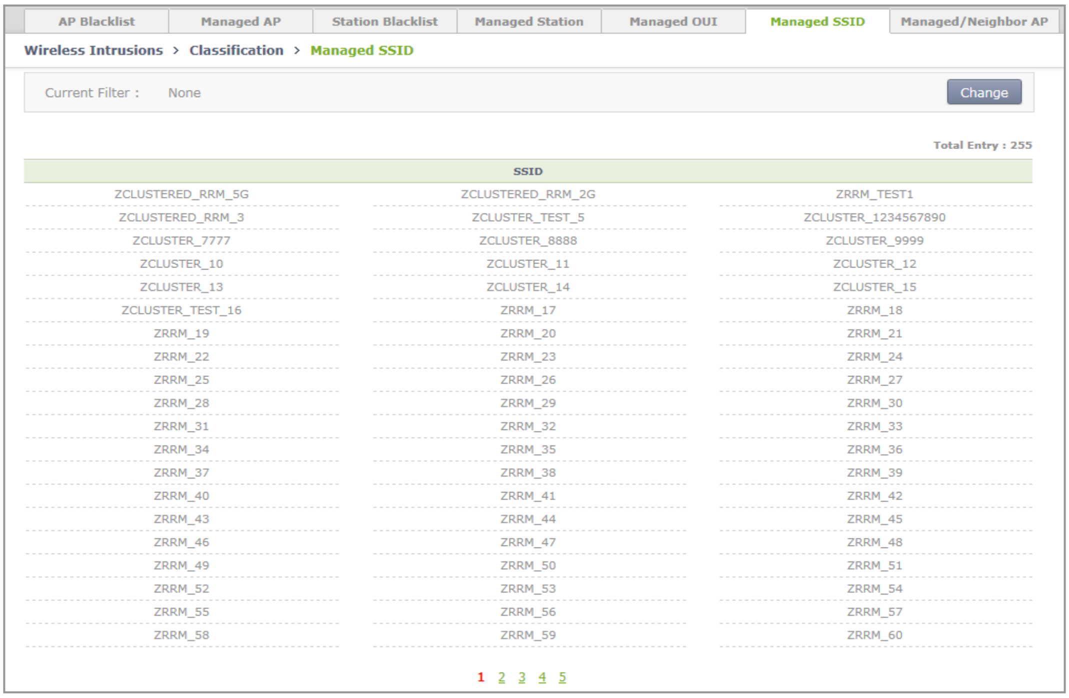
OUI 00 : 00 : 00

Total Entry : 6052

□	OUI	□		□	
□	33:33:01	□	33:33:02	□	33:33:03
□	33:33:04	□	a0:11:01	□	a0:11:02
□	a0:11:03	□	a0:11:04	□	a0:11:05
□	a0:11:06	□	a0:11:07	□	a0:11:08
□	a0:11:09	□	a0:11:10	□	a0:11:11
□	a0:11:12	□	a0:11:13	□	a0:11:14
□	a0:11:15	□	a0:11:16	□	a0:11:17
□	a0:11:18	□	a0:11:19	□	a0:11:20
□	a0:11:21	□	a0:11:22	□	a0:11:23
□	a0:11:24	□	a0:11:25	□	a0:11:26
□	a0:11:27	□	a0:11:28	□	a0:11:29
□	a0:11:30	□	a0:11:31	□	a0:11:32
□	a0:11:33	□	a0:11:34	□	a0:11:35
□	a0:11:36	□	a0:11:37	□	a0:11:38
□	a0:11:39	□	a0:11:40	□	a0:11:41
□	a0:11:42	□	a0:11:43	□	a0:11:44
□	a0:11:45	□	a0:11:46	□	a0:11:47
□	a0:11:48	□	a0:11:49	□	a0:11:50
□	a0:11:51	□	a0:11:52	□	a0:11:53
□	a0:11:54	□	a0:11:55	□	a0:11:56

1 2 3 4 5 > ... [101]

6) In the [Managed SSID] tab, you can check the SSID that the WLAN is using.



Wireless Intrusions > Classification > Managed SSID

Current Filter : None

Total Entry : 255

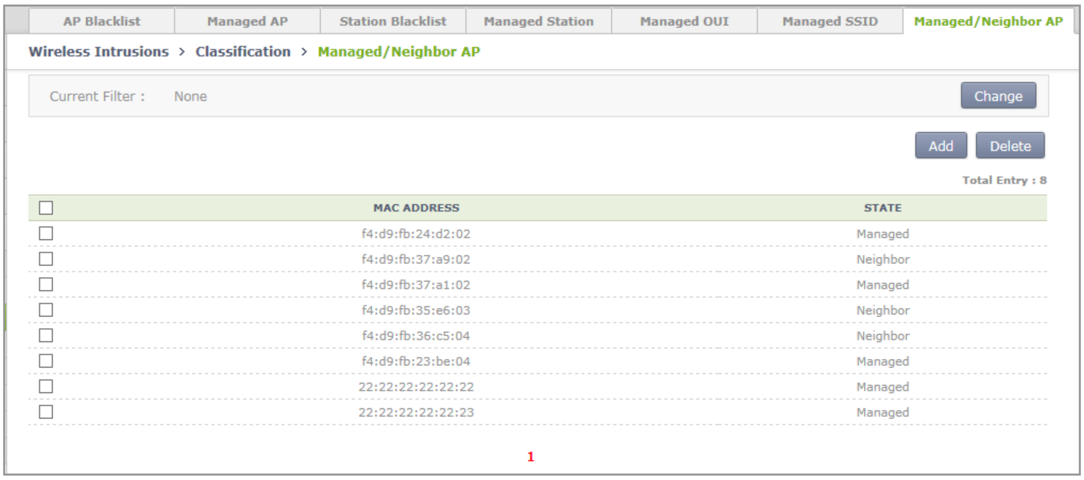
SSID		
ZCLUSTERED_RRM_5G	ZCLUSTERED_RRM_2G	ZRRM_TEST1
ZCLUSTERED_RRM_3	ZCLUSTER_TEST_5	ZCLUSTER_1234567890
ZCLUSTER_7777	ZCLUSTER_8888	ZCLUSTER_9999
ZCLUSTER_10	ZCLUSTER_11	ZCLUSTER_12
ZCLUSTER_13	ZCLUSTER_14	ZCLUSTER_15
ZCLUSTER_TEST_16	ZRRM_17	ZRRM_18
ZRRM_19	ZRRM_20	ZRRM_21
ZRRM_22	ZRRM_23	ZRRM_24
ZRRM_25	ZRRM_26	ZRRM_27
ZRRM_28	ZRRM_29	ZRRM_30
ZRRM_31	ZRRM_32	ZRRM_33
ZRRM_34	ZRRM_35	ZRRM_36
ZRRM_37	ZRRM_38	ZRRM_39
ZRRM_40	ZRRM_41	ZRRM_42
ZRRM_43	ZRRM_44	ZRRM_45
ZRRM_46	ZRRM_47	ZRRM_48
ZRRM_49	ZRRM_50	ZRRM_51
ZRRM_52	ZRRM_53	ZRRM_54
ZRRM_55	ZRRM_56	ZRRM_57
ZRRM_58	ZRRM_59	ZRRM_60

1 2 3 4 5

Figure 169. Managed SSID Window

7) If you click Add in the [Managed/Neighbor AP] tab, operator can go to the Managed/ Neighbor AP list addition screen and can add a Managed/Neighbor AP list. Operator can also delete it by using Delete.

- [Managed/Neighbor AP] tab main screen



Current Filter : None

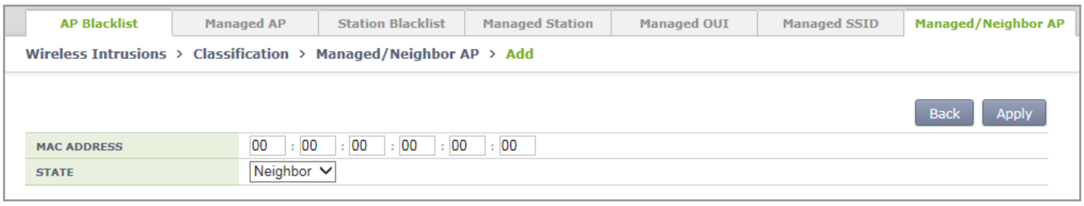
Total Entry : 8

☐	MAC ADDRESS	STATE
☐	f4:d9:fb:24:d2:02	Managed
☐	f4:d9:fb:37:a9:02	Neighbor
☐	f4:d9:fb:37:a1:02	Managed
☐	f4:d9:fb:35:e6:03	Neighbor
☐	f4:d9:fb:36:c5:04	Neighbor
☐	f4:d9:fb:23:be:04	Managed
☐	22:22:22:22:22:22	Managed
☐	22:22:22:22:22:23	Managed

1

Figure 170. Managed/Neighbor AP Search/Configuration Window

- Managed/Neighbor AP list addition screen



MAC ADDRESS	00 : 00 : 00 : 00 : 00 : 00
STATE	Neighbor

Figure 171. Managed/Neighbor AP List Addition Window

8.2.1.9 Station Allow Limit

The WIDS counts the number of frames and number of authentication failures to distinguish a station that generates too many management frames in a network or that is continuously failed for authentication. A threshold value is defined for the count and a station is recognized as an unauthorized station if the count exceeds the threshold.

Configuration using CLI

1) Go to the configure → wi → device → client configuration mode.

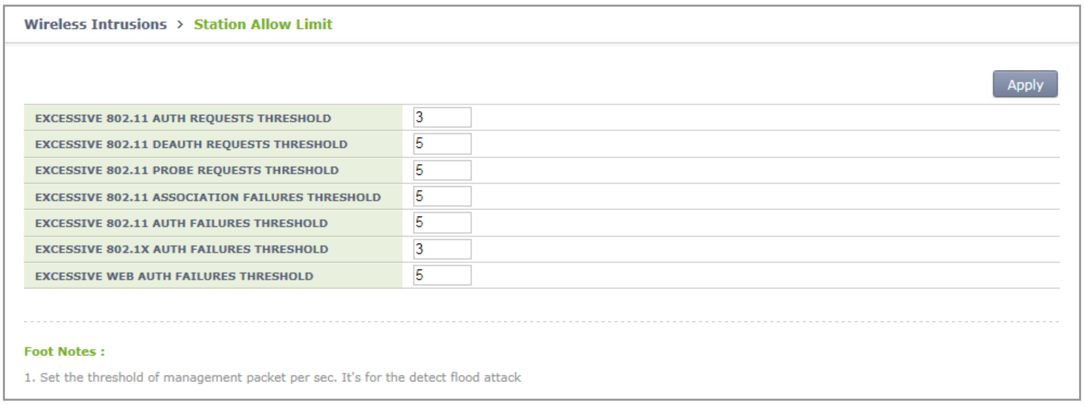
```
WEC8500# configure terminal
WEC8500/configure# wi
WEC8500/configure/wi# device
WEC8500/configure/wi/device# client
WEC8500/configure/wi/device/client#
```

2) Configure a threshold.
   - allowed-limit [OPTION] [COUNT]

Parameter	Description
OPTION	- 80211-auth-req: Authentication requests threshold per second - 80211-probe-req: Probe requests threshold per second - 80211-deauth-req: De-authentication requests threshold per second - 80211-assoc-fail: Association failures threshold per second - 80211-auth-fail: Authentication failures threshold per second - 8021x-auth-fail: 802.1x authentication failures threshold per WIDS interval - web-auth-fail: Web authentication failures threshold that occurs continuously
COUNT	Threshold value of [OPTION] ranging from 3 to 20

Configuration using Web UI

In the menu bar of **<WEC Main window>**, select **<Configuration>** and then select the **<Wireless Intrusion>** → **<Station Allow Limit>** menu in the sub-menus. And then, enter a threshold value and click Apply to configure the value in the screen.



EXCESSIVE 802.11 AUTH REQUESTS THRESHOLD	3
EXCESSIVE 802.11 DEAUTH REQUESTS THRESHOLD	5
EXCESSIVE 802.11 PROBE REQUESTS THRESHOLD	5
EXCESSIVE 802.11 ASSOCIATION FAILURES THRESHOLD	5
EXCESSIVE 802.11 AUTH FAILURES THRESHOLD	5
EXCESSIVE 802.1X AUTH FAILURES THRESHOLD	3
EXCESSIVE WEB AUTH FAILURES THRESHOLD	5

Foot Notes :

1. Set the threshold of management packet per sec. It's for the detect flood attack

Figure 172. Station Allowed Limit Configuration Window

8.3 Captive Portal

The W-EP wireless LAN system provides the Guest Access function. A guest user can receive a limited service after connected to a specific WLAN (SSID) and going through authentication.

8.3.1 WLAN Security Configuration

Configuration using CLI

To configure WLAN security for guest connection control, execute the command as follows:

1) Go to configure → wlan configuration mode of CLI.

```
WEC8500# configure terminal
WEC8500/configure# wlan 1
```

2) Disable the WLAN.

```
WEC8500/configure/wlan 1# no enable
```

3) Configure the WEB policy (default: disabled).

```
WEC8500/configure/wlan 1/security/layer3# web-policy
```

4) Enable the WEB authentication (default: disabled)

```
WEC8500/configure/wlan 1/security/layer3# web-policy authentication
```

5) Configure a guest flag (default: disabled).

```
WEC8500/configure/wlan 1# guest-flag
```

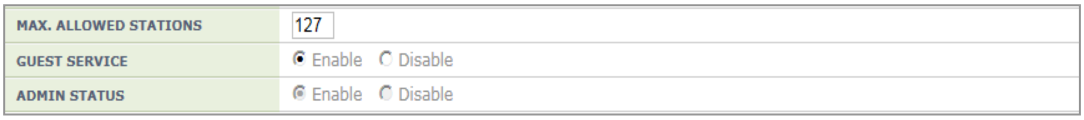
6) Enable the WLAN.

```
WEC8500/configure/wlan 1# enable
```

7) To check the configured environment, use the ‘show wlan security summary’ command.

Configuration using Web UI

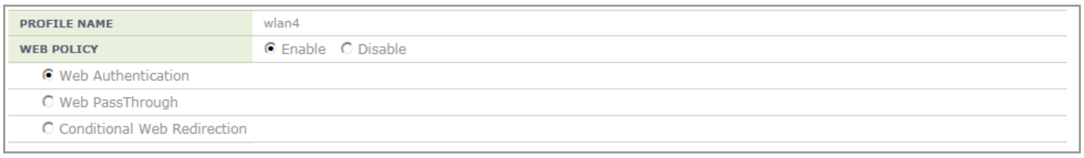
In the menu bar of **<WEC Main window>**, select **<Configuration>** and then select the **<WLANs>** menu in the sub-menus. In the WLANs screen, select WLAN ID and enable the **<GUEST SERVICE>** option.



MAX. ALLOWED STATIONS	127
GUEST SERVICE	● Enable ○ Disable
ADMIN STATUS	● Enable ○ Disable

Figure 173. WLAN Guest Configuration Window

Go to the **<L3>** of **<Security>** tab. Enable **<WEB POLICY>** and select Web Authentication.



PROFILE NAME	wlan4
WEB POLICY	● Enable ○ Disable

● Web Authentication
○ Web PassThrough
○ Conditional Web Redirection

Figure 174. WLAN Web Policy Configuration Window

8.3.2 Guest Connection Configuration

Configuration using CLI

By executing the 'security captive-portal' command, operator can configure various Captive Portal related options.
First of all, enter into the configuration mode to execute the command.

```
WEC8500# configure terminal
```

[Adding User]
To add a guest user, execute the command as follows:

- security captive-portal guest add [ID] [PASSWD] [START_TIME] [END_TIME]

Parameter	Description
ID	Login ID of a user
PASSWD	Password
START_TIME	start time (YYYY-MM-DD:HH:MM:SS format)
END_TIME	end time (YYYY-MM-DD:HH:MM:SS format)

[Deleting User]

To add a guest user, execute the command as follows:

- security captive-portal guest delete [ID]

Parameter	Description
ID	User ID

[Auth Type Configuration]

To select the authentication method for a guest service, execute the command as follows:

- security captive-portal auth-type [FLAG]

Parameter	Description
FLAG	Authentication method - local-only: Uses internal authentication. - radius-only: Uses RADIUS server authentication. - local-radius: Uses Radius authentication if the internal authentication is failed. - radius-local: Uses the internal authentication if the RADIUS server authentication is failed.

[RADIUS Server Configuration]

For RADIUS authentication, operator can configure the primary and secondary server by using a profile id.

- security captive-portal radius-primary [PROFILE_ID]
- security captive-portal radius-secondary [PROFILE_ID]

Parameter	Description
PROFILE_ID	Profile ID

[Operation Configuration after Authentication]

To configure the operation after authentication, execute the command as follows:

- security captive-portal web-auth after-auth [FLAG]
- security captive-portal web-auth redirect-url [URL]

Parameter	Description
FLAG	Operation after authentication - redirect: Redirect to a specified URL - request: Redirect to a requested URL
URL	URL specified as the operation after authentication

[Web Authentication Method Configuration]

To configure the web authentication method used for guest authentication, execute the command as follows:

- security captive-portal web-auth web-type [FLAG]
- security captive-portal web-auth external-url [URL]

Parameter	Description
FLAG	Web Authentication Method - internal: Uses the internal authentication page. - external: Uses the authentication page of an external web server. - downloaded: Uses the authentication page downloaded from the system. - customized: Uses the authentication page created through configuration.
URL	Address of an external authentication server

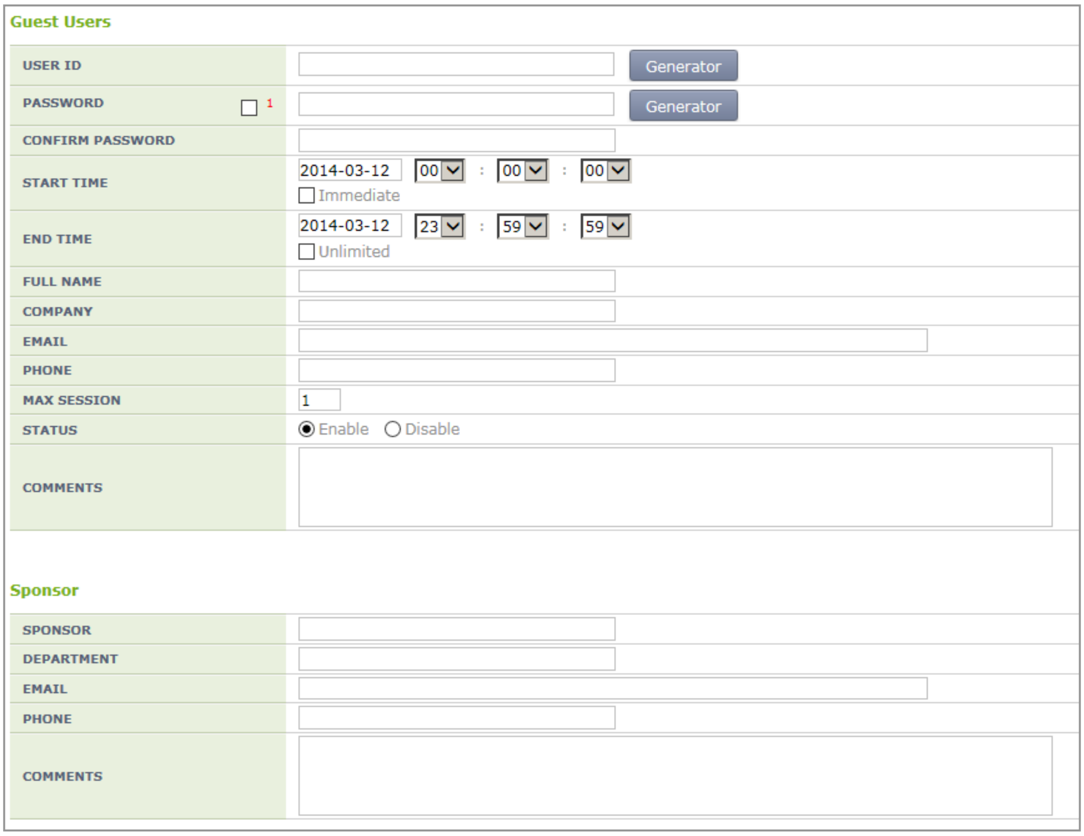
[Retrieving Captive Portal Configuration]

To retrieve the configured environment, execute the following command.

- show security captive-portal summary
- show security captive-portal guest
- show security captive-portal web-auth

Configuration using Web UI

In the menu bar of <**WEC Main window**>, select <**Configuration**> and then select the <**Security**> → <**CaptivePortal**> → <**Guest Users**> menu in the sub-menus.



Guest Users

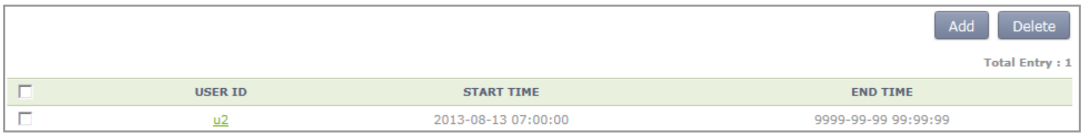
USER ID	Generator
PASSWORD □ 1	Generator
CONFIRM PASSWORD	
START TIME	2014-03-12 00 : 00 : 00 □ Immediate
END TIME	2014-03-12 23 : 59 : 59 □ Unlimited
FULL NAME	
COMPANY	
EMAIL	
PHONE	
MAX SESSION	1
STATUS	● Enable ○ Disable
COMMENTS	

Sponsor

SPONSOR	
DEPARTMENT	
EMAIL	
PHONE	
COMMENTS	

Figure 175. Guest User Configuration Window

Operator can check and delete a guest created in the <**Guest Users**> menu.

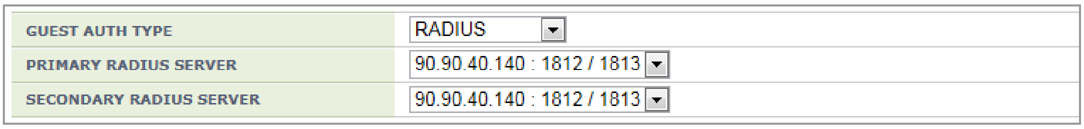


Total Entry : 1

□	USER ID	START TIME	END TIME
□	u2	2013-08-13 07:00:00	9999-99-99 99:99:99

Figure 176. Guest User List Window

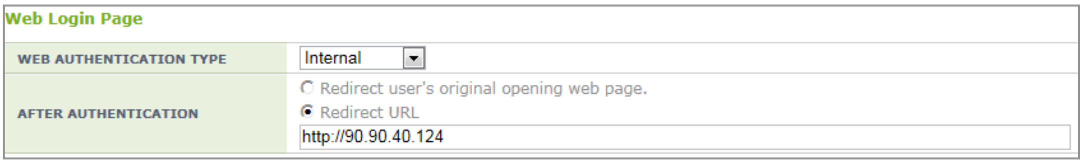
In the <**Guest Users**> menu, operator can select Auth Type and also PRIMARY RADIUS and SECONDARY RADIUS server.



GUEST AUTH TYPE	RADIUS
PRIMARY RADIUS SERVER	90.90.40.140 : 1812 / 1813
SECONDARY RADIUS SERVER	90.90.40.140 : 1812 / 1813

Figure 177. Guest Auth Configuration Window

In the **<CaptivePortal>** → **<Web Authentication>** menu, operator can select web authentication method. Operator can also configure Redirect as the operation after authentication.



Web Login Page

WEB AUTHENTICATION TYPE	Internal
AFTER AUTHENTICATION	○ Redirect user's original opening web page. ● Redirect URL http://90.90.40.124

Figure 178. Web Auth Configuration Window

8.4 WEB Pass-through

The APC provides the WEB Pass through function that transmits a user packet to the redirect URL configured by an operator.

8.4.1 WLAN Security Configuration

Configuration using CLI

1) Go to configure → wlan configuration mode of CLI.

```
WEC8500# configure terminal
WEC8500/configure# wlan 1
```

2) Disable the WLAN.

```
WEC8500/configure/wlan 1# no enable
```

3) Configure the WEB policy (default: disabled).

```
WEC8500/configure/wlan 1/security/layer3# web-policy
```

4) Configure the Pass through function (default: disabled).

```
WEC8500/configure/wlan 1/security/layer3# web-policy pass-through
```

5) Configure the Overriding Redirect URL function (Default: Disabled)

```
WEC8500/configure/wlan 1/security/layer3# redirect-URL-override enable
WEC8500/configure/wlan 1/security/layer3# redirect-URL-override [URL]
```

Parameter	Description
URL	Web server redirect URL

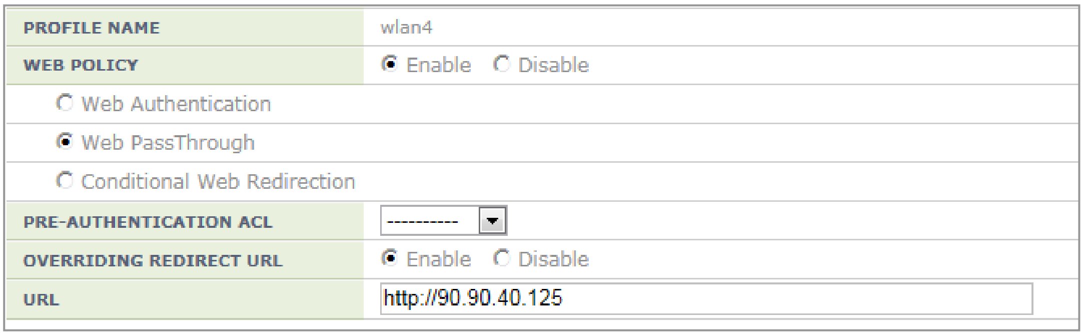
6) Enable the WLAN.

```
WEC8500/configure/wlan 1# enable
```

7) To check the configured environment, use the ‘show wlan security summary’ command.

Configuration using Web UI

In the menu bar of <**WEC Main window**>, select <**Configuration**> and then select the <**WLANs**> menu in the sub-menus. Select a WLAN ID in the WLANs screen and go to the <**L3**> of <**Security**> tab. Enable <**WEB POLICY**> and select Web PassThrough. Enable <**OVERRIDING REDIRECT URL**> and configure <**URL**>.



PROFILE NAME	wlan4
WEB POLICY	● Enable ○ Disable
○ Web Authentication	
● Web PassThrough	
○ Conditional Web Redirection	
PRE-AUTHENTICATION ACL	----------
OVERRIDING REDIRECT URL	● Enable ○ Disable
URL	http://90.90.40.125

Figure 179. Web Pass-through Configuration Window

8.5 NAT and Firewall Configuration

The APC provides the NAT and firewall function to provide stable network to a WLAN user.

8.5.1 Firewall Configuration

Configuration using CLI

[Firewall Configuration]

1) Go to configure mode of CLI.

```
WEC8500# configure terminal
```

2) Configure the accelerator function of a firewall.

```
WEC8500/configure# firewall enable
```

[Firewall Configuration using Access List]

1) Go to configure mode of CLI.

```
WEC8500# configure terminal
```

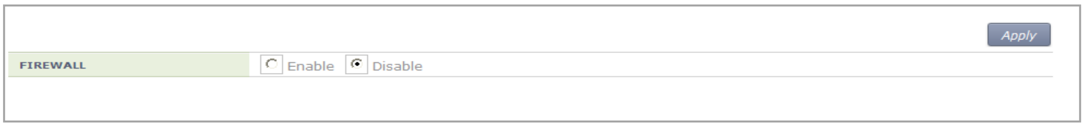
2) Create an access-list.

```
WEC8500/configure# access-list fw fw4 deny tcp any any eq 23
```

3) Configure a firewall to the interface using an access-list.

```
WEC8500/configure# interface vlan1.10
WEC8500/configure/interface vlan1.10# ip access-group fw forward fw4
WEC8500/configure/interface vlan1.10# exit
```

Configuration using Web UI

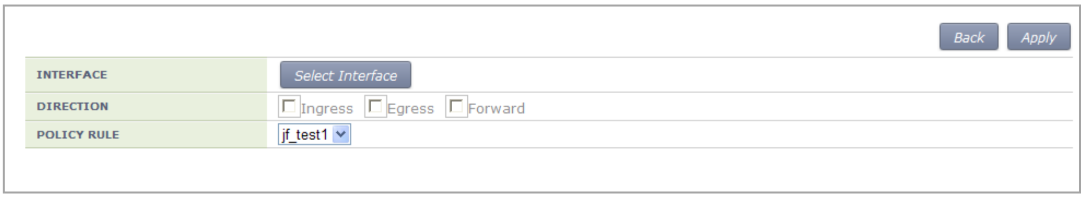


FIREWALL ○ Enable ● Disable

In the menu bar of <**WEC Main window**>, select <**Configuration**> and then select the <**Security**> → <**Firewall**> → <**General**> menu in the sub-menus. You can configure whether to use a firewall.

Figure 180. Firewall configuration (1)

In the menu bar of **<WEC Main window>**, select **<Configuration>** and then select the **<Security>** → **<Firewall>** → **<Interface>** menu in the sub-menus.
You can configure an interface for which a firewall will be applied by clicking the **<Add>** button of Interface window.



INTERFACE	Select Interface
DIRECTION	□ Ingress □ Egress □ Forward
POLICY RULE	jf_test1

Figure 181. Firewall configuration (2)

8.5.2 Access List Configuration

Configuration using CLI

1) Go to configure mode of CLI.

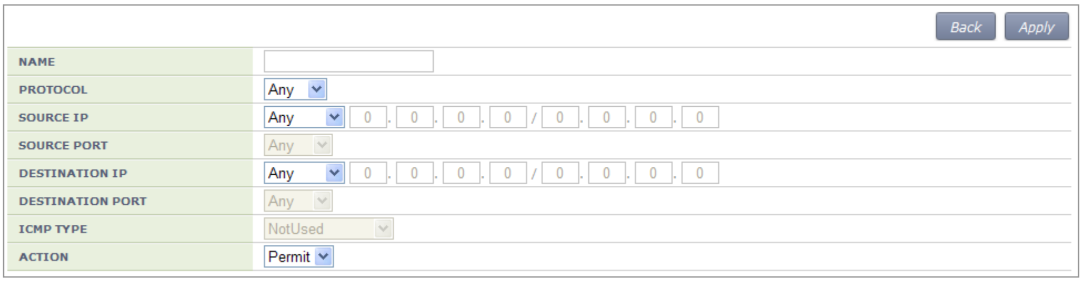
```
WEC8500# configure terminal
WEC8500/configure#
```

2) Create an access-list.
   - access-list fw [ACL_NAME] [ACTION] [SRC_ADDRESS (SRC_PORT)] [DST_ADDRESS (DST_PORT)] [PROTOCOL]

Parameter	Description
ACL_NAME	ACL name to configure
ACTION	Action configuration (deny/permit)
SRC_ADDRESS(SRC_PORT)	Source IP address and port
DST_ADDRESS(DST_PORT)	Destination IP address and port
PROTOCOL	Protocol

Configuration using Web UI

In the menu bar of <**WEC Main window**>, select <**Configuration**> and then select the <**Security**> → <**Firewall**> → <<**Policy**> menu in the sub-menus. Click the <**Add**> button to configure the firewall Policy.



NAME	
PROTOCOL	Any
SOURCE IP	Any 0 . 0 . 0 . 0 / 0 . 0 . 0 . 0
SOURCE PORT	Any
DESTINATION IP	Any 0 . 0 . 0 . 0 / 0 . 0 . 0 . 0
DESTINATION PORT	Any
ICMP TYPE	NotUsed
ACTION	Permit

Figure 182. Access-list configuration

8.5.3 NAT Configuration

Configuration using CLI

[SNAT Configuration using Access List]

To add Source NAT (SNAT) using an access-list, execute the command as follows:

1) Go to configure mode of CLI.

```
WEC8500# configure terminal
```

2) Create an access-list.

```
WEC8500/configure# access-list fw fw1 deny any 10.10.10.10/32 any
```

3) Create a NAT pool.

```
WEC8500/configure# ip nat pool pool1 30.30.30.1 30.30.30.1
255.255.255.0
```

4) Configure a NAT to the interface.

```
WEC8500/configure# interface vlan1.30
WEC8500/configure/interface vlan1.30# ip nat inside
WEC8500/configure/interface vlan1.30#exit
```

5) Add the NAT rule by using access-list and pool.

```
WEC8500/configure# ip nat outside source list fw1 pool pool1
```

[SNAT Configuration using Static IP]

To add SNAT using a static IP, execute the command as follows:

1) Go to configure mode of CLI.

```
WEC8500# configure terminal
```

2) Configure a NAT to the interface.

```
WEC8500/configure# interface vlan1.30
WEC8500/configure/interface vlan1.30#ip nat outside
WEC8500/configure/interface vlan1.30#exit
```

3) Configure a NAT rule using a static IP.

```
WEC8500/configure# ip nat outside source static 10.10.10.10 30.30.30.1
```

[DNAT Configuration using Access List]

To add Destination NAT (DNAT) using an access-list, execute the command as follows:

1) Go to configure mode of CLI.

```
WEC8500# configure terminal
```

2) Create a NAT pool.

```
WEC8500/configure# ip nat pool pool2 10.10.10.10 10.10.10.10
255.255.255.0
```

3) Configure a NAT to the interface.

```
WEC8500/configure# interface vlan1.30
WEC8500/configure/interface vlan1.30#ip nat outside
WEC8500/configure/interface vlan1.30#exit
```

4) Add the NAT rule by using access-list and pool.

```
WEC8500/configure# ip nat outside destination list fw6 pool pool2
```

[DNAT Configuration using Static IP]

To add DNAT using a static IP, execute the command as follows:

1) Go to configure mode of CLI.

```
WEC8500# configure terminal
```

2) Configure a NAT to the interface.

```
WEC8500/configure# interface vlan1.30
WEC8500/configure/interface vlan1.30#ip nat outside
WEC8500/configure/interface vlan1.30#exit
```

3) Configure a NAT rule using a static IP (A port can be also specified for DNAT).

```
WEC8500/configure# ip nat outside destination static tcp 10.10.10.1
4300 30.30.30.2 23
```

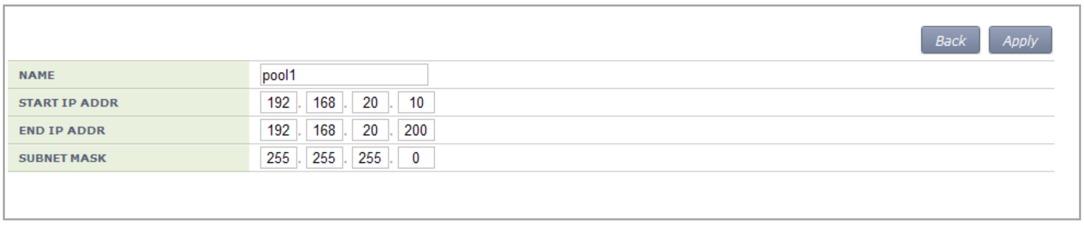
[Checking NAT Configuration]

To check the created NAT, use the following command.

```
WEC8500/configure# show nat
```

Configuration using Web UI

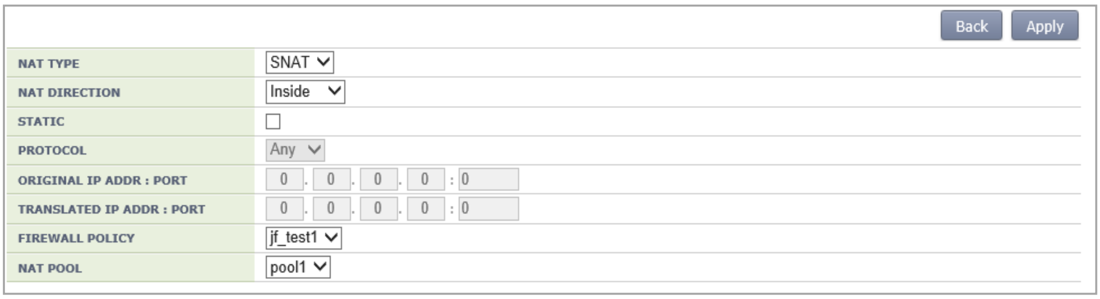
1) In the menu bar of <**WEC Main window**>, select <**Configuration**> and then select the <**Security**> → <**NAT**> → <**Pool**> menu in the sub-menus. **Click the <Add>** button and configure the NAT pool.



NAME	pool1
START IP ADDR	192 . 168 . 20 . 10
END IP ADDR	192 . 168 . 20 . 200
SUBNET MASK	255 . 255 . 255 . 0

Figure 183. NAT configuration (1)

2) Click the <**Add**> button in the Translation Rule window and configure the Translation Rule. Select NAT TYPE as either SNAT or DANT. Select STATIC checkbox to configure Static and configure the values of Original IP Addr: Port and Translated IP Addr: Port.



NAT TYPE	SNAT
NAT DIRECTION	Inside
STATIC	□
PROTOCOL	Any
ORIGINAL IP ADDR : PORT	0 . 0 . 0 . 0 : 0
TRANSLATED IP ADDR : PORT	0 . 0 . 0 . 0 : 0
FIREWALL POLICY	jf_test1
NAT POOL	pool1

Figure 184. NAT configuration (2)

NOTE

To proceed with NAT configuration, you must create an access list first.

8.6 MAC Filter

The W-EP wireless LAN system provides the MAC filter function. A user may experience connection restriction due to MAC filtering when connecting to a specific WLAN (SSID).

Configuration using CLI

To configure a MAC list for connection control by the MAC filter, execute the command as follows:

1) Go to configure → security configuration mode of CLI.

```
WEC8500# configure terminal
WEC8500/configure# security
```

2) Creates a MAC filter list.

```
WEC8500/configure/security# mac-filter [ID]
```

Parameter	Description
ID	MAC filter list table ID (range: 1-20)

3) Configure the filtering policy.

```
WEC8500/configure/security/mac-filter 1# policy [POLICY]
```

Parameter	Description
POLICY	Table policy of MAC filtering list

4) Configure a MAC entry.

```
WEC8500/configure/security/mac-filter 1# mac [MAC_ADDRESS]
```

Parameter	Description
MAC_ADDRESS	MAC address (XX:XX:XX:XX:XX:XX format)

5) Specify the MAC filter ID that is configured in the WLAN to which a MAC filter will be applied.

```
WEC8500/configure/wlan 1/security# mac-filter <MAC_FILTER_ID>
```

Parameter	Description
MAC_FILTER_ID	MAC FILTER ID (range: 1-20)

6) You can check the configured information below.

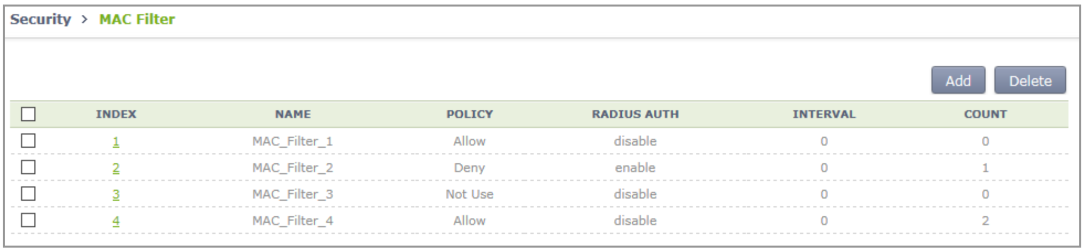
```
show security mac-filter summary
```

```
WEC8500# show security mac-filter detail
```

Configuration using Web UI

In the menu bar of <**WEC Main window**>, select <**Configuration**> and then select the <**Security**> → <**MAC Filter**> menu in the sub-menus.

You can create a MAC filter table for station access control by clicking the <**Add**> button.

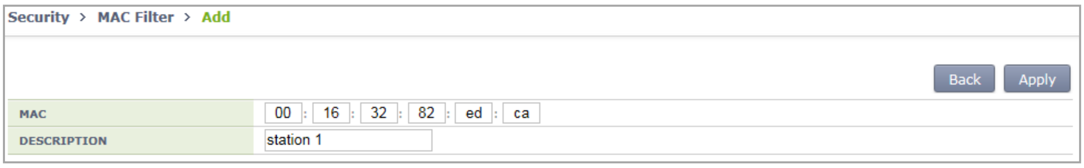


□	INDEX	NAME	POLICY	RADIUS AUTH	INTERVAL	COUNT
□	1	MAC_Filter_1	Allow	disable	0	0
□	2	MAC_Filter_2	Deny	enable	0	1
□	3	MAC_Filter_3	Not Use	disable	0	0
□	4	MAC_Filter_4	Allow	disable	0	2

Figure 185. MAC configuration

The procedure for MAC entry configuration is given below.

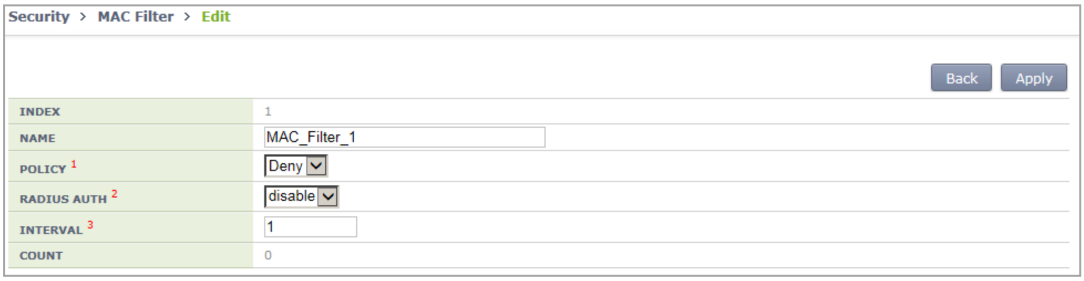
1) In the MAC Filter initial window, select an INDEX item to switch to the Edit screen and then click the <**Add**> button to configure a MAC entry.



MAC	00 : 16 : 32 : 82 : ed : ca
DESCRIPTION	station 1

Figure 186. MAC entry configuration window(1)

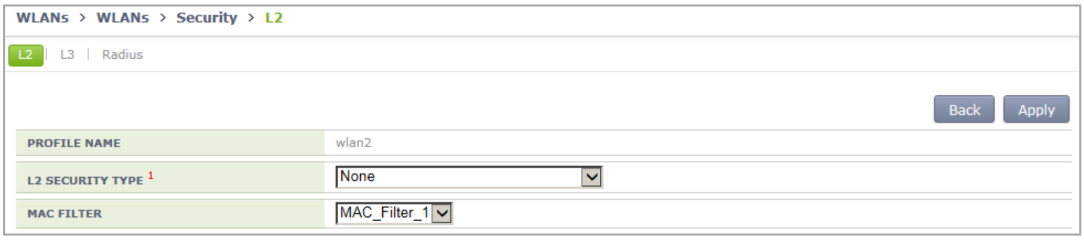
2) Configure the policy in the Edit configuration screen by selecting the index of MAC filter list.



INDEX	1
NAME	MAC_Filter_1
POLICY [1]	Deny
RADIUS AUTH [2]	disable
INTERVAL [3]	1
COUNT	0

Figure 187. MAC entry configuration(2)

3) Select a WLAN for which the MAC filter will be applied. Check a MAC FILTER ID to apply in the Security > L2 configuration screen.
To apply the configuration, click the <**Apply**> button.



PROFILE NAME	wlan2
L2 SECURITY TYPE [1]	None
MAC FILTER	MAC_Filter_1

Figure 188. MAC entry configuration(3)

8.7 Operator Authentication through Interoperation with TACACS+ Server

A W-EP wireless LAN system provides an operator authentication function by interoperating with an external TACACS+ server.

8.7.1 Configuring External TACACS+ Server

A W-EP wireless LAN system provides an operator authentication function by interoperating with an external TACACS+ server and the procedure detailed below is carried out for interoperation with a TACACS+ server.

8.7.1.1 Basic Settings

The default configuration of the TACACS+ server is as follows:

Configuration using CLI

1) Go to configure → security → tacacs configuration mode of CLI.

```
WEC8500# configure terminal
WEC8500/configure# security
WEC8500/configure/security# tacacs 1
WEC8500/configure/security/tacacs 1#
```

2) Configure the IP address of the TACACS+ server.

```
WEC8500/configure/security/tacacs 1# server-ip [IP_ADDRESS]
```

Parameter	Description
IP_ADDRESS	IP address of the TACACS+ server

3) Set the public key of the TACACS+ server.

```
WEC8500/configure/security/tacacs 1# shared-secret [KEY_STRING]
```

Parameter	Description
KEY_STRING	Public key of the TACACS+ server

4) Configure the port number of the TACACS+ server.

```
WEC8500/configure/security/tacacs 1# server-port [PORT_NUMBER]
```

Parameter	Description
PORT_NUMBER	Port number of the TACACS+ server (range: 1-65,535, default value: 49)

5) Configure the items related to retransmissions in TACACS+ communications. You can use default values without changing configuration.

```
WEC8500/configure/security/tacacs 1# retransmit-interval
[RETRY_INTERVAL]
WEC8500/configure/security/tacacs 1# retransmit-count [FO_RETRY_COUNT]
```

Parameter	Description
RETRY_INTERVAL	Retransmission interval for a TACACS+ message (unit: seconds, range: 1-5, default value: 3)
FO_RETRY_COUNT	Maximum message retransmission count before a TACACS+ server failover is attempted (range: 0-3, default value: 2)

6) If necessary, configure the source IP address of the TACACS+ message.

```
WEC8500/configure/security/tacacs 1# source-ip [IP_ADDRESS]
```

Parameter	Description
IP_ADDRESS	Source IP address of the TACACS+ message Note: it must be one of the IP addresses configured in the W-EP wireless LAN system.

7) Configure whether to transfer packets to the TACACS+ server. You can use default values without changing configuration.

```
WEC8500/configure/security/tacacs 1# status [STATUS]
```

Parameter	Description
STATUS	Status indicating whether packets are transferred to the TACACS+ server (default value: enable)

8) Exit TACACS+ server configuration and then security configuration mode.

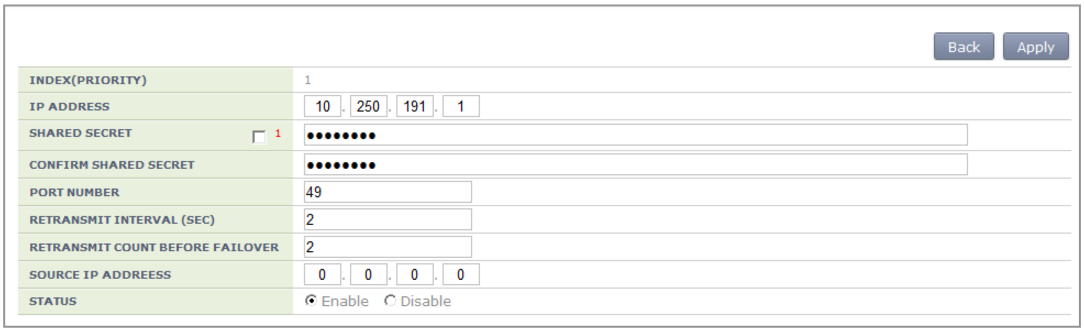
```
WEC8500/configure/security/tacacs 1# exit
WEC8500/configure/security# exit
```

9) You can view configuration information by using the ‘show security tacacs server config’ and ‘show security tacacs server detail [SERVER ID]’ commands.

Configuration using Web UI

In the menu bar of <**WEC Main Window**>, select <**Configuration**>, and then select <**Security**> → <**AAA**> → <**TACACS+**> in the submenus.

If you click the <**Add**> button in the TACACS+ initial window, you can add a TACACS+ server.
The server addition window is shown below.



INDEX(PRIORITY)	1
IP ADDRESS	10 . 250 . 191 . 1
SHARED SECRET □ 1	••••••••
CONFIRM SHARED SECRET	••••••••
PORT NUMBER	49
RETRANSMIT INTERVAL (SEC)	2
RETRANSMIT COUNT BEFORE FAILOVER	2
SOURCE IP ADDREESS	0 . 0 . 0 . 0
STATUS	● Enable ○ Disable

Figure 189. TTACACS+ Server Configuration Window

Item	Description
INDEX (PRIORITY)	ID that distinguishes TACACS+ server configurations
IP ADDRESS	IP address of the TACACS+ server
SHARED SECRET	Public key of the TACACS+ server
CONFIRM SHARED SECRET	Re-enters the key for TACACS+ server communications for confirmation
PORT NUMBER	Communication port number of the TACACS+ server (range: 1-65,535, default value: 49)
RETRANSMIT INTERVAL	Retransmission interval for a TACACS+ message (range: 1-5, default value: 2, unit: seconds)
RETRANSMIT COUNT BEFORE FAILOVER	Maximum message retransmission count before a TACACS+ server failover is attempted (range: 0-3, default value: 2)
SOURCE IP ADDRESS	Source IP address of the TACACS+ message - Note: it must be one of the IP addresses configured in the W-EP wireless LAN system.
STATUS	Status indicating whether packets are transferred to the TACACS+ server (default value: enable)

8.7.2 Configuring Authentication Type of Operator Account

The steps for configuring the authentication type of the operator account are as follows:

Configuration using CLI

1) Go to configure mode of CLI.

```
WEC8500# configure terminal
WEC8500/configure#
```

2) Configure the type of operator account authentication.

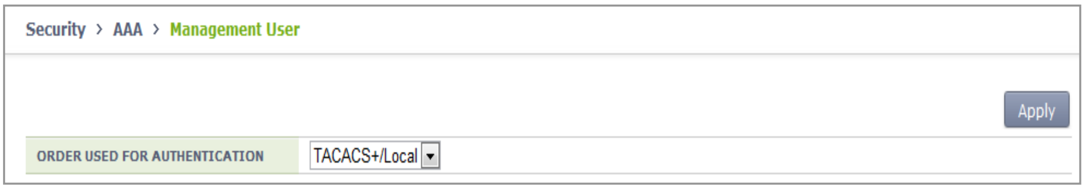
```
WEC8500/configure# mgmt-user auth-type [AUTH_TYPE]
```

Parameter	Description
AUTH_TYPE	Authentication type of the operator account (default value: local) - local: Authentication is performed using the database stored inside. - tacacs: Authentication is performed using the TACACS+ server. - local-tacacs: Authentication is performed using the database stored inside first, and, failing that, an authentication request is transmitted to the TACACS+ server. - tacacs-local: An authentication request is transmitted to the TACACS+ server first, and, failing that, authentication is performed using the DB stored inside.

3) You can view the configuration information by using the ‘show mgmt-users auth-type’ command.

Configuration using Web UI

In the menu bar of <**WEC Main Window**>, select <**Configuration**>, and then select <**Security**> → <**AAA**> → <**Management User**> in the submenus.



ORDER USED FOR AUTHENTICATION: TACACS+/Local

Figure 190. Operator Account Authentication Type Configuration Window

CHAPTER 9. IP Application

In this chapter, the IP application functions available in the APC and each configuration method are described.

9.1 DNS

The DNS is a network service that interprets a domain or host name into an IP address.
The APC gets DNS information from a DNS server and provides the DNS relay function that relays the DNS server and a client. If a wireless terminal connected to the APC configures the APC as a DNS server, it can receive the DNS service.
If a DNS server is connected to the APC and a DNS proxy is configured, a station connected to the APC can receive the DNS service by configuring the APC as a DNS server.

9.1.1 DNS Client Configuration

Configuration using CLI

1) Go to configure mode of CLI.

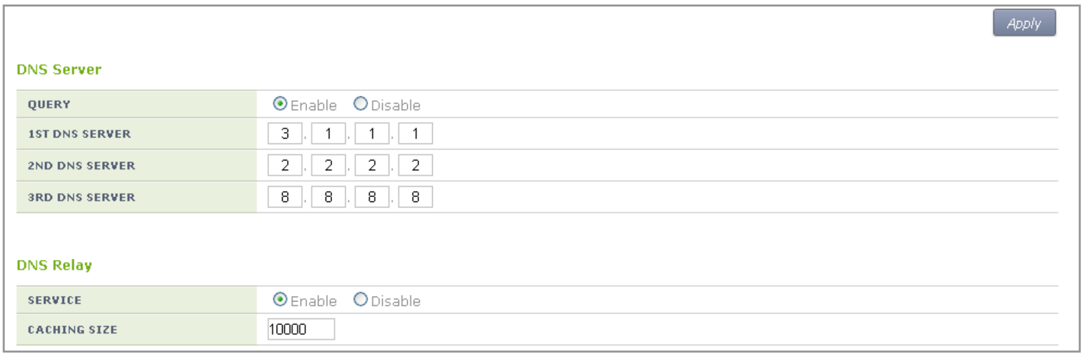
```
WEC8500# configure terminal
```

2) Configure a DNS client.
   - ip dns client enable: Enable
   - no ip dns client enable: Disable

3) Configure a DNS server to which DNS will be requested. You can enter maximum 3 DNS server addresses.
   - ip dns name-server [A.B.C.D]: Configures a DNS server.
   - no ip dns name-server [A.B.C.D]: Deletes a configured DNS server.
   - no ip dns name-server all: Deletes all the DNS servers.

Configuration using Web UI

In the menu bar of **<WEC Main window>**, select **<Configuration>** and then select the <**DNS>** menu in the sub-menus.



DNS Server

QUERY	● Enable ○ Disable
1ST DNS SERVER	3 . 1 . 1 . 1
2ND DNS SERVER	2 . 2 . 2 . 2
3RD DNS SERVER	8 . 8 . 8 . 8

DNS Relay

SERVICE	● Enable ○ Disable
CACHING SIZE	10000

Figure 191. DNS client

You can enable or disable a DNS client using the QUERY of a DNS SERVER item.
In the 1ST DNS SERVER, 2ND DNS SERVER, and 3RD DNS SERVER boxes, you can configure 3 name servers.

9.1.2 DNS Proxy Configuration

You can configure the DNS relay function or a cache for relay. The cache is a temporary space where the APC saves the DNS information obtained from a DNS server.
You can configure maximum number of entries as 10000-100000. The DNS relay is related to the DNS client configuration. If you disable the DNS client function or delete all the name servers, the DNS relay function is not working.

Configuration using CLI

1) Go to configure mode of CLI.

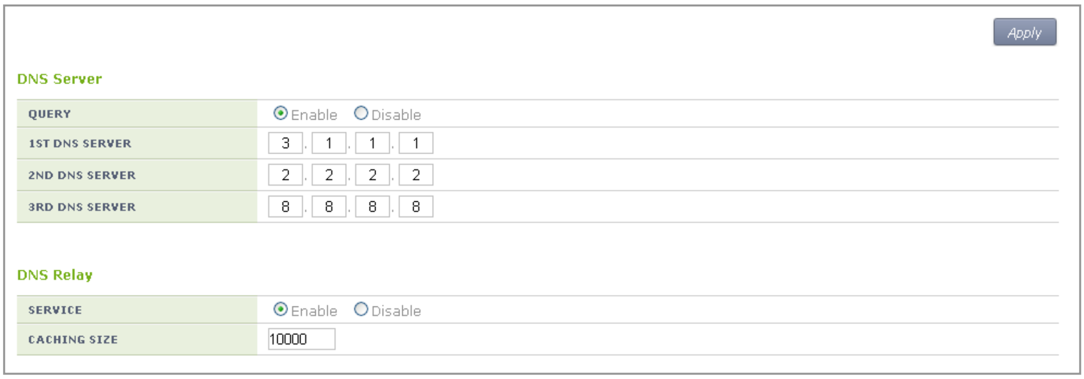
```
WEC8500# configure terminal
```

2) Configure a DNS relay. Configure the cache to a default, i.e. 10000.
   - ip dns relay enable: Enables a relay.
   - no ip dns relay enable: Disables a relay.

3) To change cache configuration, enter as follows:
   - ip dns relay enable cache: Configures a DNS relay and configures the cache to a default, i.e. 10000.
   - ip dns relay enable cache 20000: Configures a DNS relay and configures the cache to 20000.
   - ip dns relay enable no-cache: Configures a DNS relay and disables the cache settings.

Configuration using Web UI

In the menu bar of **<WEC Main window>**, select <**Configuration>** and then select the <**DNS>** menu in the sub-menus.



DNS Server

QUERY	● Enable ○ Disable
1ST DNS SERVER	3 . 1 . 1 . 1
2ND DNS SERVER	2 . 2 . 2 . 2
3RD DNS SERVER	8 . 8 . 8 . 8

DNS Relay

SERVICE	● Enable ○ Disable
CACHING SIZE	10000

Figure 192. DNS proxy

The DNS Relay item supports DNS Proxy configuration. In the SERVICE, you can enable or disable a DNS proxy and configure the cache size of the DNS proxy in the CACHING SIZE. If the cache size is 0, disable the cache.

9.2 NTP

The Network Time Protocol (NTP) is a protocol used to receive time from a configured server and synchronize the local time.
The APC can operate as a NTP server and a client. If you configure the APC as a NTP client, it receives the Coordinated Universal Time (UTC) information from the configured NTP server and synchronizes the local time. In addition, if you configure the APC as a NTP server, it transmits a local time when it receives a NTP request from a NTP client.

Configuration using CLI

[Configuring NTP Client]

The time server that is referred to when the APC is working as a NTP client can be used based on a domain name and IP address. But, if it is working based on a domain name, there must be a configured DNS server.

1) Go to configure mode of CLI.

```
WEC8500# configure terminal
```

2) Enable or disable a NTP client.
   - ntp client enable: Enable
   - no ntp client enable: Disable

3) Configure the interval of a NTP client.
   - ntp client interval [INTERVAL]: Configures an interval.
   - no ntp client interval: Disables an interval.

Parameter	Description
INTERVAL	Interval (range: 3-14)

4) Configure a server that a NTP client will refer to.

[Configuring based on a domain name]

Enables or disables.

- ntp client server-addr hostname <WORD>: Enable
- no ntp client server-addr hostname <WORD>: Disable

Configure the index of a server that a NTP client will refer to. (Use a default value 1 if it is not configured.)

- ntp client server-addr hostname <WORD> index [INDEX]: Enable
- no ntp client server-addr hostname <WORD> index [INDEX]: Disable

Parameter	Description
INDEX	Server index (range: 1-5)

Configure the version of a server that a NTP client will refer to. (Use a default value 1 if it is not configured.)

- ntp client server-addr hostname <WORD> version [1-4]: Enable
- no ntp client server-addr hostname <WORD> version [1-4]: Disable

[Configuring based on IP address]

Enable or disable.

- ntp client server-addr ip <A.B.C.D>: Enable
- no ntp client server-addr ip <A.B.C.D>: Disable

Configure the index of a server that a NTP client will refer to. (Use a default value 1 if it is not configured.)

- ntp client server-addr ip <A.B.C.D> index [1-5]: Enable
- no ntp client server-addr ip <A.B.C.D> index [1-5]: Disable

Configure the version of a server that a NTP client will refer to. (Use a default value 1 if it is not configured.)

- ntp client server-addr ip <A.B.C.D> version [1-4]
- no ntp client server-addr ip <A.B.C.D> version [1-4]

You can proceed with configurations simultaneously as shown below.

- ntp client server-addr hostname <WORD> index [1-5] version [1-4]
- ntp client server-addr hostname <WORD> version [1-4] index [1-5]
- ntp client server-addr ip <A.B.C.D> index [1-5] version [1-4]
- ntp client server-addr ip <A.B.C.D> version [1-4] index [1-5]
- no ntp client server-addr hostname <WORD> index [1-5] version [1-4]
- no ntp client server-addr hostname <WORD> version [1-4] index [1-5]
- no ntp client server-addr ip <A.B.C.D> index [1-5] version [1-4]
- no ntp client server-addr ip <A.B.C.D> version [1-4] index [1-5]

[NTP Server Configuration]

The NTP server configuration is as follows:

1) Go to configure mode of CLI.

```
WEC8500# configure terminal
```

2) Configure a NTP server.
   - ntp server enable: Configures a NTP server.
   - no ntp server enable: Disables a NTP server.

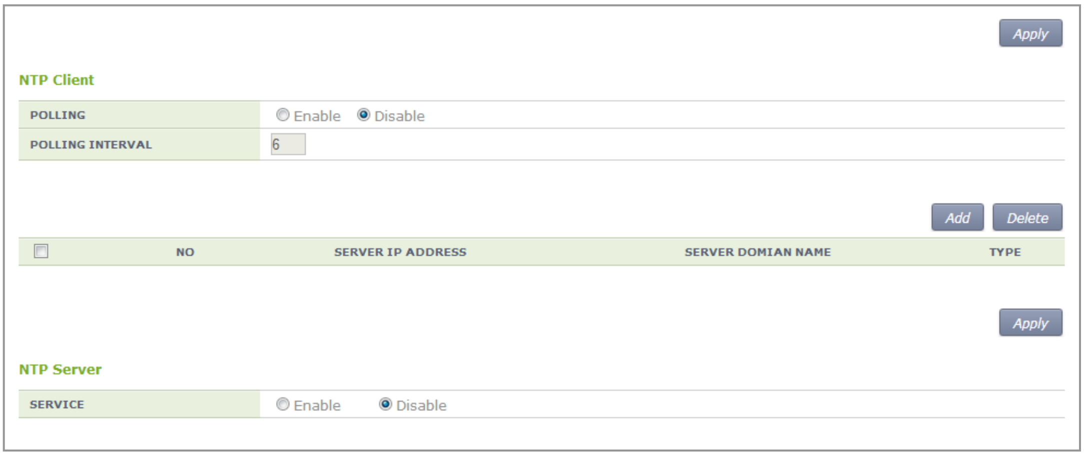
[Checking NTP Configuration Status]

To check the status of a NTP client or server, enter the ‘show ntp’ command.

Configuration using Web UI

In the menu bar of <**WEC Main window**>, select <**Configuration**> and then select the <**NTP**> menu in the sub-menus.

The NTP initial window is shown below.



NTP Client

POLLING	○ Enable ● Disable
POLLING INTERVAL	6

□	NO	SERVER IP ADDRESS	SERVER DOMIAN NAME	TYPE

NTP Server

SERVICE	○ Enable ● Disable

Figure 193. NTP client configuration

The Enable/Disable of a NTP server can be performed using a radio box.

You can configure polling interval enable/disable of a NTP client and also configure the polling interval during enabling. The range of polling interval is 3-14.

Click the <**Add**> or <**Delete**> button to add or delete a NTP proxy server. Click the <**Add**> button to configure a specific ‘Server IP’ or ‘Server DOMAIN NAME’ that will be used by a NTP proxy.

9.3 FTP/sFTP

The FTP is a network service for file transmission. The APC support the client and server function for FTP and sFTP (Secure FTP).

Configuration using CLI

[SFTP Server Configuration]

The secure FTP server configuration is as follows:

1) Go to configure mode of CLI.

```
WEC8500# configure terminal
```

2) Enable or disable the sFTP server.
   - sftp-server enable: Enable
   - no sftp-server enable: Disable

3) Enter as follows to change a user's ID and password.
   - sftp-server chguser [ID] [PASSWORD]

Parameter	Description
ID	User ID of a server
PASSWORD	User password of a server

4) To check the status of sFTP server, enter the 'show sftp-server' command.

[FTP Server Configuration]

1) Go to configure mode of CLI.

```
WEC8500# configure terminal
```

2) Enable or disable the sFTP server.
   - ftp-server enable: Enable
   - no ftp-server enable: Disable

3) Enter as follows to change a user's ID and password.
   - ftp-server chguser [ID] [PASSWORD]

Parameter	Description
ID	User ID of a server
PASSWORD	User password of a server

4) To change the idle timeout, enter the command below. The unit of timeout is minutes and the default value is 15 minutes.
   - ftp-server idle-timeout [timeout]

5) To check the status of FTP server, enter the ‘show ftp-server’ command.

[Using as Client]

Using the following commands, you can download or upload a file using a FTP/sFTP client.

- file download
- file upload

A usage example is provided below.

- File download using a sFTP client

```
WEC8500# file download samsung Samsung 90.90.21.108 wec8500 wec8500
sftp
```

- File upload using a sFTP client

```
WEC8500# file upload samsung Samsung 90.90.21.108 wec8500 wec8500 sftp
```

- File download using a FTP client

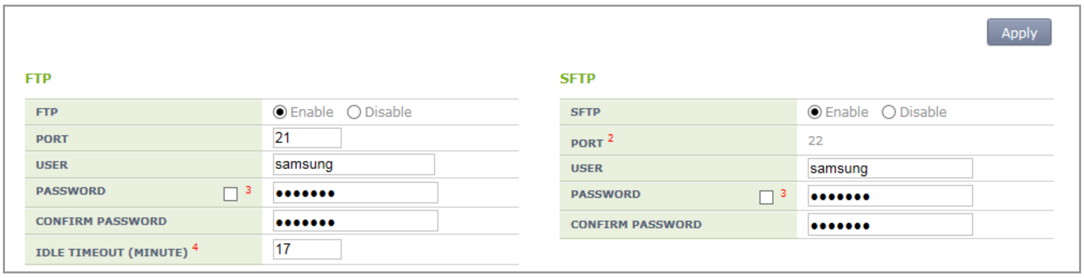
```
WEC8500# file download samsung Samsung 90.90.21.108 wec8500 wec8500
```

- File upload using a FTP client

```
WEC8500# file upload samsung Samsung 90.90.21.108 wec8500 wec8500
```

Configuration using Web UI

To configure the FTP/SFTP server configuration, in the menu bar of **<WEC Main window>**, select **<Administrator>** and then select the **<FTP-SFTP>** menu in the sub-menus.



FTP

FTP	● Enable ○ Disable
PORT	21
USER	samsung
PASSWORD □ [3]	•••••••
CONFIRM PASSWORD	•••••••
IDLE TIMEOUT (MINUTE) [4]	17

SFTP

SFTP	● Enable ○ Disable
PORT [2]	22
USER	samsung
PASSWORD □ [3]	•••••••
CONFIRM PASSWORD	•••••••

Figure 194. FTP/SFTP server configuration

The FTP and SFTP can be configured using the Enable/Disable radio box.
For FTP, you can configure a port number that will be used for FTP by using ‘PORT’ and can change the user name and password of a FTP server by entering ‘USER’, ‘PASSWORD’, or ‘CONFIRM PASSWORD’. Enter an idle timeout value in ‘IDLE TIMEOUT’.
Also for SFTP, you can change the user name and password of a SFTP server by entering ‘USER’, ‘PASSWORD’, or ‘CONFIRM PASSWORD’.

9.4 Telnet/SSH

The telnet or Secure Shell (SSH) is an Internet protocol that helps login to another computer in a network or connects to a virtual remote system. Using telnet or SSH, you can connect to another computer while staying at a current computer.
Because the SSH can access a remote system and transmit an encrypted message by using public key-based encryption method, it provides better security.

Configuration using CLI

[Telnet Server Configuration]
The Telnet server configuration is as follows:

1) Go to configure mode of CLI.

```
WEC8500# configure terminal
```

2) Enable or disable the telnet service. If you configure the telnet service, you can use the APC as a telnet server.
   - telnet-server enable: Enable
   - no telnet-server enable: Disable

3) If you configure the telnet service, specify the port number of telnet server.
   - telnet-server port [PORT_NUMBER]

Parameter	Description
PORT_NUMBER	Port number to configure (range: 1-65535)

[SSH Server Configuration]
The SSH server configuration is as follows:

1) Go to configure mode of CLI.

```
WEC8500# configure terminal
```

2) Enable or disable the SSH server.
   - ssh-server enable: Enable
   - no ssh-server enable: Disable

3) Specify the port number of SSH server.
   - ssh-server port [PORT_NUMBER]

Parameter	Description
PORT_NUMBER	Port number to configure (range: 1-65535)

[Checking Server Configuration Status]

To check the status of telnet or ssh server, enter the following command. You can retrieve the configured port number as well as server status.

- show ssh-server: Retrieves the status of SSH server
- show telnet-server: Retrieves the status of telnet server

[Using as Client]

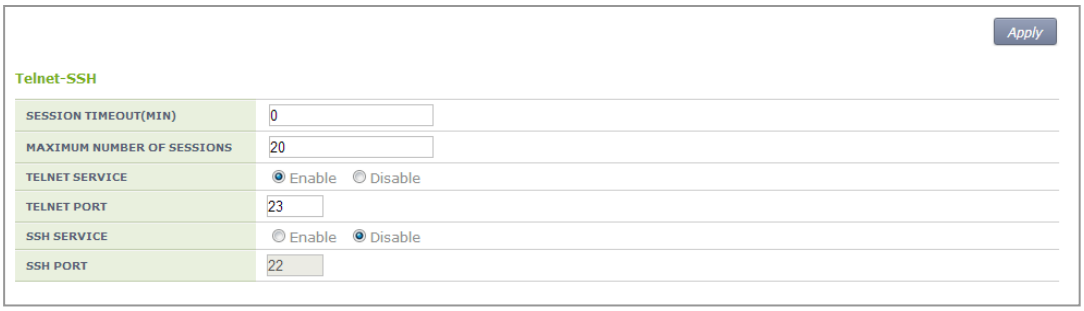
By using the APC as a telnet or SSH client, you can connect to a server.
Enter as follows in CLI.

- telnet [IP_ADDRESS] [PORT_NUMBER]
- ssh [IP_ADDRESS] [ID] [PORT_NUMBER]

Parameter	Description
IP_ADDRESS	IP address or domain name of a server to connect
ID	login ID
PORT_NUMBER	Port number (range: 1-65535) If the port number is not entered, its default is shown below. - telnet: 23 - ssh: 22

Configuration using Web UI

To configure the Telnet/SSH server configuration, in the menu bar of <**WEC Main window**>, select <**Administrator**> and then select the <**Telnet-SSH**> menu in the sub-menus.



Telnet-SSH

SESSION TIMEOUT(MIN)	0
MAXIMUM NUMBER OF SESSIONS	20
TELNET SERVICE	● Enable ○ Disable
TELNET PORT	23
SSH SERVICE	○ Enable ● Disable
SSH PORT	22

Figure 195. Telnet/SSH server configuration

You can configure the service by using the Enable/Disable radio box of ‘TELNET SERVICE’ or ‘SSH SERVICE’.
You can configure the port number of service by using ‘TELNET PORT’ or ‘SSH PORT’.
By using ‘SESSION TIMEOUT’, you can configure the session timeout of TELNET or SSH in min. and can also configure maximum number of sessions by using ‘MAXIMUM NUMBER OF SESSIONS’.

9.5 Utilities

The APC provides the functions such as ping, traceroute, or tcpdump to check a network and its problems.

[ping]
Used to check network connection status.

- ping [IP_ADDRESS]

[traceroute]
Used to check a route path.

- traceroute [IP_ADDRESS]

[tcpdump]
Used to check the packet of a specific interface.

- tcpdump [INTERFACE_NAME]

CHAPTER 10. System Management

In this chapter, the various functions used by an operator to manage the system and troubleshooting method are described. In addition, the configurations required for system operation such as system configuration management, resource management, alarm management, and package management, etc. and checking methods are described.

10.1 SNMP Configuration

10.1.1 SNMP Community

To use an external management server or to manage the system through a web server after initial system installation, you must configure the SNMP community using CLI.
When creating the SNMP community, you can restrict configuration privilege by allocating the access right such as read-only or read-write and can also restrict an IP to connect.
You can configure maximum 10 SNMP communities.

Configuration using CLI

To add a SNMP community, execute the command as follows:

1) Go to configure mode of CLI.

```
WEC8500# configure terminal
WEC8500/configure#
```

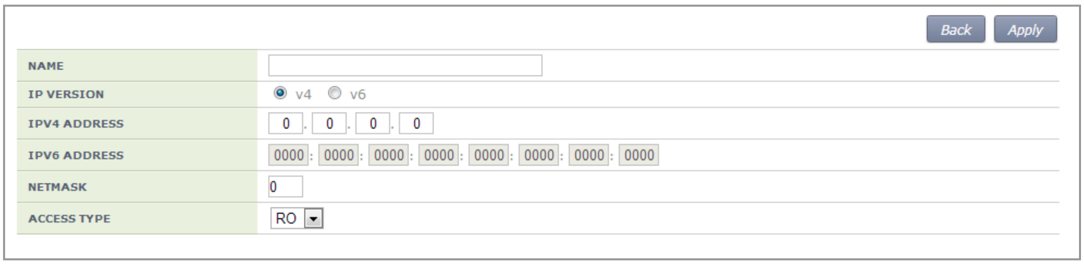
2) Use the ‘snmp community’ command to add a SNMP community.
   - snmp community [COMMUNITY_NAME] [ACCESS] [IP_VERSION] [IP_ADDRESS] [NET MAST]

Parameter	Description
COMMUNITY_NAME	Name of a community to add
ACCESS	Access privilege (rw/ro) - rw: read-write privilege - ro: read-only privilege
IP_VERSION	IP address version type (v4/v6)
IP_ADDRESS, NETMAST	IP address area that can be connected

3) To check the created SNMP community, use the ‘show snmp community’ command.

Configuration using Web UI

In the menu bar of <**WEC Main window**>, select <**Administrator**> and then select the <**SNMP**> → <**Community**> menu in the sub-menus. When you click the <**Add**> button in the Community window, the community creation window is displayed. When you enter a configuration value and click the <**Apply**> button, the configuration is applied.



NAME	
IP VERSION	● v4 ○ v6
IPV4 ADDRESS	0 . 0 . 0 . 0
IPV6 ADDRESS	0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000
NETMASK	0
ACCESS TYPE	RO

Figure 196. Adding SNMP community

10.1.2 SNMP Trap

All the alarms of the APC system are basically transmitted to outside through the SNMP trap. Therefore, to receive a system alarm from an external management server, the server address must be registered as a trap target. The trap supports v1/v2.

Configuration using CLI

To add a SNMP trap target, execute the command as follows:

1) Go to configure mode of CLI.

```
WEC8500# configure terminal
WEC8500/configure#
```

2) Add a SNMP trap target.
   - snmp trap [TRAP_VERSION] [COMMUNITY_NAME] [IP_VERSION] [IP_ADDRESS] [PORT_NUMBER]

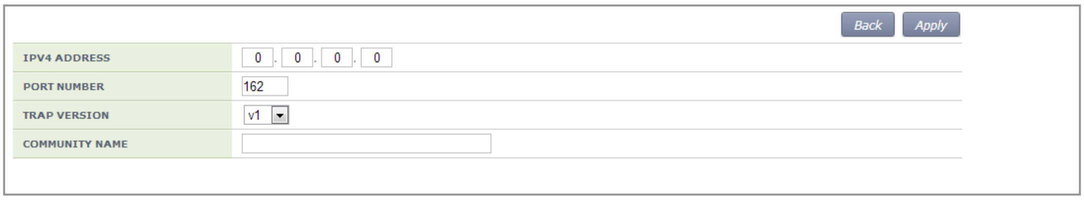
Parameter	Description
TRAP_VERSION	Trap version (v1/v2)
COMMUNITY_NAME	Name of a community to be transmitted
IP_VERSION	IP address type (v4/v6)
IP_ADDRESS	IP address to which a trap will be transmitted
PORT_NUMBER	Port number to which a trap will be transmitted (default: 162)

3) To check the added trap target, use the 'show snmp trap' command.

Configuration using Web UI

In the menu bar of **<WEC Main window>**, select **<Administrator>** and then select the **<SNMP>** → **<Trap Receiver>** menu in the sub-menus.

When you click the **<Add>** button in the Trap Receiver window, the trap creation window is displayed. When you enter a configuration value and click the **<Apply>** button, the configuration is applied.



IPV4 ADDRESS	0 . 0 . 0 . 0
PORT NUMBER	162
TRAP VERSION	v1
COMMUNITY NAME	

Figure 197. SNMP trap configuration

10.2 System Management

10.2.1 Retrieving System Information

Retrieving with CLI

By using the ‘show system info’ command, you can check the system configuration information of the APC system such as version information, memory information, disk information, temperature sensor and fan status, etc.

The execution results of the command in WEC8500 are as follows:

```
WEC8500/configure# show system info
 -----------------------------------------------------
 Item                        System Info
 -----------------------------------------------------
 System Info :
  model type                 WEC8500
  system description         Samsung AP Controller
  board version              0.1
  cpld version               0.5
  system mac address         00:7e:37:00:1e:70
  system total memory        16046580 KBytes
  system total disk          13520032 KBytes

 Temperature Sensor Status   :
  cpu upside sensor          OK
  cpu downside sensor        OK
  board sensor               OK

 Fan Status :
  fan[0]                     OK
  fan[1]                     OK
  fan[2]                     OK
  fan[3]                     OK

 Power Supply Status :
  Power Supply[0]            Equipped
   Status                    OK
  Power Supply[1]            Not Equipped
   Status                    -
 -----------------------------------------------------
```

The execution results of the command in WEC8050 are as follows:

```
WEC8050# show system info
 -----------------------------------------------------
 Item                       System Info
 -----------------------------------------------------
 System Info :
  model type                WEC8050
  system description        Samsung AP Controller
  board version             0.0
  cpld version              0.1
  serial number
  system mac address        00:7e:37:00:21:d4
  system total memory       4855272 KBytes
  system total disk         12191593 KBytes

 Temperature Sensor Status :
  CPU sensor1               OK
  CPU sensor2               OK

 Fan Status :
  fan[0]                    OK
  fan[1]                    OK
 -----------------------------------------------------
```

The descriptions of the output parameters are as follows:

[System Info]

Parameter	Description
model type	Product model name
system description	Product type
board version	Hardware version of a board
cpld version	System cpld version
system mac address	System MAC address
system total memory	System total memory capacity
system total disk	System total disk capacity

[Temperature Sensor Status]

Parameter	Description
cpu upside sensor	CPU upside sensor status (OK, NOK)
cpu downside sensor	CPU downside sensor status (OK, NOK)
board sensor	Board sensor status (OK, NOK)

[Fan Status]

For WEC8500:

Parameter	Description
Fan [0]~[3]	Fan operation status (OK, NOK)

For WEC8050:

Parameter	Description
Fan [0]~[1]	Fan operation status (OK, NOK)

[Power Supply Status]

The WEC8500 has dual detachable power module as shown below.

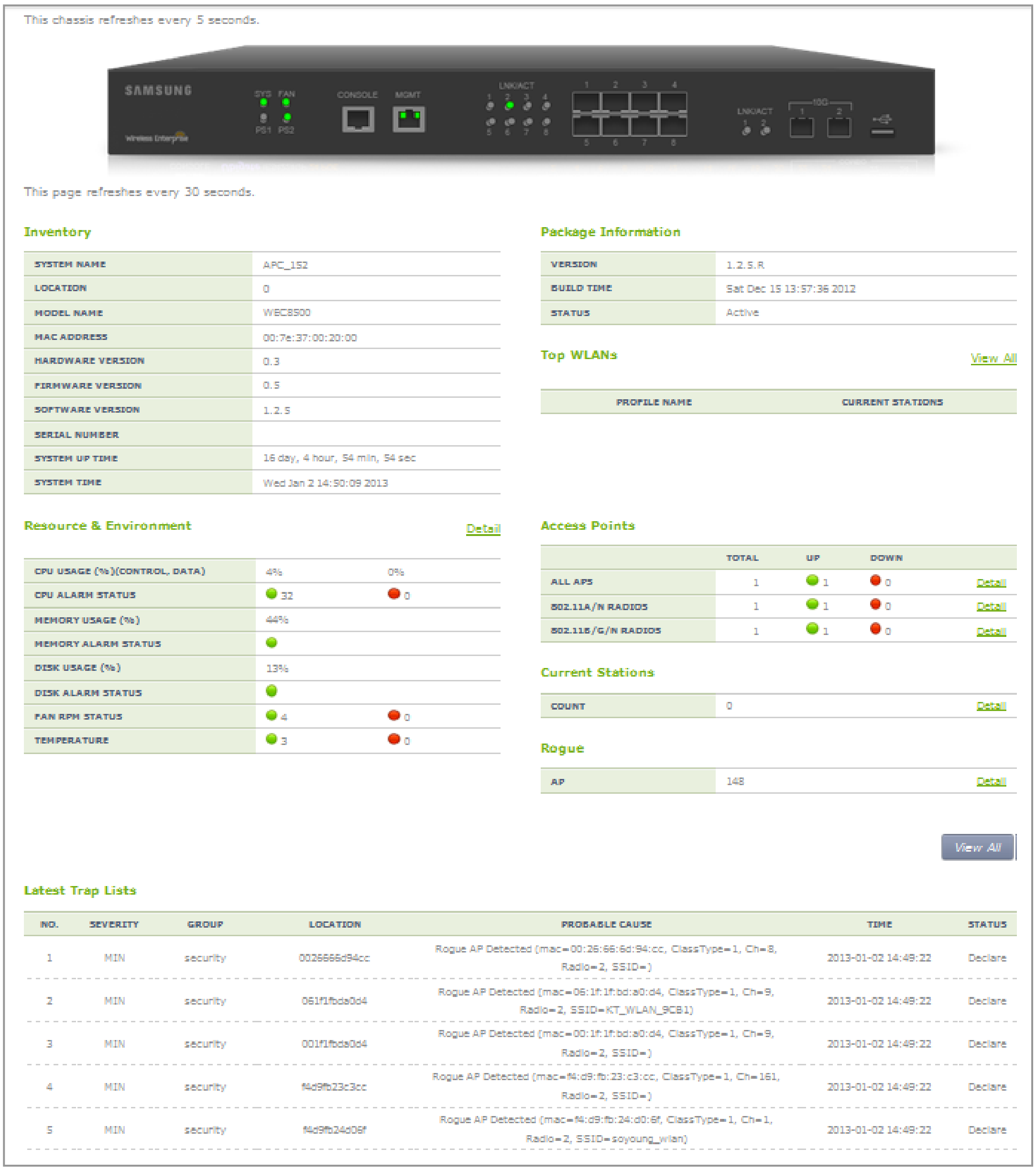
Parameter	Description
Power Supply [0]~[1]	Whether a power module is equipped (Equipped, Not Equipped)
Status	Power module operation status (OK, NOK)

The WEC8050 has only one power module as shown below.

Parameter	Description
Power Supply Status	Power module operation status (OK, NOK)

Retrieving with Web UI

In the menu bar of **<WEC Main window>,** select **<Monitor>** and then select the **<Summary>** menu in the sub-menus. It provides a wide range of information, status retrieving event and alarm retrieving function of the WEC8500 system.



This chassis refreshes every 5 seconds.

This page refreshes every 30 seconds.

Inventory

SYSTEM NAME	APC_152
LOCATION	0
MODEL NAME	WEC8500
MAC ADDRESS	00:7e:37:00:20:00
HARDWARE VERSION	0.3
FIRMWARE VERSION	0.5
SOFTWARE VERSION	1.2.5
SERIAL NUMBER	
SYSTEM UP TIME	16 day, 4 hour, 54 min, 54 sec
SYSTEM TIME	Wed Jan 2 14:50:09 2013

Package Information

VERSION	1.2.5.R
BUILD TIME	Sat Dec 15 13:57:36 2012
STATUS	Active

Top WLANs View All

PROFILE NAME	CURRENT STATIONS

Resource & Environment Detail

CPU USAGE (%)(CONTROL, DATA)	4%	0%
CPU ALARM STATUS	🟢 32	🔴 0
MEMORY USAGE (%)	44%	
MEMORY ALARM STATUS	🟢	
DISK USAGE (%)	13%	
DISK ALARM STATUS	🟢	
FAN RPM STATUS	🟢 4	🔴 0
TEMPERATURE	🟢 3	🔴 0

Access Points

	TOTAL	UP	DOWN	
ALL APS	1	🟢 1	🔴 0	Detail
802.11A/N RADIOS	1	🟢 1	🔴 0	Detail
802.11B/G/N RADIOS	1	🟢 1	🔴 0	Detail

Current Stations

COUNT	0	Detail

Rogue

AP	148	Detail

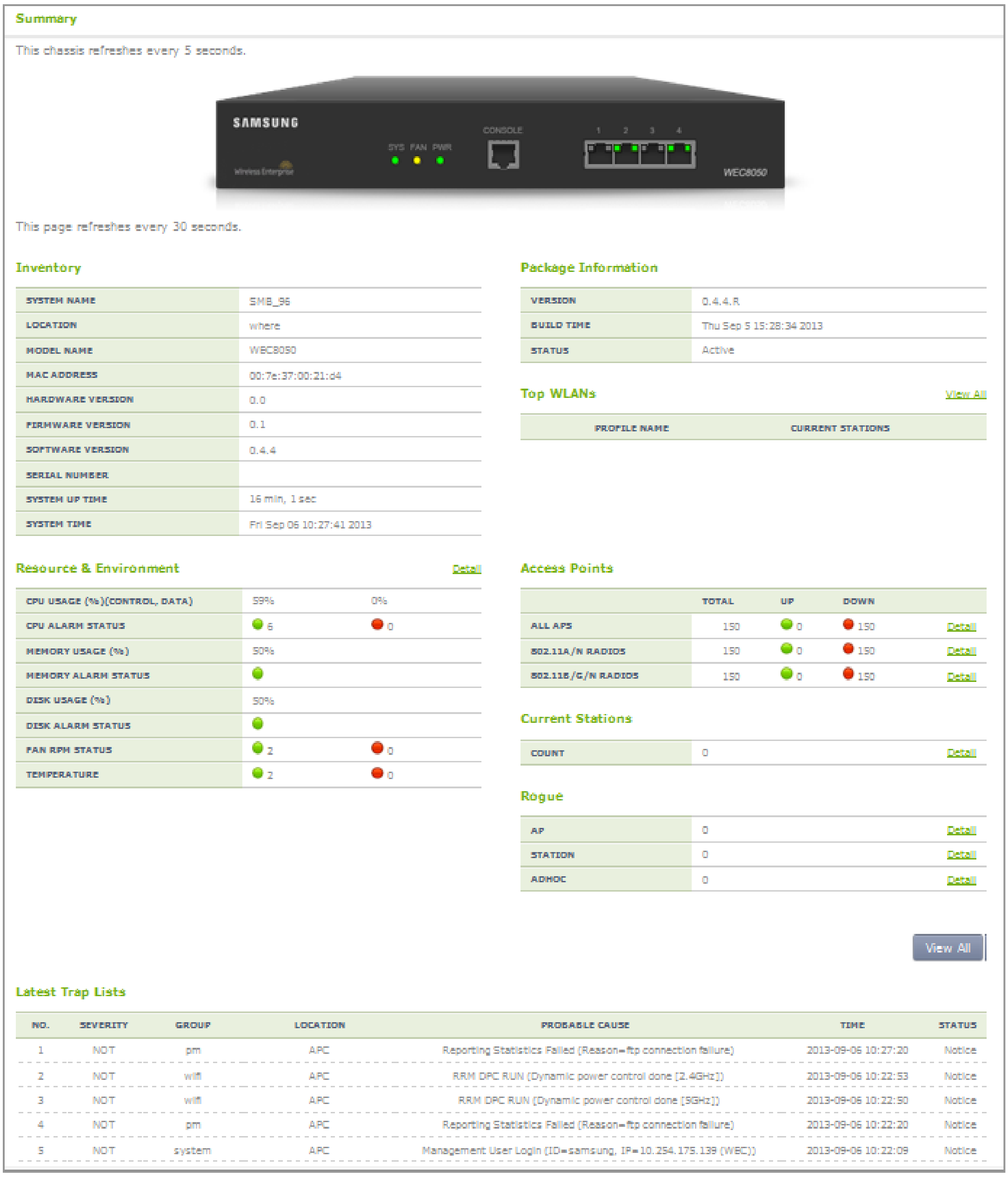
View All

Latest Trap Lists

NO.	SEVERITY	GROUP	LOCATION	PROBABLE CAUSE	TIME	STATUS
1	MIN	security	0026666d94cc	Rogue AP Detected (mac=00:26:66:6d:94:cc, ClassType=1, Ch=8, Radio=2, SSID=)	2013-01-02 14:49:22	Declare
2	MIN	security	061f1fbda0d4	Rogue AP Detected (mac=06:1f:1f:bd:a0:d4, ClassType=1, Ch=9, Radio=2, SSID=KT_WLAN_9CB1)	2013-01-02 14:49:22	Declare
3	MIN	security	001f1fbda0d4	Rogue AP Detected (mac=00:1f:1f:bd:a0:d4, ClassType=1, Ch=9, Radio=2, SSID=)	2013-01-02 14:49:22	Declare
4	MIN	security	f4d9fb23c3cc	Rogue AP Detected (mac=f4:d9:fb:23:c3:cc, ClassType=1, Ch=161, Radio=2, SSID=)	2013-01-02 14:49:22	Declare
5	MIN	security	f4d9fb24d06f	Rogue AP Detected (mac=f4:d9:fb:24:d0:6f, ClassType=1, Ch=1, Radio=2, SSID=soyoung_wlan)	2013-01-02 14:49:22	Declare

Figure 198. System information

It provides various information, status retrieving event and alarm retrieving function of the WEC8050 system.



Summary

This chassis refreshes every 5 seconds.

This page refreshes every 30 seconds.

Inventory

SYSTEM NAME	SMB_96
LOCATION	where
MODEL NAME	WEC8050
MAC ADDRESS	00:7e:37:00:21:d4
HARDWARE VERSION	0.0
FIRMWARE VERSION	0.1
SOFTWARE VERSION	0.4.4
SERIAL NUMBER	
SYSTEM UP TIME	16 min, 1 sec
SYSTEM TIME	Fri Sep 06 10:27:41 2013

Package Information

VERSION	0.4.4.R
BUILD TIME	Thu Sep 5 15:28:34 2013
STATUS	Active

Top WLANs View All

PROFILE NAME	CURRENT STATIONS

Resource & Environment Detail

CPU USAGE (%)(CONTROL, DATA)	59%	0%
CPU ALARM STATUS	🟢 6	🔴 0
MEMORY USAGE (%)	50%	
MEMORY ALARM STATUS	🟢	
DISK USAGE (%)	50%	
DISK ALARM STATUS	🟢	
FAN RPM STATUS	🟢 2	🔴 0
TEMPERATURE	🟢 2	🔴 0

Access Points

	TOTAL	UP	DOWN	
ALL APS	150	🟢 0	🔴 150	Detail
802.11A/N RADIOS	150	🟢 0	🔴 150	Detail
802.11B/G/N RADIOS	150	🟢 0	🔴 150	Detail

Current Stations

COUNT	0	Detail

Rogue

AP	0	Detail
STATION	0	Detail
ADHOC	0	Detail

Latest Trap Lists

NO.	SEVERITY	GROUP	LOCATION	PROBABLE CAUSE	TIME	STATUS
1	NOT	pm	APC	Reporting Statistics Failed (Reason=ftp connection failure)	2013-09-06 10:27:20	Notice
2	NOT	wifi	APC	RRM DPC RUN (Dynamic power control done [2.4GHz])	2013-09-06 10:22:53	Notice
3	NOT	wifi	APC	RRM DPC RUN (Dynamic power control done [5GHz])	2013-09-06 10:22:50	Notice
4	NOT	pm	APC	Reporting Statistics Failed (Reason=ftp connection failure)	2013-09-06 10:22:20	Notice
5	NOT	system	APC	Management User Login (ID=samsung, IP=10.254.175.139 (WEC))	2013-09-06 10:22:09	Notice

10.2.2 System Reboot

There is a command that can reboot the system. Rebooting can be reserved and you can cancel or retrieve the reservation.

Configuration using CLI

Use the ‘reboot’ command to reboot the system.

```
WEC8500# reboot
```

Use the ‘reboot in HH:MM:SS’ command to reserve system reboot. Once the reservation is completed, the system is rebooted after a specified time (HH:MM:SS).

```
WEC8500# reboot in 12:00:00

       Do you want to save the configuration? (y/n): y

       Do you want to restart the system? (y/n): y
Notice: The system WILL reboot in 12:00:00.
WEC8500# show reboot schedule
The reboot has scheduled in 11:58:41.
```

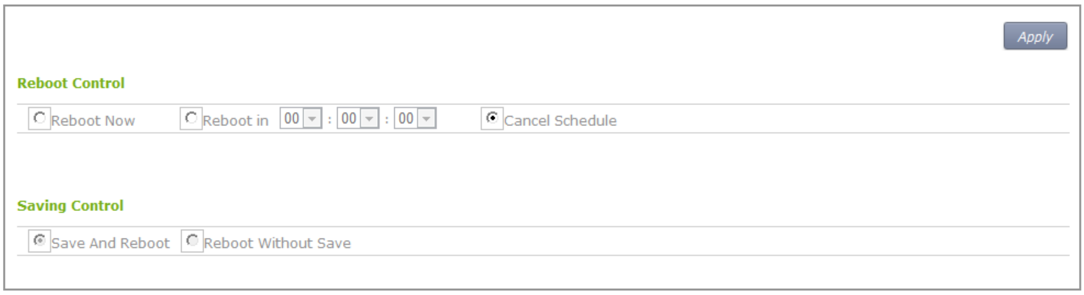
To cancel the reservation, enter the ‘no reboot’ command.

```
WEC8500# no reboot
```

Configuration using Web UI

To configure a reboot related function, in the menu bar of **<WEC Main window>**, select **<Administrator>** and then select the **<Reboot>** menu in the sub-menus.

The Reboot window is shown below.



Reboot Control

○ Reboot Now ○ Reboot in 00 : 00 : 00 ● Cancel Schedule

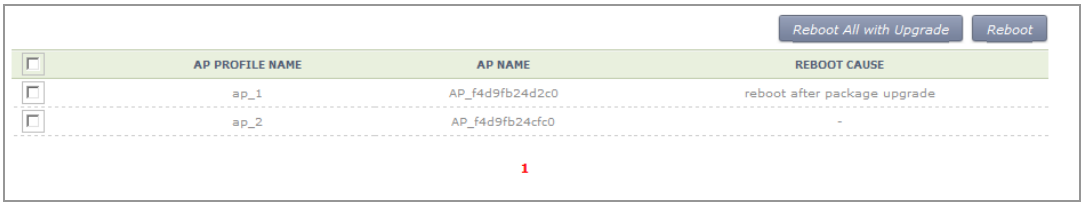
Saving Control

● Save And Reboot ○ Reboot Without Save

[APC]

Figure 199. Reboot (APC)

[AP]



□	AP PROFILE NAME	AP NAME	REBOOT CAUSE
□	ap_1	AP_f4d9fb24d2c0	reboot after package upgrade
□	ap_2	AP_f4d9fb24cfc0	-

Figure 200. Reboot (AP)

10.3 System Resource Management

10.3.1 Retrieving System Status

Retrieving with CLI

By using the ‘show system’ command, you can check the status of each system resource such as CPU load, memory usage, disk usage, Fan RPM level, or system temperature, etc.

- show system cpu: Retrieves CPU load. If there are several cores, the CPU load of each core is displayed.
- show system memory: Retrieves memory usage.
- show system disk: Retrieves disk usage.
- show system fan: Retrieves system fan speed (RPM level range: 0-3)
- show system temp: Retrieves system temperature (°C).

The result of system status retrieval using each command is as follows:

[CPU Load]

The retrieving CLI execution result of WEC8500 is as follows:

```
WEC8500# show system cpu
 Average CPU usage  (%)
  control plane   :  3.84
  data plane      :  0.00
WEC8500# show system cpu detail
 -----------------------------------------------------------------
 Average CPU usage                                          (%)
  control plane                                           2.12
  data plane                                              0.00
 -----------------------------------------------------------------
 Detail CPU usage                                           (%)
  control plane
   [10.00] [04.23] [00.00] [02.74] [00.00] [00.00] [00.00] [00.00]
  data plane
   [00.00] [00.00] [00.00] [00.00] [00.00] [00.00] [00.00] [00.00]
   [00.00] [00.00] [00.00] [00.00] [00.00] [00.00] [00.00] [00.00]
```

The retrieving CLI execution result of WEC8050 is as follows:

```
WEC8050# show system cpu
 Average CPU usage  (%)
  control plane    : 39.43
  data plane       :  0.01
WEC8050# show system cpu  detail
 -----------------------------------------------------------------
 Average CPU usage                                           (%)
  control plane                                           21.97
  data plane                                               0.01
 -----------------------------------------------------------------
 Detail CPU usage                                         (%)
  control plane
   [23.29] [25.71] [16.90]
  data plane
   [00.01] [00.00] [00.00]
```

[Memory usage]

```
WEC8500# show system memory
 Total      Memory :  7657960 KBytes
 Used       Memory :  3341868 KBytes
 Available  Memory :  4316092 KBytes
 Reserved   Memory :  8900608 Kbytes
```

[Disk usage]

```
WEC8500# show system disk
 Total  Disk   :  13520032 KBytes
 Used   Disk   :   4338296 KBytes
 Free   Disk   :   9181736 KBytes
```

[Fan RPM Level]

The retrieving CLI execution result of WEC8500 is as follows:

```
WEC8500# show system fan
 FAN ID   rpm Level(0-3)
 -------  --------------
 FAN[0]      1 level
 FAN[1]      1 level
 FAN[2]      1 level
 FAN[3]      1 level
```

The retrieving CLI execution result of WEC8050 is as follows:

```
WEC8050# show system fan
 FAN ID   rpm Level(0-3)
 -------  --------------
 FAN[0]       1 level
 FAN[1]       1 level
```

[System Temperature (°C)]

The retrieving CLI execution result of WEC8500 is as follows:

```
WEC8500# show system temp
 Sensor Location   Temperature
 ---------------   -----------
CPU sensor 1          33
CPU sensor 2          38
Board                 29
```

The retrieving CLI execution result of WEC8050 is as follows:

```
WEC8050# show system temp
 Sensor Location   Temperature(‘C)
 ---------------   ---------------
 CPU sensor 1         45
 CPU sensor 2         52
```

Retrieving with Web UI

In the menu bar of **<WEC Main window>,** select **<Monitor>** and then select the **<Summary>** menu in the sub-menus. For more information about detail window, see ‘10.2.1 Retrieving System Information’.

10.3.2 Retrieving and Configuring Threshold

If each resource of the system exceeds its configured threshold, there occurs an alarm. The APC helps an operator check and configure each threshold.

Configuration using CLI

To check each threshold, use the below command.

- show system threshold cpu: CPU load (%)
- show system threshold memory: Memory usage (%)
- show system threshold disk: Disk usage (%)
- show system threshold fan: Fan RPM level
- show system threshold temp: Retrieves system temperature (°C).

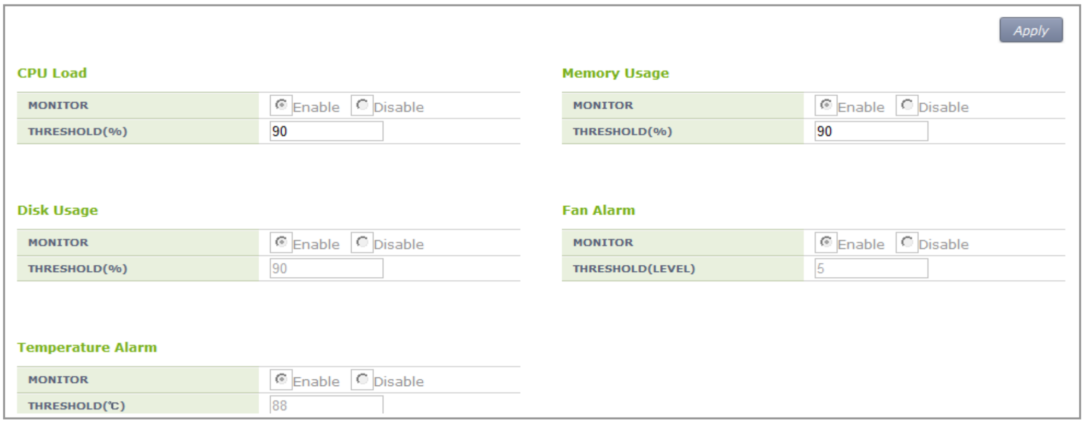
To change a threshold related to CPU load or memory usage, enter the command as follows:

- system monitor cpu threshold [THRESHOLD]: Configures the CPU load threshold.
- system monitor memory threshold [THRESHOLD]: Configures the memory usage threshold.

Parameter	Description
THRESHOLD	Threshold to configure (%)

Configuration using Web UI

In the menu bar of <WEC Main window>, select <Administrator> and then select the <SNMP> → <Trap Control> → <Alarm Threshold> menu in the sub-menus.
You can retrieve and configure a threshold at which CPU load, disk usage, temperature alarm, memory usage, or fan alarm occurs. Enter a value for each item, and click the **<Apply>** button to make the configuration applied.



CPU Load

MONITOR	● Enable ○ Disable
THRESHOLD(%)	90

Memory Usage

MONITOR	● Enable ○ Disable
THRESHOLD(%)	90

Disk Usage

MONITOR	● Enable ○ Disable
THRESHOLD(%)	90

Fan Alarm

MONITOR	● Enable ○ Disable
THRESHOLD(LEVEL)	5

Temperature Alarm

MONITOR	● Enable ○ Disable
THRESHOLD(℃)	88

Figure 201. Configuring SNMP alarm threshold

10.4 Managing Alarm and Event

The system alarms and events are saved into a system log and transmitted to an external server according to the filtering policy. An alarm is managed in terms of occurrence and release and an event is managed in the report format.

The alarm and event are managed according to group or level. Each group or level is classified into the following item. You can select an item to retrieve.

Alarm, event group

Group	Description
system	Retrieves system alarm or event.
pm	Retrieves performance monitoring alarm or event.
ap	Retrieves AP related alarm or event.
wlan	Retrieves WLAN related alarm or event.
wifi	Retrieves WI-FI related alarm or event.
security	Retrieves security related alarm or event.
network	Retrieves network related alarm or event.
interface	Retrieves interface related alarm or event.
se	Retrieves system engine related alarm or event.
list	Retrieves alarm or event list information.

Alarm level

Level	Description
critical	Retrieves a critical alarm. A critical alarm is a system log that could give a critical effect to a service.
major	Retrieves a major alarm. A major alarm is a system log that could give a major effect to a service.
minor	Retrieves a minor alarm. A minor alarm is a system log that could give a minor effect to a service.

10.4.1 Retrieving Current Alarm

All the system alarms are basically recorded into a system log. The procedure of retrieving current alarms is as follows:

Retrieving with CLI

To retrieve current alarms, execute the command as follows:

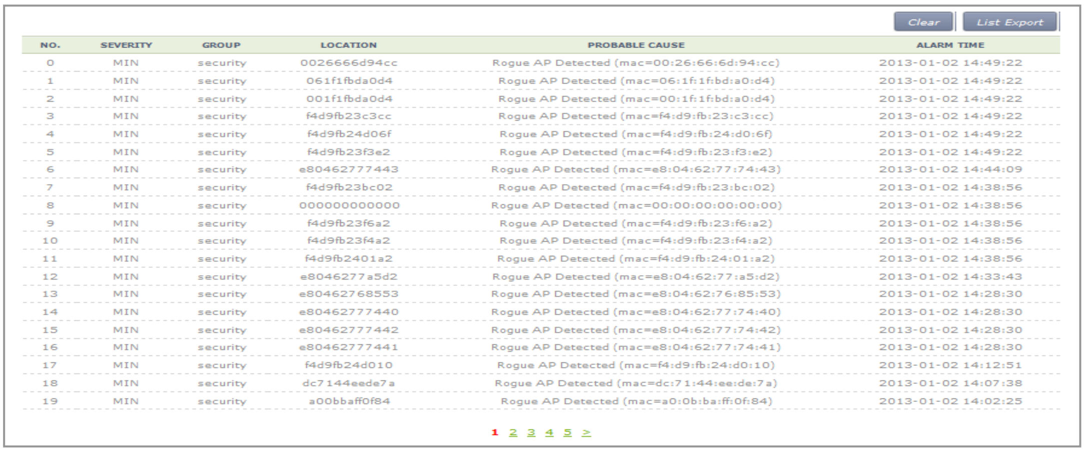
```
WEC8500# show alarm list all
1 network    2012-12-17 09:56:13 MAJ APC ge8 1301 NET Link dn
AdminStatus[up] OperStatus[down]
2 network    2012-12-17 09:56:13 MAJ APC xe1 1301 NET Link dn
AdminStatus[up] OperStatus[down]
3 network    2012-12-17 09:56:13 MAJ APC xe2 1301 NET Link dn
AdminStatus[up] OperStatus[down]
…
```

To selectively retrieve a group or level, execute the command as follows:

```
WEC8500# show alarm list group network
1 network    2012-12-17 09:56:13 MAJ APC ge8 1301 NET Link dn
AdminStatus[up] OperStatus[down]
```

```
WEC8500# show alarm history level major
1 network    2012-12-17 09:56:13 MAJ APC ge8 1301 NET Link dn
AdminStatus[up] OperStatus[down]
```

Retrieving with Web UI



NO.	SEVERITY	GROUP	LOCATION	PROBABLE CAUSE	ALARM TIME
0	MIN	security	0026666d94cc	Rogue AP Detected (mac=00:26:66:6d:94:cc)	2013-01-02 14:49:22
1	MIN	security	061f1fbda0d4	Rogue AP Detected (mac=06:1f:1f:bd:a0:d4)	2013-01-02 14:49:22
2	MIN	security	001f1fbda0d4	Rogue AP Detected (mac=00:1f:1f:bd:a0:d4)	2013-01-02 14:49:22
3	MIN	security	f4d9fb23c3cc	Rogue AP Detected (mac=f4:d9:fb:23:c3:cc)	2013-01-02 14:49:22
4	MIN	security	f4d9fb24d06f	Rogue AP Detected (mac=f4:d9:fb:24:d0:6f)	2013-01-02 14:49:22
5	MIN	security	f4d9fb23f3e2	Rogue AP Detected (mac=f4:d9:fb:23:f3:e2)	2013-01-02 14:49:22
6	MIN	security	e80462777443	Rogue AP Detected (mac=e8:04:62:77:74:43)	2013-01-02 14:44:09
7	MIN	security	f4d9fb23bc02	Rogue AP Detected (mac=f4:d9:fb:23:bc:02)	2013-01-02 14:38:56
8	MIN	security	000000000000	Rogue AP Detected (mac=00:00:00:00:00:00)	2013-01-02 14:38:56
9	MIN	security	f4d9fb23f6a2	Rogue AP Detected (mac=f4:d9:fb:23:f6:a2)	2013-01-02 14:38:56
10	MIN	security	f4d9fb23f4a2	Rogue AP Detected (mac=f4:d9:fb:23:f4:a2)	2013-01-02 14:38:56
11	MIN	security	f4d9fb2401a2	Rogue AP Detected (mac=f4:d9:fb:24:01:a2)	2013-01-02 14:38:56
12	MIN	security	e8046277a5d2	Rogue AP Detected (mac=e8:04:62:77:a5:d2)	2013-01-02 14:33:43
13	MIN	security	e80462768553	Rogue AP Detected (mac=e8:04:62:76:85:53)	2013-01-02 14:28:30
14	MIN	security	e80462777440	Rogue AP Detected (mac=e8:04:62:77:74:40)	2013-01-02 14:28:30
15	MIN	security	e80462777442	Rogue AP Detected (mac=e8:04:62:77:74:42)	2013-01-02 14:28:30
16	MIN	security	e80462777441	Rogue AP Detected (mac=e8:04:62:77:74:41)	2013-01-02 14:28:30
17	MIN	security	f4d9fb24d010	Rogue AP Detected (mac=f4:d9:fb:24:d0:10)	2013-01-02 14:12:51
18	MIN	security	dc7144eede7a	Rogue AP Detected (mac=dc:71:44:ee:de:7a)	2013-01-02 14:07:38
19	MIN	security	a00bbaff0f84	Rogue AP Detected (mac=a0:0b:ba:ff:0f:84)	2013-01-02 14:02:25

To retrieve the list of current alarms, in the menu bar of **<WEC Main window>**, select **<Monitor>** and then select the **<Active Alarm>** menu in the sub-menus.

Figure 202. Current alarm

10.4.2 Retrieving History

Retrieving with CLI

The APC retrieves the history of alarm and event using the following command.

[Alarm History]

```
WEC8500# show alarm history all
1 ap       2012-12-20 13:13:25 MAJ AP_f4:d9:fb:24:cf:80 r=1 AP RADIO
CARD TX FAIL Clear radio(1)
2 ap       2012-12-20 13:13:25 MAJ AP_f4:d9:fb:24:cf:80 r=2 AP RADIO
CARD TX FAIL Clear radio(2)
3 ap       2012-12-20 13:13:25 MAJ AP_f4:d9:fb:24:cf:80 r=1,w=1 BSS
…
```

Because all the alarms are managed per group or level, you can retrieve it selectively using the following command.

```
WEC8500# show alarm history group system
1 system    2012-12-21 17:49:45 MAJ APC core2 CPU Load Alarm Declare
LOAD(100.00)
…
```

```
WEC8500# show alarm history level major
1 system    2012-12-21 17:49:45 MAJ APC core 2 CPU Load Alarm Declare
LOAD(100.00)
…
```

[Event History]

You can retrieve event information using the following command.

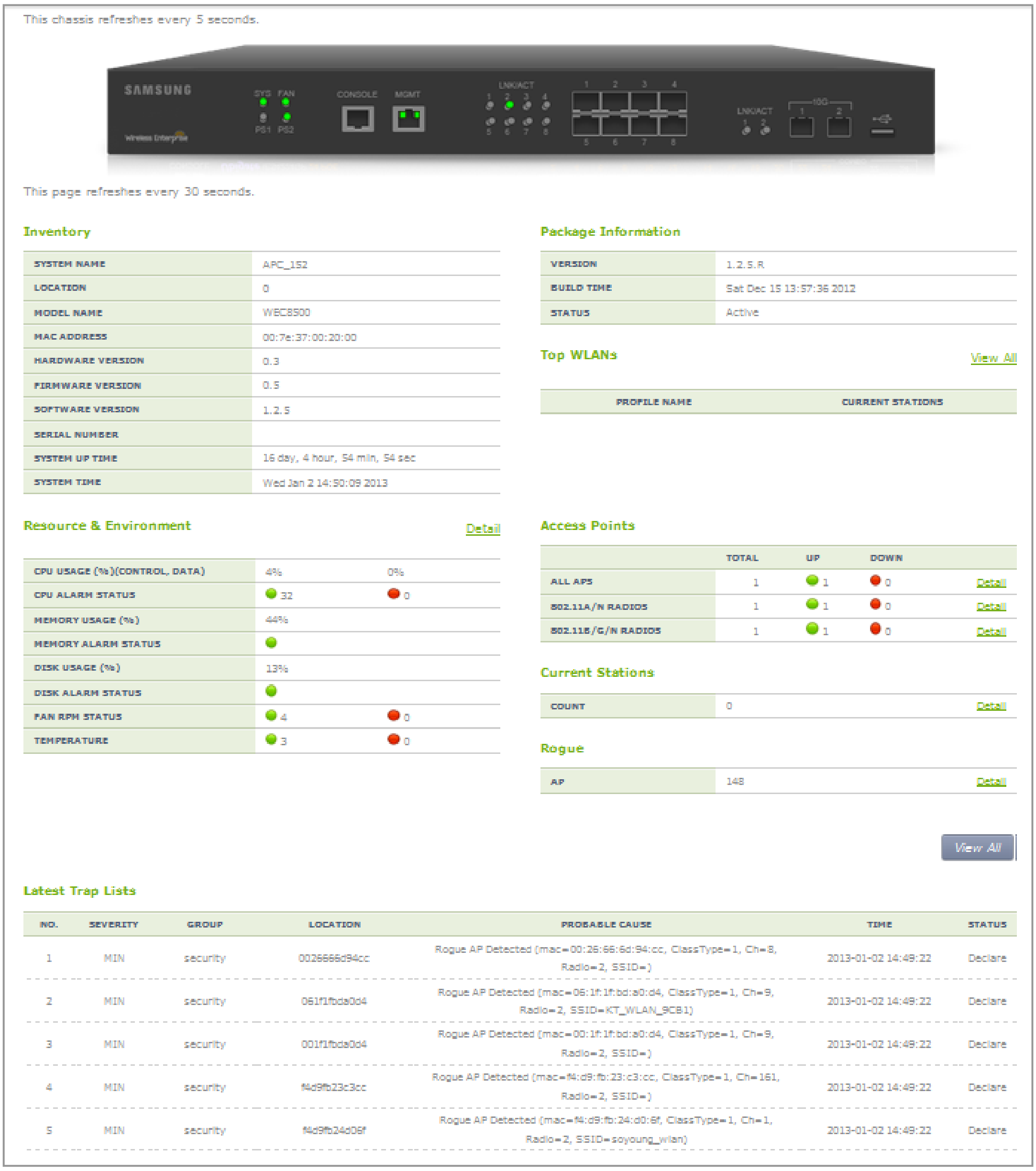
```
WEC8500# show event
1 system  2012-08-31 13:59:46 NOT APC MGMT User Login ID=samsung,
IP=192.168.0.91
2 system  2012-08-31 13:48:33 NOT SWM:system Boot Complete -
…
```

An event is managed per group and you can retrieve it selectively using the following command.

```
WEC8500# show event group interface
1 interface  2012-08-31 13:48:32 NOT APC Index[1] Name[ge1] IF Admin No
Shut AdminStatus[up] OperStatus[up]
…
```

Configuration using Web UI

In the menu bar of **<WEC Main window>,** select **<Monitor>** and then select the **<Summary>** menu in the sub-menus. It provides status retrieving event and alarm retrieving function.



This chassis refreshes every 5 seconds.

This page refreshes every 30 seconds.

Inventory

SYSTEM NAME	APC_152
LOCATION	0
MODEL NAME	WEC8500
MAC ADDRESS	00:7e:37:00:20:00
HARDWARE VERSION	0.3
FIRMWARE VERSION	0.5
SOFTWARE VERSION	1.2.5
SERIAL NUMBER	
SYSTEM UP TIME	16 day, 4 hour, 54 min, 54 sec
SYSTEM TIME	Wed Jan 2 14:50:09 2013

Resource & Environment Detail

CPU USAGE (%)(CONTROL, DATA)	4%	0%
CPU ALARM STATUS	● 32	● 0
MEMORY USAGE (%)	44%	
MEMORY ALARM STATUS	●	
DISK USAGE (%)	13%	
DISK ALARM STATUS	●	
FAN RPM STATUS	● 4	● 0
TEMPERATURE	● 3	● 0

Package Information

VERSION	1.2.5.R
BUILD TIME	Sat Dec 15 13:57:36 2012
STATUS	Active

Top WLANs View All

PROFILE NAME	CURRENT STATIONS

Access Points

	TOTAL	UP	DOWN	
ALL APS	1	● 1	● 0	Detail
802.11A/N RADIOS	1	● 1	● 0	Detail
802.11B/G/N RADIOS	1	● 1	● 0	Detail

Current Stations

COUNT	0	Detail

Rogue

AP	148	Detail

Latest Trap Lists

NO.	SEVERITY	GROUP	LOCATION	PROBABLE CAUSE	TIME	STATUS
1	MIN	security	0026666d94cc	Rogue AP Detected (mac=00:26:66:6d:94:cc, ClassType=1, Ch=8, Radio=2, SSID=)	2013-01-02 14:49:22	Declare
2	MIN	security	061f1fbda0d4	Rogue AP Detected (mac=06:1f:1f:bd:a0:d4, ClassType=1, Ch=9, Radio=2, SSID=KT_WLAN_9CB1)	2013-01-02 14:49:22	Declare
3	MIN	security	001f1fbda0d4	Rogue AP Detected (mac=00:1f:1f:bd:a0:d4, ClassType=1, Ch=9, Radio=2, SSID=)	2013-01-02 14:49:22	Declare
4	MIN	security	f4d9fb23c3cc	Rogue AP Detected (mac=f4:d9:fb:23:c3:cc, ClassType=1, Ch=161, Radio=2, SSID=)	2013-01-02 14:49:22	Declare
5	MIN	security	f4d9fb24d06f	Rogue AP Detected (mac=f4:d9:fb:24:d0:6f, ClassType=1, Ch=1, Radio=2, SSID=soyoung_wlan)	2013-01-02 14:49:22	Declare

Figure 203. History

10.4.3 External Transmission Configuration

All the alarms and events in the system are transmitted to outside through the SNMP trap and syslog. If the alarm filter information is configured, only filtered alarm is transmitted to an external management server.

10.4.4 Alarm Filter and Level Configuration

An alarm filter can be configured per group or level (severity). The filtered alarms are transmitted to an external server through the SNMP trap and syslog.

Configuration using CLI

The procedure of alarm filter configuration is as follows:

1) Go to configure mode of CLI.

```
WEC8500# configure terminal
```

2) Configure group information.

```
WEC8500/configure# alarm group system
```

3) Configure level information.

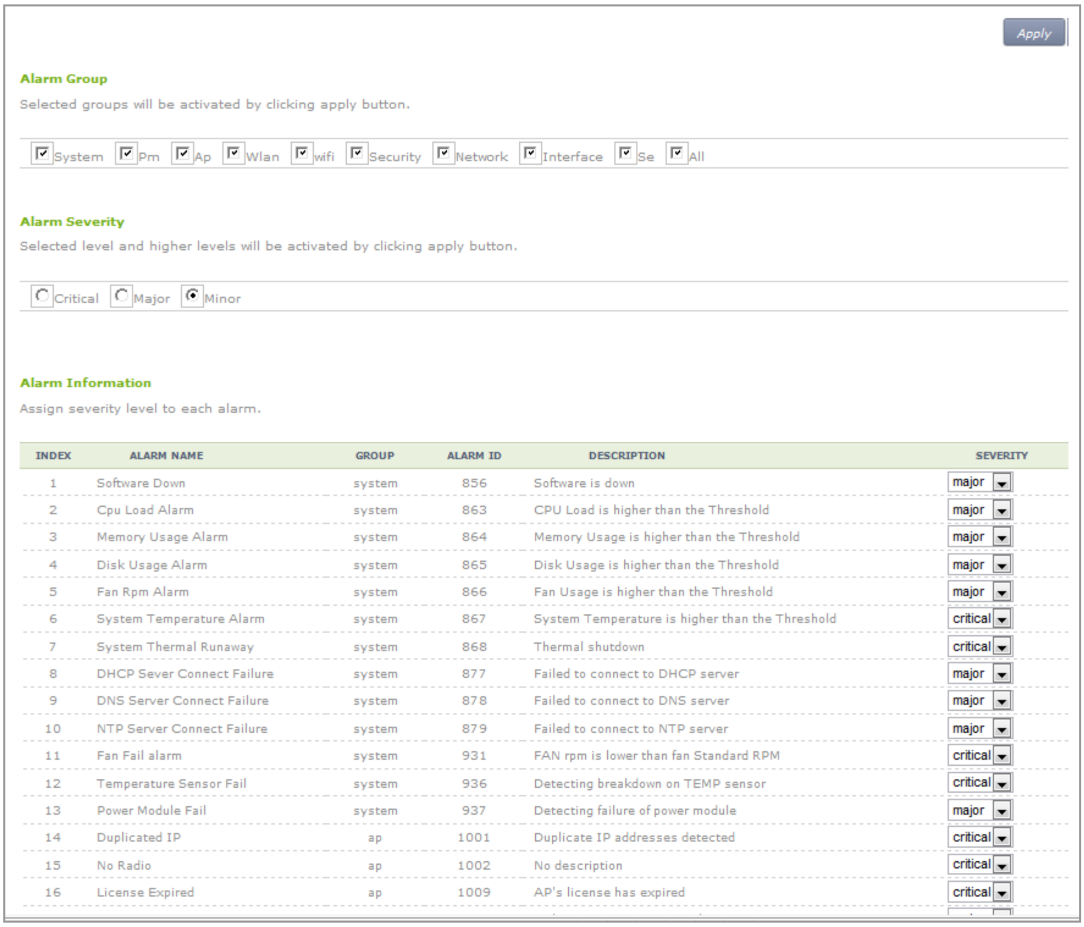
```
WEC8500/configure# alarm level major
```

4) To check the configured alarm filter information, use the ‘show alarm conf’ command.

Configuration using Web UI

In the menu bar of <**WEC Main window**>, select <**Administrator**> and then select the <**SNMP**> → <**Trap Control**> → <**Alarm Information**> menu in the sub-menus.

You can retrieve the configuration related to alarm filter and alarm level.



Alarm Group

Selected groups will be activated by clicking apply button.

☑ System ☑ Pm ☑ Ap ☑ Wlan ☑ wifi ☑ Security ☑ Network ☑ Interface ☑ Se ☑ All

Alarm Severity

Selected level and higher levels will be activated by clicking apply button.

○ Critical ○ Major ● Minor

Alarm Information

Assign severity level to each alarm.

INDEX	ALARM NAME	GROUP	ALARM ID	DESCRIPTION	SEVERITY
1	Software Down	system	856	Software is down	major
2	Cpu Load Alarm	system	863	CPU Load is higher than the Threshold	major
3	Memory Usage Alarm	system	864	Memory Usage is higher than the Threshold	major
4	Disk Usage Alarm	system	865	Disk Usage is higher than the Threshold	major
5	Fan Rpm Alarm	system	866	Fan Usage is higher than the Threshold	major
6	System Temperature Alarm	system	867	System Temperature is higher than the Threshold	critical
7	System Thermal Runaway	system	868	Thermal shutdown	critical
8	DHCP Sever Connect Failure	system	877	Failed to connect to DHCP server	major
9	DNS Server Connect Failure	system	878	Failed to connect to DNS server	major
10	NTP Server Connect Failure	system	879	Failed to connect to NTP server	major
11	Fan Fail alarm	system	931	FAN rpm is lower than fan Standard RPM	critical
12	Temperature Sensor Fail	system	936	Detecting breakdown on TEMP sensor	critical
13	Power Module Fail	system	937	Detecting failure of power module	major
14	Duplicated IP	ap	1001	Duplicate IP addresses detected	critical
15	No Radio	ap	1002	No description	critical
16	License Expired	ap	1009	AP's license has expired	critical

Figure 204. Configuring alarm filter and level

10.5 Managing Traffic Performance

You can manage the traffic performance statistics information and accumulated data for the APC system and the interface of each AP.

10.5.1 Managing History Information

When the traffic performance information management is enabled, the APC system creates history information at every 5 minute. But, if the FTP server information is not configured, the history information is not transmitted to outside although it is created.

Collecting information

1) Go to configure mode of CLI.

```
WEC8500# configure terminal
WEC8500/configure#
```

2) Configure the traffic performance information.

```
WEC8500/configure# stats-report enable
```

3) Configure a FTP server to transmit history information.
   - stats-report target ip [IP_ADDRESS] port [PORT_NUMBER] id [ID] password [PASSWORD] path [PATH]

Parameter	Description
IP_ADDRESS	IP address of a target server
PORT_NUMBER	Port number of a target server
ID	User ID of a target server
PASSWORD	User password of a target server
PATH	File storage path of a target server

4) To check the information of traffic performance information management, use the ‘show stats-report conf’ command.

5) Configure so that the performance information is uploaded to the FTP server. But, because the default is the ‘start’ status, this step may be skipped.

```
WEC8500/configure# stats-report upload start
```

Stopping information collection

1) Go to configure mode of CLI.

```
WEC8500# configure terminal
```

2) ‘Disable’ the traffic performance information management.

```
WEC8500/configure# no stats-report enable
```

3) To check the configured information, use the ‘show stats-report conf’ command.

10.5.2 Managing Real-time Information Collection

1) Go to configure mode of CLI.

```
WEC8500# configure terminal
WEC8500/configure#
```

2) To collect real-time information, execute the following command. At this time, you must specify the name and status of an interface whose information will be collected.
   - stats-report current-stats [INTERFACE_NAME] [STATE]

Parameter	Description
INTERFACE_NAME	Name of an interface to collect or stop collection
STATE	Status of real-time information (start/stop) - start: Starts real-time information collection - stop: Stops or initializes the real-time information collection.

3) To check the entered information, use the ‘show stats-report conf’ command.

4) To check the information of a configured interface when the real-time information collection is configured, execute the following command.
   - show stats-report current-stats [INTERFACE_NAME]

   If the real-time information collection is suspended or initialized, you cannot check the real-time information of the interface.

```
WEC8500/configure# show stats-report current-stats ge3
Error: This interface was not configured to gather statistics.
```

10.6 Managing License Key

The Samsung Electronics Common License Method (SLM) is applied to Version 1.5 or newer of the APC system.
Therefore, SLM licensing is applied to new websites that are installed using Version 1.5 or later.
However, if Version 1.4 is upgraded to Version 1.5, the existing license key is used without any modification. The existing license which is not SLM must be installed and used also in the case of expanding or reissuing the APC system.

In this document, license keys supported by Version 1.4 or later are referred to as 'old license keys' and license keys supported by Version 1.5 or later are referred to as 'Activation keys'.

These details are summarized in the table below.

Initially installed version	Reinstalling the license	Expanding/reissuing	After an upgrade
APC Version 1.4 or below	Install the old license	Install the old license	Re-use the old license
APC 1.5 or higher	Install the SLM license	Install the SLM license	Re-use the SLM license

If an APC system is shipped out without a license installed, only the following services are offered:

System Model	Number of APs	VQM	Firewall
WEC8050	5 units connected	Not provided	Not provided
WEC8500	2 units connected	Not provided	Not provided

10.6.1 Managing SLM License (Activation) Key

An SLM activation key can have differences in regard to the number of manageable APs, whether to support the VQM function, whether to support the firewall function, and the period of use of a function.
Every system has a unique activation key and activation keys are provided in the form of encrypted files.
To clear an SLM activation key installed in a system, the deactivation command needs to be executed and after the execution of the command, a deactivation key is issued to notify that clearing has been completed successfully.

NOTE

Installation

Only two activation keys can be installed/registered in an APC system.
If two unexpired activation keys co-exist, available services are offered as shown in the following example:

(Example)
- Activation Key 1: AP (100 units), VQM (Disable), Firewall (Disable)
- Activation Key 2: AP (50 units), VQM (Enable), Firewall (Disable)
- result: AP (100 units), VQM (Enable), Firewall (Disable)

NOTE

Period of Use

Each activation key has its own information regarding the start and end times, and if the current time is not within the set period, the activation key expires.

NOTE

Application

An activation key only functions correctly after the system is rebooted after deletion or installation of a key.

Configuration using CLI

To configure an activation key, first execute the following commands and enter license mode:

```
WEC8500# configure terminal
WEC8500/configure# system license
WEC8500/configure/system/license#
```

[Installing Activation Key]

When the system is shipped out, there is no registered license key. Therefore, you must install the license key you received immediately after the first system installation. You can install a license key directly or remotely using CLI.

- activate-key [Fullpath filename]
  Registers an activation key file. If a license key file exists in a specified folder, use the license key file for registration.
  When entering the file name of an activation key, you must enter the file name including its full path.

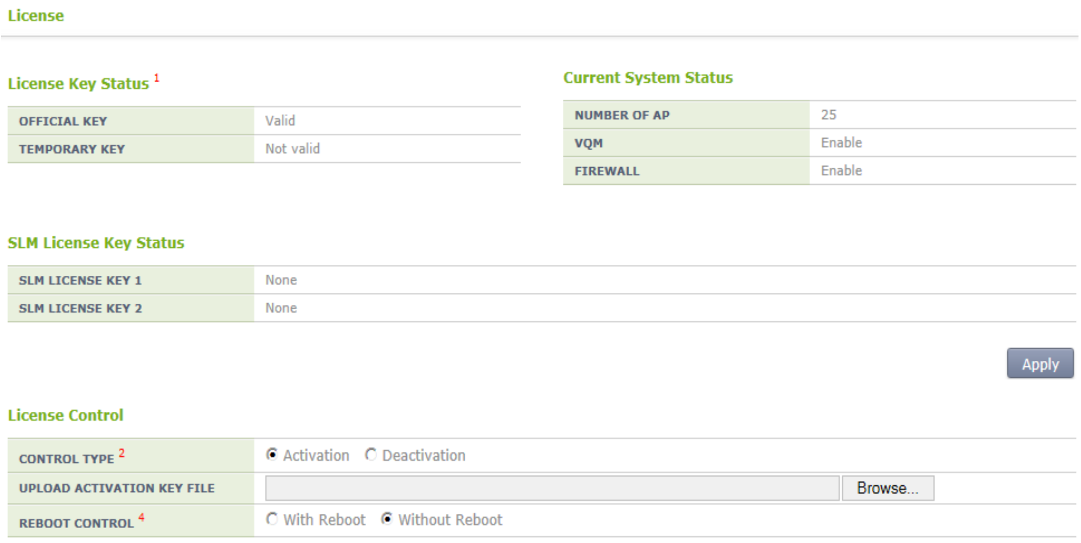
[Clearing Activation Key]

- no activate-key [the activation key’s license key]
  Clears an activation key registered in the system.
  You can view the license key information of an activation key in the ‘License’ field of the activation key by executing the ‘show system license-key’ command.
  After clearance, you can view information about the deactivation key in the ‘License Key’ of the key after executing the ‘show system license-key’ command.

Configuration using Web UI

In the menu bar of **<WEC Main window>**, select **<Configuration>** and then select the **<License>** menu in the sub-menus.

In the figure below, the ‘SLM License Key Status’ shows the installation and application statuses of SLM activation keys.
In the ‘License Control’ section, the operator can select an activation key stored in their PC and install it in the system.
In addition, the operator can also deactivate an installed activation key. The operator can clear an installed activation key by selecting Deactivation in ‘License Control’ and then entering the license key shown in ‘SLM License Key Status’.



License

License Key Status [1]

OFFICIAL KEY	Valid
TEMPORARY KEY	Not valid

Current System Status

NUMBER OF AP	25
VQM	Enable
FIREWALL	Enable

SLM License Key Status

SLM LICENSE KEY 1	None
SLM LICENSE KEY 2	None

License Control

CONTROL TYPE [2]	● Activation ○ Deactivation
UPLOAD ACTIVATION KEY FILE	Browse...
REBOOT CONTROL [4]	○ With Reboot ● Without Reboot

Figure 205. SLM License Search and Configuration Window

10.6.2 Managing Old License Key

An old license key can differ in regard to the number of manageable APs, whether to support the VQM function, whether to support the firewall function, and the period of use of a function.

A license key is unique for each system and it consists of encrypted 53 characters.

A license key is distributed in a file or text format.

NOTE

Installation

APC system can install/register only one official license key and one temporary license key. A license key (temporary license Key) with time duration can be installed only 3 times.

NOTE

Use period

An official license key has no restriction on use period.

A temporary license key has a restriction on use period and the period can be 1, 30, or 60-day.

NOTE

Apply

A license key becomes active only after system rebooting after the key is installed or deleted.

Configuration using CLI

To configure a license key related function, go to license mode by executing the following command.

```
WEC8500# configure terminal
WEC8500/configure# system license
WEC8500/configure/system/license#
```

[Installing License Key]

When the system is shipped out, basically there is no registered license key. Therefore, you must install the license key you received right after the first system installation. You can install a license key directly or remotely using CLI.

- install-key: Registers a file. If a license key file exists in a specified folder, use the license key file for registration. Once it is installed, the license key file is deleted from the system.
- install-key [LICENSE_KEY]: Direct registration
- install-key [IP_ADDRESS] [PORT_NUMBER] [ID] [PASSWORD] [PATH]: Remote registration

Parameter	Description
LICENSE_KEY	Issued license key
IP_ADDRESS	IP address
PORT_NUMBER	Port number
ID	login ID
PASSWORD	Password
PATH	Server path

[Deleting License Key]

You can delete a license key directly.

- no install-key [LICENSE_KEY]

Parameter	Description
LICENSE_KEY	License key to delete

[Retrieving License Key Information]

To check the license key information, use the ‘show system license-key’ command.

```
===== Current System Status ======
Number of APs                : 2
VQM                          : Disabled
Firewall                     : Disabled

===== License Information ======
* Old License - Official License Key
   License Key               : YNHSHPWP-5MNMTE04-UJHKDO4U-A2WGSBGX-
OJZ2MJ5R-7Z5DBYMT
   MAC Address               : F4D9FB236C01
   System Model              : Any
   Lifetime                  : Permanet
   Number of APs             : 75
   VQM                       : Eanbed
   Firewall                  : Eanbed
   Installation Time         : 00
```

[Analyzing License Key]

Before registering a license key to the system, you can check the functions supported by the license key.

- analyze-key [LICENSE-KEY]

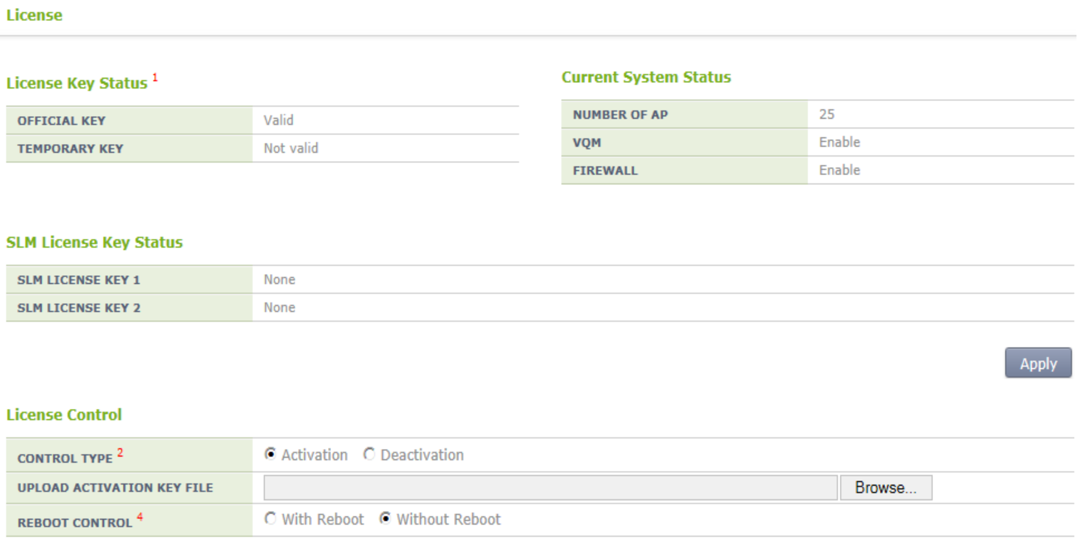
Parameter	Description
LICENSE_KEY	License key

Configuration using Web UI

In the menu bar of <**WEC Main window**>, select <**Configuration**> and then select the <**License**> menu in the sub-menus.

From the APC Version 1.5 and later, in respect of old license keys, the web UI does not provide input/deletion functions and shows only whether they are installed properly.

In the figure below, ‘License Key Status’ is the section that shows whether old license keys are installed properly and ‘Current System Status’ shows license information currently applied to the system.



License

License Key Status [1]

OFFICIAL KEY	Valid
TEMPORARY KEY	Not valid

Current System Status

NUMBER OF AP	25
VQM	Enable
FIREWALL	Enable

SLM License Key Status

SLM LICENSE KEY 1	None
SLM LICENSE KEY 2	None

License Control

CONTROL TYPE [2]	● Activation ○ Deactivation
UPLOAD ACTIVATION KEY FILE	Browse...
REBOOT CONTROL [4]	○ With Reboot ● Without Reboot

Figure 206. Old License Installation Check Window

10.7 Syslog Configuration

The system log (syslog) configuration is required to transmit an event, alarm, and system log information to a target syslog server. You can configure maximum two target syslog servers in the system and you can configure the IP address and port number independently. In addition, because you can configure a filter level, only filtered log information is transmitted to the syslog server.

Configuration using CLI

To transmit an alarm, event, and system log to the syslog server, executes the command as follows:

1) Go to configure mode of CLI.

```
WEC8500# configure terminal
```

2) To transmit an alarm, event, and system log information to the syslog server, specify ‘enable’ as a parameter.

```
WEC8500/configure# syslog enable
```

3) Configure the IP address and UDP port of a target syslog server (The default of the UDP port is ‘514’.).

```
WEC8500/configure# syslog add 192.168.0.91
WEC8500/configure# syslog add 192.168.0.99 udpport 510
```

4) Configure a log level to filter.

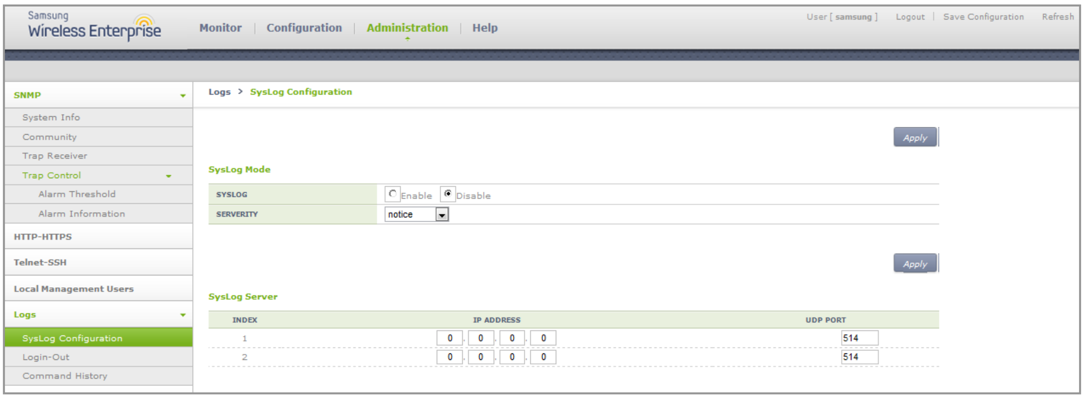
```
WEC8500/configure# syslog level information
```

5) To check the configured syslog information, use the ‘show syslog conf’ command.

Configuration using Web UI

In the menu bar of **<WEC Main window>**, select **<Administrator>** and then select the **<Logs>** → **<SysLog Configuration>** menu in the sub-menus.

It provides syslog related configuration and retrieving function.



SysLog Mode

SYSLOG	○ Enable ● Disable
SERVERITY	notice

SysLog Server

INDEX	IP ADDRESS	UDP PORT
1	0 . 0 . 0 . 0	514
2	0 . 0 . 0 . 0	514

Figure 207. Syslog window

10.8 Upgrade

The APC provides the upgrade function and version checking function that applies a new version of package when it is distributed.

10.8.1 Checking Package Version

You can check the version of a current system by using the following command.

- show version

The following shows the execution results of the command:

```
WEC8500# show version
Samsung package version information
Primary (currently running)
  ver           : 1.4.4.R
  buildTime     : Fri Sep  6 06:08:35 2013
  builder       : apcbuild
  buildDir      : /home2/apcbuild/release/wec8500_1.4.4
Backup
  ver           : 1.4.4.R
  buildTime     : Fri Sep  6 06:08:35 2013
  builder       : apcbuild
  buildDir      : /home2/apcbuild/release/wec8500_1.4.4

Boot rom version information
  ver           : GC15
```

10.8.2 System Upgrade

The APC does system upgrade using CLI and Web UI.

Configuration using CLI

Apply a new package to the system by using the following command.

1) Go to configure mode of CLI.

```
WEC8500# configure terminal
WEC8500/configure#
```

2) Perform upgrade by using a package.
   - package upgrade [FILE_NAME]

Parameter	Description
FILE_NAME	Package file to upgrade The package must be located in the /user/package directory.

A usage example is provided below. When the upgrade is completed, the system is rebooted to apply the package.
When executing the package upgrade command, the message recommending to save the configuration file is displayed.
If you save the current configuration, operator can use it for any future version downgrade.
If there is a configuration file saved during previous upgrade, the message asking whether you are going to use the file is displayed.

```
WEC8500/configure# package upgrade wec8500_1.4.4.R.bin
Notice: It is recommended that you save the configuration before
upgrade.
       You can reapply the configuration, if you need to downgrade.

       Do you want to save the configuration? (y/n): y

       Previous configuration file is existed. Do you want to use it?
(y/n): y
Package Validation check ... success
Package Upgrade ............................................... done
Success
```

3) If package upgrade fails, upgrade is cancelled.
Possible causes and the troubleshooting methods are described below.

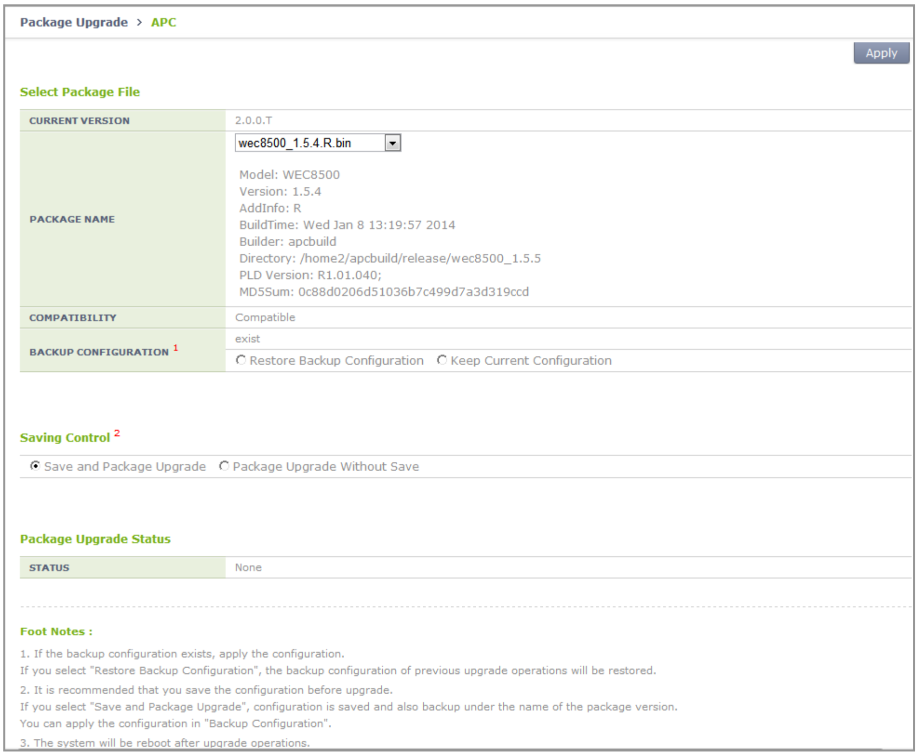
Possible Cause	Error Message	Troubleshooting
File does not exist	Error: no exist ‘wec8500_ 1.3.11.R.bin’ file	Download the package to be upgraded again as the package error has occurred during the package downloading.
Checksum error on the file	Error: Package validation check	
Upgrade terminated due to an internal error	Error: Internal error	1) Execute the ‘show process status’ command to check the process status. 2) Execute the ‘show system cpu detail’ command to check the CPU status. 3) Transmit the logs above to the Samsung Technical Support.
Upgrade terminated due to timeout	saving the configuration- failed (time-out)	1) Execute the ‘show process status’ command to check the process status. 2) Execute the ‘show system cpu detail’ command to check the CPU status. 3) Transmit the logs above to the Samsung Technical Support.

4) After system rebooting, check if the new package is applied to the system.

```
WEC8500# show reboot cause
 Reboot Cause: Block: Upgrade/ Code: Package Upgrade

WEC8500# show version
Samsung package version information
Primary (currently running)
  ver            : 0.7.1.R
  buildTime      : Mon Aug 20 11:35:43 2012
  builder        : gampul
  buildDir       : /data/nome/ymkim/apc_0817
Backup
  ver            : 0.7.1.R
  buildTime      : Mon Aug 20 11:35:43 2012
  builder        : gampul
  buildDir       : /data/nome/ymkim/apc_0817

Boot rom version information
  ver            : unknown
```

Configuration using Web UI

In the menu bar of **<WEC Main window>**, select **<Administrator>** and then select the **<Package Upgrade>** → **<APC>** menu in the sub-menus.



Select Package File

CURRENT VERSION	2.0.0.T
PACKAGE NAME	wec8500_1.5.4.R.bin Model: WEC8500 Version: 1.5.4 AddInfo: R BuildTime: Wed Jan 8 13:19:57 2014 Builder: apcbuild Directory: /home2/apcbuild/release/wec8500_1.5.5 PLD Version: R1.01.040; MD5Sum: 0c88d0206d51036b7c499d7a3d319ccd
COMPATIBILITY	Compatible
BACKUP CONFIGURATION [1]	exist ○ Restore Backup Configuration ○ Keep Current Configuration

Saving Control [2]

● Save and Package Upgrade ○ Package Upgrade Without Save

Package Upgrade Status

STATUS	None

Foot Notes :

1. If the backup configuration exists, apply the configuration.
If you select "Restore Backup Configuration", the backup configuration of previous upgrade operations will be restored.
2. It is recommended that you save the configuration before upgrade.
If you select "Save and Package Upgrade", configuration is saved and also backup under the name of the package version.
You can apply the configuration in "Backup Configuration".
3. The system will be reboot after upgrade operations.

Figure 208. Package upgrade (APC)

10.9 Configuration Management

The APC supports the following functions for configuration management.

- Saves the current configuration information.
- Exports/imports the current configuration information (import/export).
- Initializes system

Configuration using CLI

To save the current configuration information in the system, execute the command as follows:

```
WEC8500# save local
```

To transmit the current configuration information in the system to outside, execute the command as follows: When you execute the command, the configuration information is compressed into the entered 'FILENAME' as a file.

```
WEC8500# export [FILENAME]
```

In addition, to apply a file ('FILENAME') from outside to the current system, execute the command as follows:

```
WEC8500# import [FILENAME]
```

To initialize the current configuration information to the factory default, execute the command as follows: If the 'full-erase' parameter is not entered, only the configuration information is initialized.

```
WEC8500# factory-reset (full-erase)
```

Configuration using Web UI

In the menu bar of **<WEC Main window>**, select **<Administrator>** and then select the **<DB backup/restore>** menu in the sub-menus.

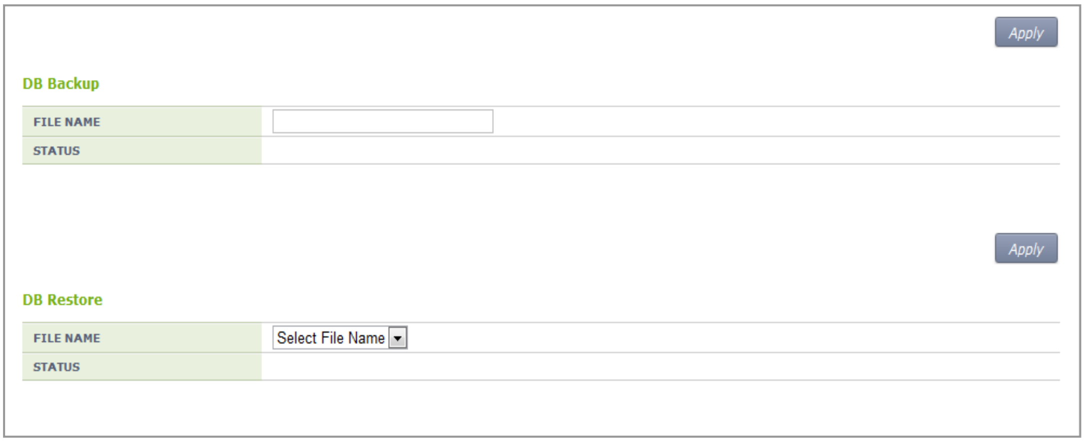


Figure 209. DB Backup/Restore

In the DB backup/restore window, enter FILE NAME and click the **<Apply>** button to create the configuration information as a file or apply an external configuration information file. The STATUS shows the execution results of backup/restore function.

10.10 Debug and Diagnosis

10.10.1 Process

The APC can retrieve the status of an active process in the system and an error associated with each process.

Retrieving the Process Status

```
WEC8500# show processes
Processes Info.
Status: D - usually IO, R - Running, S - Sleep
        T - Stop, X - Dead, Z - Zombie
        up - Active, down - Inactive
        dis - Disable

id        name      pid     activationTime      status  reStart
--      --------    ----    ---------------     ------  ------
 0        swmmon    6222   2012-08-31 14:38:21   up(S)   0
 1        evm       1759   2012-08-31 13:47:08   up(S)   0
 2        evmlogd   1760   2012-08-31 13:47:08   up(S)   0
 3        db        1807   2012-08-31 13:47:14   up(S)   0
 4        license   1838   2012-08-31 13:47:34   up(S)   0
 5        pcap      1839   2012-08-31 13:47:34   up(S)   0
 6        filemgr   1840   2012-08-31 13:47:34   up(S)   0
 7        filemib   1841   2012-08-31 13:47:34   up(S)   0
 8        cm        1846   2012-08-31 13:47:34   up(S)   0
 9        iim       1847   2012-08-31 13:47:34   up(S)   0
10        iimp      1850   2012-08-31 13:47:34   up(S)   0
11        nsm       1902   2012-08-31 13:47:35   up(S)   0
12        mstpd     1903   2012-08-31 13:47:35   up(S)   0
13        pimd      1904   2012-08-31 13:47:35   up(S)   0
14        ripd      1905   2012-08-31 13:47:35   up(S)   0
15        ospfd     1906   2012-08-31 13:47:35   up(S)   0
16        lacpd     1907   2012-08-31 13:47:35   up(S)   0
17        fqm       1909   2012-08-31 13:47:35   up(S)   0
18        imi       1942   2012-08-31 13:47:35   up(S)   0
19        zebosm    2188   2012-08-31 13:47:55   up(S)   0
20        awmb      2226   2012-08-31 13:48:00   up(S)   0
21        apm       2385   2012-08-31 13:48:30   up(S)   0
22        capwap    2386   2012-08-31 13:48:30   up(S)   0
23        hostapd   2387   2012-08-31 13:48:30   up(S)   0
24        eqm       2388   2012-08-31 13:48:30   up(S)   0
```

Checking process error log

You can check the log of errors that occurred in a current process

```
WEC8500# show processes log
   id date                 name        pid  signal       backtrace    reason
 ----- -------------------- ----------- ---- ------------ ----------  ---------
 2509. 2012-12-21 15:59:50  iimp        1800 SIGTERM(15)   traced      signal
 2510. 2012-12-21 15:59:50  sipalg      2377 SIGTERM(15)   traced      signal
 2511. 2012-12-21 15:59:50  apclt       2375 SIGTERM(15)   traced      signal
 2511. 2012-12-21 15:59:50  apccluster  2217 SIGTERM(15)   traced      signal
 2512. 2012-12-21 15:59:50  evmlogd     1766 SIGTERM(15)   traced      signal
 2513. 2012-12-21 15:59:50  imi         1893 SIGTERM(15)   traced      signal
 2514. 2012-12-21 15:59:50  wids        2293 SIGTERM(15)   traced      signal
 2515. 2012-12-21 15:59:50  ipwlogd     2416 SIGTERM(15)   traced      signal
 2516. 2012-12-21 15:59:50  nfm         2417 SIGTERM(15)   traced      signal
 2517. 2012-12-21 15:59:50  httprd      2379 SIGTERM(15)   traced      signal
 2518. 2012-12-21 15:59:50  fqm         1882 SIGTERM(15)   traced      signal
 2519. 2012-12-21 15:59:50  irfm        2297 SIGTERM(15)   traced      signal
 2520. 2012-12-21 15:59:50  filemib     1770 SIGTERM(15)   traced      signal
 2520. 2012-12-21 15:59:50  pm          2376 SIGTERM(15)   traced      signal
 2521. 2012-12-21 15:59:50  salh        2415 SIGTERM(15)   traced      signal
 2522. 2012-12-21 15:59:50  guestService 2294 SIGTERM(15)
```

In addition, you can check the detail information corresponding to the ‘id’ of each error log by using the following command.

```
WEC8500# show processes log id 15
   id date                 name         pid   signal       backtrace    reason
 ----- ------------------- ------------ ----- ----------- ----------- ---------
  15. 2012-08-02 18:39:08   eqm          2311  NONE(0)      -            coredump

 detail (additional info.)
  → core_dump (comm:eqm, signr:11, pid:2311)
  → detected unixtime: 1343900344 -> Thu Aug  2 18:39:04 2012


   id date                 name         pid   signal       backtrace    reason
 ----- ------------------- ------------ ----- ----------- ----------- ---------
  15. 2012-08-09 12:37:09   eqm         30103  NONE(0)       -           coredump

 detail (additional info.)
  → core_dump (comm:eqm, signr:11, pid:30103)
```

10.10.2 Retrieving Crash Information

When a critical problem occurs in the system platform during operation, the APC saves important system information at that time to provide the crash information that can be used for post mortem analysis. The crash information includes the Crash Detect and Report (CDR) information that has the context about the crash status and the core dump information that has the memory dump about the crash status of a user process.

10.10.2.1 Managing CDR Information

To manage the CDR information, the system provides the following function.

- Retrieving CDR Information
- Exports CDR history information
- Deletes CDR history information

[Retrieving Summarized CDR History Information]

To retrieve the entire history information for all the rebooting including rebooting due to a crash, enter the 'show debug reboot summary' command.

- show debug reboot summary

```
WEC8500# show debug reboot summary
======================================================================
====================================
ID  EVENT_NAME      EVENT_DESCRIPTION
REBOOT_TIME
======================================================================
====================================
0001 DIE            DIE_VAL[1] - Unhandled kernel unaligned access
03:56:00, Aug 22 2012
0000 PANIC           softlockup: hung tasks
03:51:51, Aug 22 2012
```

[Retrieving Detail CDR History Information]

To check the detail crash information, execute the 'show debug reboot info [id/all]' command. By using this command, you can view the key information including a kernel log that exists before the system is rebooted due to a critical crash. The description of each parameter is shown below.

- show debug reboot info [DATA]

Parameter	Description
DATA	Selects crash information (id/all) - id: A specific CDR ID value to view - all: Retrieve all the CDR histories

If no parameter is entered, the most recent reboot information is retrieved.

```
WEC8500# show debug reboot info

######################################################################

[REBOOT_SUMMARY]======================================================

ID              : 0001
EVENT NAME      : DIE
EVENT DESC      : DIE_VAL[1] - Unhandled kernel unaligned access
REBOOT TIME     : 03:56:00, Aug 22 2012

[KERNEL_LOG]==========================================================

console [cdr-1] enabled
Creating 1 MTD partitions on “nor0”:
0x000000dc0000-0x000000fc0000 : “crash_raw”
CDR connector initialized (ID = {8.1})
…
…
```

[Exporting CDR history information]

The crash information of system can be extracted to text file for post analysis.
By entering the ‘show debug reboot export’ command, you can send the system crash information created in a text file to outside using the ‘transfer’ command.

- show debug reboot export

[Deleting CDR history information]

To delete CDR information remaining in a device, execute the following command.

- debug reboot erase [DATA]

Parameter	Description
DATA	If there is no reboot information selection (id/all) option, the most recent system reboot information is deleted. - id: A specific CDR ID value to delete - all: Delete all the CDR histories

10.10.2.2 Retrieving Core Dump Information

Use the ‘show debug coredump summary’ command to retrieve the status of core dump.

```
WEC8500# show debug coredump summary

CORE_DUMP      :    enable
DUMP_QUOTA     :      1024 (MB)
CORE_SIZE      :    204800 (KB)
POLL_PERIOD    :        60 (sec)
THRESHOLD      :        80 (%)
----------------------------------------------------------------------
--------------------------------------------------
   PROCESS     |           SIGNAL           |         TIME          |
CORE_FILE
----------------------------------------------------------------------
--------------------------------------------------
eqm             Segmentation fault   Wed Aug 22 03:05:16 2012 core-eqm-
11-1345572316-2437.gz
hostapd         Aborted Wed Aug 22 03:06:02 2012 core-hostapd-6-
1345572362-2436.gz
nsm             Bus error Wed Aug 22 03:07:21 2012 core-nsm-10-
1345572441-2013.gz
```

10.11 File Management

The APC provides the file management functions of copying, moving, or retrieving a file and also file download and upload. In addition, it checks the integrity of a package file and provides version retrieving method.

To use a file related command, go to the file mode first. The command is basically used as follows:

1) Go to the file mode of CLI.

```
WEC8500# file
WEC8500/file#
```

2) Use each command. The following commands are used in the file mode.

Command	Description
cd	Changes the current directory.
copy	Copies a file.
df	Retrieves the brief information of a storage media connected to the system.
download	Downloads a file using FTP protocol.
dump	Shows the content of a file.
ls	Retrieves the list of files or directories in a specified path.
move	Changes the name of a file.
pwd	Shows the current directory.
remove	Deletes a file.
upload	Uploads a file using FTP protocol.
verify	Checks the integrity of a package file and shows the result.
version	Shows the information of a package file.

10.11.1 Retrieving Configuration of Current Directory

The file management command supports both a relative path and an absolute path based on the current (working) directory. The current directory is a path that is a reference of a relative path. For example, if the current directory is ‘disk:/’, the ‘copy test1 test2’ is the same as the ‘copy disk:/test1 disk:/test2’ command.

To retrieve a current directory, enter the ‘pwd’ command.

```
WEC8500/file# pwd

 disk:/
```

To change a directory, use the ‘cd [TARGET_DIR]’ command.

```
WEC8500/file# cd etc
WEC8500/file# pwd

 disk:/etc
```

Parameter	Description
TARGET_DIR	Name of a directory to change

10.11.2 Retrieving Directory List

To retrieve a file or directory in a specific directory, use the ‘ls’ command. If you enter only ‘ls’, all the contents in the current directory are displayed.
To check only a specific directory, enter the ‘ls [TARGET_DIR]’ command.

A usage example is provided below.

```
WEC8500/file# ls
Current working directory: disk:/
 directory       4.0K     Jul   5  13:49:49  etc
 directory      16K       Jan   1  09:00:39  lost+found
 directory       4.0K     Jun   9  15:36:02  opt
 directory       4.0K     Jun   9  16:46:59  stats
 directory       4.0K     Jun  12  01:11:01  var
WEC8500/file# ls etc
Current working directory: disk:/
 directory       4.0K     Jun   9  15:36:02  ap
 directory       4.0K     Jun   9  15:36:02  config
 directory       4.0K     Jun   9  15:36:02  db
 file         168         Jul   5  13:49:49  PKG_INFO_STANDBY
WEC8500/file# ls disk:/etc
Current working directory: disk:/
 directory       4.0K     Jun   9  15:36:02  ap
 directory       4.0K     Jun   9  15:36:02  config
 directory       4.0K     Jun   9  15:36:02  db
 file         168         Jul   5  13:49:49 P KG_INFO_STANDBY
WEC8500/file#
```

10.11.3 Revising File

To copy a file, use the ‘copy [SRC_FILENAME] [DES_FILENAME]’ command.
The below command copies the ‘test’ file into ‘disk:/test2’.

```
WEC8500/file# copy test disk:/test2
```

To delete a file, use the ‘remove [FILENAME]’ command. If you enter the below command and enter ‘y’, the ‘test2’ file is deleted.

```
WEC8500/file# remove test2
‘disk:/test2’ Do you really want to remove it ? (y/n)
y
```

To change a filename, use the ‘move [SRC_FILENAME] [DES_FILENAME]’ command.
If you enter the below command, the ‘test’ file is changed to ‘test2’.

```
WEC8500/file# move test test2
```

10.11.4 Retrieve File Content

To retrieve the content of a file, use the ‘dump’ command. It can be displayed in the hexa or ascii format.

```
WEC8500/file# dump test2
0000000 7f45 4c46 0202 0100 0000 0000 0000 0000  |.ELF............ |
0000010 0002 0008 0000 0001 0000 0001 2000 4950  |............ .IP |
0000020 0000 0000 0000 0040 0000 0000 0002 9600  |.......@........ |
0000030 808d 0007 0040 0038 0007 0040 001e 001d  |.....@.8...@.... |
0000040 0000 0006 0000 0005 0000 0000 0000 0040  |...............@ |
0000050 0000 0001 2000 0040 0000 0001 2000 0040  |.... ..@.... ..@ |
0000060 0000 0000 0000 0188 0000 0000 0000 0188  |................ |
0000070 0000 0000 0000 0008 0000 0003 0000 0004  |................ |
0000080 0000 0000 0002 5b40 0000 0001 2002 5b40  |......[@.... .[@ |
0000090 0000 0001 2002 5b40 0000 0000 0000 000f  |.... .[@........ |
```

10.11.5 File Download and Upload

A file is downloaded or uploaded through FTP protocol.

To download a file, use the ‘download’ command. An example of downloading the ‘test’ file from ‘192.168.1.1’ to ‘disk:/test’ is shown below.

```
WEC8500/file# download  guest guest 192.168.1.1 test disk:/test
```

To upload a file, use the ‘upload’ command.
An example of uploading the ‘disk:/uploadtest’ file to ‘192.168.1.1’ is shown below.

```
WEC8500/file# upload  guest guest 192.168.1.1 disk:/uploadtest
uploadtest
```

10.11.6 Package File

You can use a package file by downloading it from a network or copying it from a USB memory. The APC checks the integrity of a package file and provides the information retrieving function.

Checking the integrity of a package file

Checking if a package file is damaged is called integrity checking. An example of checking integrity using the ‘verify’ command is shown below.

[Checking APC package file]

```
WEC8500/file# verify package/wec8500_0.3.0.R.bin
 Verify: success!!
```

[Checking AP package file]

```
WEC8500/file# verify package/ap/wea302.img
 Verify: success!!
```

Retrieving the information of a package file

A package file includes the information such as version information, model information, package build information, etc. To check the content of a package file, use the ‘version’ command.

[Retrieving the information of APC package file]

```
WEC8500/file# version package/wec8500_0.3.0.R.bin
=====================================================
 Model         :   WEC8500
 Version       :   0.3.0.R
 Build Date    :   Sat Jun 30 15:57:09 2012
 Builder       :   apcbuild
 Build Path    :   /home2/apcbuild/release/apc
 MD5SUM        :   b715450abf1be81616fd7e6391e12cee
```

[Retrieving the information of AP package file]

```
WEC8500/file# version package/ap/wea302.img
=====================================================
 Model         :   wea302
 Version       :   0.1.0.R
 Build Date    :   Fri Apr 13 18:41:26 KST 2012
 Sisze         :   31998080
 CRC           :   d5aa76ad
```

10.11.7 Retrieving Storage Media

The WEC8500 supports a disk and USB memory as a storage media. And the WEC8050 supports only a disk as a storage media. Both current directory-based relative path and absolute path are all supported during command execution and the path of each device is shown in the below table.

Device	Path	Description
Disk	disk:/	Uses the system disk as a storage media. (basic path)
USB memory	usb [N]:/	Uses a USB memory as a storage media. ('N' represents a partition number in a USB memory.)

The check the information of a storage media connected to the APC, use the 'df' command.

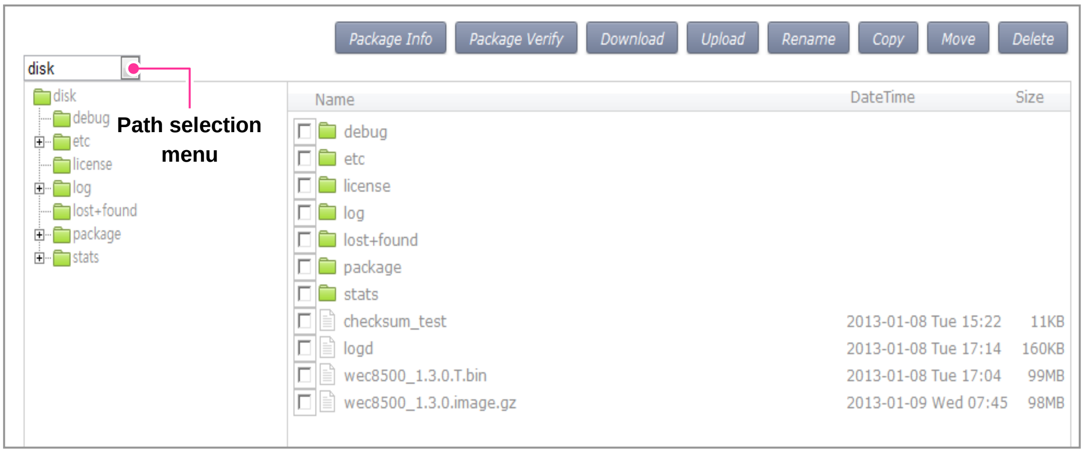
```
WEC8500/file# df
Device        : disk
Filesystem    : ext4
Total size    : 12.9G Free space:  11.3G

Device        : usb1
Filesystem    : vfat
Total size    : 7.4G Free space:   7.0G
```

Using the results of entering the above command, an operator can check the below information.

- The disk and USB memory are connected.
- Disk free space: 11.3 GB
- USB memory free space: 7 GB

10.11.8 Managing File in Web UI

In the menu bar of <**WEC Main window**>, select < **Administration** > and then select the <**File Management**> → <**APC-Local PC**> menu in the sub-menus.



	Name	DateTime	Size
□	debug		
□	etc		
□	license		
□	log		
□	lost+found		
□	package		
□	stats		
□	checksum_test	2013-01-08 Tue 15:22	11KB
□	logd	2013-01-08 Tue 17:14	160KB
□	wec8500_1.3.0.T.bin	2013-01-08 Tue 17:04	99MB
□	wec8500_1.3.0.image.gz	2013-01-09 Wed 07:45	98MB

Figure 210. File management window

The File Management window provides the following functions:

Retrieving a file list

Select a desired path in the path selection menu, which is categorized based on the following criteria:

- disk: Select this to retrieve the entire files in the SSD disk of APC.
- APC Package: Select this to retrieve an APC package file.
- AP Package: Select this to retrieve an AP package file.
- Log: Select this to retrieve a log file.
- Stats: Select this to retrieve a statistics file.
- USBN: Select this to retrieve a file in a USB memory connected to the APC. (The N represents a partition number in a USB memory.)

Copying a file

After selecting the checkbox of a file to copy, click the <**Copy**> button. Then a popup window is displayed. In the popup window, specify a location where the file will be copied.

Moving a file

After selecting the checkbox of a file to move, click the <**Move**> button. Then a popup window is displayed. In the popup window, specify a location where the file will be moved.

Deleting a file

After selecting the checkbox of a file to delete, click the **<Delete>** button.

Changing a filename

After selecting the checkbox of a file to change its name, click the **<Rename>** button. Then a popup window is displayed. In the popup window, enter a file name to change.

Downloading a file

After selecting the checkbox of a file to download, click the **<Download>** button.

Uploading a file

When you click the **<Upload>** button, the popup window where you can select a file to upload is displayed. After selecting a file in the upload window, click the **<Upload>** button.

Retrieving a package file

In the path selection menu, select **<APC Package>**. After selecting the checkbox of a package file to retrieve, click the **<Package Info>** button. The package file information is displayed in the popup window.

Checking the integrity of a package file

In the path selection menu, select **<APC Package>**. After selecting the checkbox of a package file to retrieve, click the **<Package Verify>** button. The result of checking the integrity of a package file is displayed in the popup window.

ANNEX A. CLI Command Structure

The structure of CLI command is as follows.

A.1 configure

```
|-- configure
|       |-- spectrum-analysis
|       |       |-- ap
|       |       |       |-- service
|       |       |       |-- channel-request
|       |       |       |       |-- channel-interval
|       |       |       |       |-- channel-control
|       |       |       |       |       |-- dot11b
|       |       |       |       |       |-- dot11aLow
|       |       |       |       |       |-- dot11aMid
|       |       |       |       |       |-- dot11aHigh
|       |       |       |-- configuration-request
|       |       |       |       |-- sample
|       |       |       |       |-- interference
|       |       |       |       |-- duty-cycle
|       |-- interferer
|       |       |-- 80211a
|       |       |       |-- continuous_transmitter
|       |       |       |-- cordless_phone
|       |       |       |-- video_camera
|       |       |-- 80211b
|       |       |       |-- bluetooth
|       |       |       |-- microwave_oven
|       |       |       |-- continuous_transmitter
|       |       |       |-- cordless_phone
|       |       |       |-- video_camera
|       |       |       |-- zigbee
|       |       |-- unknown
|       |-- hostname
|       |-- call-fail-detect
|       |-- mgmt-user-password
|       |-- mgmt-user
|       |-- telnet-timeout
|       |-- console-timeout
|       |-- system
|       |       |-- monitor
|       |       |       |-- cpu
|       |       |       |       |-- threshold
|       |       |       |-- memory
|       |       |       |       |-- threshold
|       |       |-- license
|       |       |       |-- install-key
|       |       |       |-- analyze-key
|       |-- qos
|       |       |-- description
|       |       |-- max-dot1p
|       |       |-- ac
|       |       |-- bw-contract-downstream
|       |       |-- bw-contract-upstream
|       |       |-- call-test
|       |-- country
|       |       |-- set-global
|       |       |-- set-ap
|       |       |-- add-channel
|       |       |-- del-channel
|       |       |-- max-tx-power
|       |-- handover
|       |       |-- time
|       |       |       |-- ho-decision
|       |       |       |-- command
|       |       |       |-- scan-suppress
|       |       |-- mode
|       |       |-- opmode
|       |       |-- scan-trigger-level
|       |       |-- scan-report-level
|       |       |-- scan-time-channel
|       |       |-- scan-time-service
|       |       |-- scan-time-interleave
|       |       |-- number-of-proreq
|       |       |-- number-of-channel
|       |       |-- buffered-forwarding
|       |       |-- handover-timer
|       |       |-- command
|       |       |-- scanmode-clear
|       |       |-- start-buffering
|       |       |-- fwd-buffering
|       |       |-- upload-data
|       |       |-- decision-delta
|       |       |-- station-decision-delta
|       |       |-- nchostats-req
|       |       |-- inter-apc
|       |-- station
|       |       |-- number-of-assoc-tracking
|       |       |-- stats-req
|       |       |-- device_type
|       |       |-- data
|       |       |       |-- collection
|       |       |       |-- assoc-latency-threshold
|       |       |       |-- ho-latency-threshold
|       |       |       |-- assoc-fail-threshold
|       |       |       |-- ho-fail-threshold
|       |-- security
|       |       |-- radius
|       |       |       |-- auth
|       |       |       |-- acct
|       |       |       |-- serverIp
|       |       |       |-- secret
|       |       |       |-- fo-retransmit-count
|       |       |       |-- retransmit-count
|       |       |       |-- retransmit-interval
|       |       |       |-- use-vip
|       |       |-- advanced
|       |       |       |-- eap-retransmit-interval
|       |       |       |-- eap-retransmit-count
|       |       |       |-- eap-key-retransmit-interval
|       |       |       |-- eap-key-retransmit-interval-1st
|       |       |       |-- eap-key-retransmit-count
|       |       |       |-- allow-last-eap-key-timeout
|       |       |       |-- rsn-ie-ptksa-replay-counter
|       |       |       |-- rsn-ie-gtksa-replay-counter
|       |       |       |-- sta-info-free-timer-after-disassoc
|       |       |       |-- log-mic-error
|       |       |       |-- sta-auth-session-limit
|       |       |       |-- eap-failure-quiet-period
|       |       |-- guestaccess
|       |       |       |-- enable
|       |       |       |-- secure-auth-enable
|       |       |       |-- idle-session-timeout
|       |       |       |-- add-user
|       |       |       |-- del-user
|       |       |       |-- db-access-flag
|       |       |       |-- ext-primary-radius-server
|       |       |       |-- ext-secondary-radius-server
|       |       |       |-- web-server
|       |       |-- captive-portal
|       |       |       |-- web-auth
|       |       |       |       |-- auth-type
|       |       |       |       |-- after-auth
|       |       |       |       |-- redirect-url
|       |       |       |       |-- external-url
|       |       |       |       |-- downloaded-url
|       |       |       |       |-- title
|       |       |       |       |-- content
|       |       |       |       |-- message
|       |       |       |-- enable
|       |       |       |-- guest-auth
|       |       |       |-- radius-primary
|       |       |       |-- radius-secondary
|       |       |       |-- web-server
|       |       |       |-- add-user
|       |       |       |-- del-user
|       |       |-- mac-filter
|       |       |       |-- policy
|       |       |       |-- mac
|       |       |       |-- wlan_id
|       |       |       |-- name
|       |       |-- ext-wips
|       |       |       |-- enable
|       |       |       |-- interval
|       |       |       |-- primary
|       |       |       |-- secondary
|       |       |       |-- port
|       |       |       |-- user
|       |       |       |-- password
|       |-- remote-ap-group
|       |       |-- add-ap
|       |       |-- local-auth
|       |       |-- primary-radius
|       |       |-- secondary-radius
|       |-- ap-group
|       |       |-- add-wlan
|       |       |-- add-ap
|       |       |-- profile
|       |       |       |-- echo-interval
|       |       |       |-- discovery-interval
|       |       |       |-- report-interval
|       |       |       |-- statistics-timer
|       |       |       |-- retransmit-interval
|       |       |       |-- max-retransmit
|       |       |       |-- echo-retransmit-interval
|       |       |       |-- max-echo-retransmit
|       |       |       |-- ip-mode
|       |       |       |-- primary-apc
|       |       |       |-- secondary-apc
|       |       |       |-- tertiary-apc
|       |       |       |-- vlan-support
|       |       |       |-- native-vlanId
|       |       |       |-- auto-mode
|       |       |       |-- description
|       |       |       |-- telnet-enable
|       |       |       |-- ssh-enable
|       |       |       |-- led-config
|       |       |       |-- fragment-size
|       |       |       |-- discovery
|       |       |       |-- time-config
|       |       |       |       |-- mode
|       |       |       |       |-- ac-stamp-interval
|       |       |       |       |-- timezone
|       |       |-- airmove
|       |       |       |-- enable
|       |       |       |-- target-ap
|       |       |       |-- scan-trigger-level
|       |       |       |-- scan-time-channel
|       |       |       |-- scan-time-service
|       |       |       |-- scan-time-interleave
|       |       |       |-- number-of-proreq
|       |       |       |-- number-of-channel
|       |       |       |-- decision-delta
|       |-- if-group
|       |       |-- add-if
|       |-- wlan
|       |       |-- band-steering
|       |       |-- load-balancing
|       |       |-- multicast-to-unicast
|       |       |       |-- enable
|       |       |       |-- discard
|       |       |       |-- max-entry
|       |       |-- enable
|       |       |-- guest-flag
|       |       |-- radio
|       |       |-- ssid
|       |       |-- security
|       |       |       |-- apply
|       |       |       |-- wpa
|       |       |       |-- psk
|       |       |       |-- wpa2
|       |       |       |-- ieee8021x
|       |       |       |-- keymgmt
|       |       |       |-- wep
|       |       |       |-- okc
|       |       |       |-- dynamicVlan
|       |       |       |-- setDefault
|       |       |       |-- grpRekeyTime
|       |       |       |-- pmkLifeTime
|       |       |       |-- radius-server
|       |       |       |       |-- auth-servers
|       |       |       |       |-- acct-servers
|       |       |       |-- eapReauthTime
|       |       |       |-- eapolVersion
|       |       |       |-- radiusPrimaryRetryInterval
|       |       |       |-- acct_interim_interval
|       |       |       |-- layer3
|       |       |       |       |-- web-policy
|       |       |       |       |-- pre-auth-acl
|       |       |       |       |-- redirect-URL-override
|       |       |       |-- mac-filter
|       |       |-- iuts
|       |       |       |-- mode
|       |       |       |-- latency
|       |       |       |-- queue-length
|       |       |       |-- filter-mode
|       |       |       |-- codec-list
|       |       |-- if-group
|       |       |-- acl
|       |       |-- aaa-override
|       |       |-- mac-type
|       |       |-- tunnel-mode
|       |       |-- qos-class
|       |       |-- ext-wips
|       |       |-- suppress-ssid
|       |       |-- dls-allowed
|       |       |-- local-vlan
|       |       |-- max-associated-stations
|       |       |-- vdm
|       |       |       |-- multicast-info
|       |       |       |-- station-policy
|       |       |       |-- mode
|       |       |       |-- threshold
|       |       |       |-- default-policy
|       |       |       |-- join-gap
|       |       |       |-- session-timeout
|       |       |       |-- multiframing_threshold
|       |       |       |-- limit
|       |       |       |-- retry-limit
|       |       |       |-- schedule-interval
|       |       |       |-- min-mux-packets
|       |       |       |-- mux-skip-limit
|       |       |       |-- station-queue-limit
|       |       |       |-- packet-lifetime
|       |       |       |-- pifs-access
|       |       |       |-- tx-rate
|       |       |       |-- retry-ratio-update-period
|       |       |       |-- stop-threshold
|       |       |       |-- stop-interval
|       |       |       |-- start-rssi
|       |       |       |-- seq-list-size
|       |       |       |-- nack-interval
|       |       |       |-- rx-timeout
|       |       |-- sds
|       |       |       |-- weight
|       |       |-- dhcp-override
|       |       |-- ampdu
|       |       |-- reject-probe-mode
|       |-- ap
|       |       |-- profile
|       |       |       |-- dtls-policy
|       |       |       |-- discovery
|       |       |       |-- mac
|       |       |       |-- location
|       |       |       |-- name
|       |       |       |-- echo-interval
|       |       |       |-- discovery-interval
|       |       |       |-- report-interval
|       |       |       |-- statistics-timer
|       |       |       |-- retransmit-interval
|       |       |       |-- max-retransmit
|       |       |       |-- echo-retransmit-interval
|       |       |       |-- max-echo-retransmit
|       |       |       |-- ap-mode
|       |       |       |-- ip-mode
|       |       |       |-- static-ip
|       |       |       |-- sync-group
|       |       |       |-- primary-apc
|       |       |       |-- secondary-apc
|       |       |       |-- tertiary-apc
|       |       |       |-- ap-stats-history-enable
|       |       |       |-- vlan-support
|       |       |       |-- native-vlanId
|       |       |       |-- telnet-enable
|       |       |       |-- ssh-enable
|       |       |       |-- led-config
|       |       |       |-- edge-ap
|       |       |       |-- fragment-size
|       |       |       |-- client-ip
|       |       |       |-- repeater-whitelist
|       |       |       |-- wlan-vlanId
|       |       |       |-- time-config
|       |       |       |       |-- mode
|       |       |       |       |-- ac-stamp-interval
|       |       |       |       |-- timezone
|       |       |-- reboot
|       |       |-- upgrade-request
|       |       |-- tech-support
|       |       |       |-- get-all
|       |       |       |-- get-crash-file
|       |       |       |-- get-coredump
|       |       |       |-- get-log-file
|       |       |       |-- get-system-report
|       |       |-- get-if-stats
|       |       |-- syslog-config
|       |       |-- shutdown
|       |       |-- audit
|       |       |       |-- wlan-reprovisioning
|       |       |       |-- bss-status
|       |       |-- airmove
|       |       |       |-- config-priority
|       |       |       |-- scan-trigger-level
|       |       |       |-- scan-time-channel
|       |       |       |-- scan-time-service
|       |       |       |-- scan-time-interleave
|       |       |       |-- number-of-proreq
|       |       |       |-- number-of-channel
|       |       |       |-- decision-delta
|       |-- ap-all
|       |       |-- upgrade
|       |       |       |-- transfer-protocol
|       |       |       |-- start
|       |       |       |-- stop
|       |       |       |-- max-retry
|       |       |       |-- max-download
|       |       |       |-- select-package
|       |       |       |-- target
|       |       |-- reboot
|       |-- apc
|       |       |-- security-auth-type
|       |       |-- R-MAC
|       |       |-- apc-list
|       |       |       |-- add-apc
|       |       |       |-- del-apc
|       |       |       |-- change-name
|       |       |       |-- change-mac
|       |       |-- ap-mgmt-if
|       |       |-- capwap
|       |       |       |-- ctr-src-port
|       |       |       |-- window-size
|       |       |       |-- change-state-pending-timer
|       |       |       |-- data-check-timer
|       |       |       |-- dtls-session-delete
|       |       |       |-- retransmit-interval
|       |       |       |-- wait-dtls-timer
|       |       |       |-- wait-join-timer
|       |       |       |-- discovery-del-timer
|       |       |       |-- max-retransmit
|       |       |       |-- mutal-auth-enable
|       |       |       |-- discovery-by-multicast
|       |       |       |-- add-multicast-if
|       |       |       |-- discovery-by-broadcast
|       |       |       |-- auto-discovery
|       |       |       |-- auto-discovery-ap-group
|       |       |       |-- add-admin-user
|       |       |       |-- add-user
|       |       |       |-- ecn-support
|       |       |-- tech-support
|       |       |       |-- mode
|       |       |       |-- max-retry
|       |       |-- ap-stats-history
|       |       |       |-- mode
|       |       |       |-- period
|       |       |       |-- max-retry
|       |       |       |-- enable
|       |       |-- ap-if-stats
|       |       |       |-- period
|       |       |-- ap-time-config
|       |       |       |-- add-ntp
|       |       |       |-- ntp-interval
|       |       |-- service
|       |       |       |-- wlan-reprovisioning
|       |       |       |-- wlan-reprovisioning-count
|       |       |       |-- wlan-reprovisioning-interval
|       |-- redundancy
|       |       |-- fallback-enable
|       |       |-- fallback-interval
|       |       |-- add-apc
|       |       |-- del-apc
|       |-- 80211a
|       |       |-- max-associated-stations
|       |       |-- edca-parameters
|       |       |-- qos
|       |       |       |-- protocol
|       |       |       |-- edca-profile
|       |       |       |       |-- cw-min
|       |       |       |       |-- cw-max
|       |       |       |       |-- aifsn
|       |       |       |       |-- txop-limit
|       |       |       |       |-- msdu-lifetime
|       |       |       |-- policy
|       |       |       |       |-- dot1p
|       |       |       |       |       |-- enable
|       |       |       |       |       |-- policy
|       |       |       |       |-- dscp
|       |       |       |       |       |-- enable
|       |       |       |       |       |-- policy
|       |       |       |-- dot1p-tag
|       |       |       |-- dscp-tag
|       |       |       |-- ap-tags
|       |       |       |-- qap-missing-ack-retry-limit
|       |       |       |-- edca-avg-period
|       |       |       |-- reset-edca-profiles
|       |       |-- cac
|       |       |       |-- acm
|       |       |       |-- reserved-ho-calls
|       |       |       |-- max-calls
|       |       |       |-- alarming-count
|       |       |-- rate
|       |       |       |-- basic
|       |       |       |-- supported
|       |       |-- txPower
|       |       |-- channel
|       |       |-- 11n-support
|       |       |       |-- enable
|       |       |       |-- mcs
|       |       |       |-- forty-mhz
|       |       |       |-- guard-interval
|       |       |       |-- rifs
|       |       |       |-- forty-mhz-intolerant
|       |       |       |-- phy-format
|       |       |       |-- tx-stbc
|       |       |       |-- rx-stbc
|       |       |       |-- beamforming
|       |       |       |-- tx-mcs-set
|       |       |       |-- protection
|       |       |       |-- spatial-stream
|       |       |-- retry-limit
|       |       |       |-- short
|       |       |       |-- long
|       |       |-- threshold
|       |       |       |-- rts
|       |       |       |-- fragmentation
|       |       |-- msdu-lifetime
|       |       |       |-- tx
|       |       |       |-- rx
|       |       |-- beacon
|       |       |       |-- period
|       |       |-- ofdm
|       |       |       |-- channel-width
|       |       |       |-- channel-starting-factor
|       |       |       |-- ti-threshold
|       |       |-- sds
|       |       |       |-- enable
|       |       |       |-- ampdu-control
|       |       |       |-- schedule-interval
|       |       |       |-- ac
|       |       |       |       |-- scheduler
|       |       |       |       |-- wfq-metric
|       |       |       |       |-- sq-max-length
|       |       |       |       |-- sq-drop-option
|       |       |       |       |-- token-unit
|       |       |       |       |-- fs-direction
|       |       |       |       |-- sq-retry-limit
|       |       |       |       |-- long-retry-limit
|       |       |       |       |-- short-retry-limit
|       |       |       |       |-- ampdu-tx-time-limit
|       |       |-- enable
|       |       |-- cvo
|       |       |       |-- enable
|       |       |       |-- local-call-enable
|       |       |       |-- edit-profile
|       |       |       |       |-- aifsn
|       |       |       |       |-- cw-min
|       |       |       |       |-- cw-max
|       |       |       |       |-- txop-limit
|       |       |       |       |-- ampdu-limit
|       |       |       |-- set-profile
|       |       |-- rate-control
|       |       |       |-- voice
|       |       |       |       |-- max-rate
|       |       |       |       |-- probe-interval
|       |       |       |       |-- weight
|       |       |       |       |-- threshold
|       |       |       |-- video
|       |       |       |       |-- max-rate
|       |       |       |       |-- probe-interval
|       |       |       |       |-- weight
|       |       |       |       |-- threshold
|       |       |-- antenna
|       |       |-- station-kickout
|       |-- 80211bg
|       |       |-- max-associated-stations
|       |       |-- edca-parameters
|       |       |-- qos
|       |       |       |-- protocol
|       |       |       |-- edca-profile
|       |       |       |       |-- cw-min
|       |       |       |       |-- cw-max
|       |       |       |       |-- aifsn
|       |       |       |       |-- txop-limit
|       |       |       |       |-- msdu-lifetime
|       |       |       |-- policy
|       |       |       |       |-- dot1p
|       |       |       |       |       |-- enable
|       |       |       |       |       |-- policy
|       |       |       |       |-- dscp
|       |       |       |       |       |-- enable
|       |       |       |       |       |-- policy
|       |       |       |-- dot1p-tag
|       |       |       |-- dscp-tag
|       |       |       |-- ap-tags
|       |       |       |-- qap-missing-ack-retry-limit
|       |       |       |-- edca-avg-period
|       |       |       |-- reset-edca-profiles
|       |       |-- cac
|       |       |       |-- acm
|       |       |       |-- reserved-ho-calls
|       |       |       |-- max-calls
|       |       |       |-- alarming-count
|       |       |-- rate
|       |       |       |-- basic
|       |       |       |-- supported
|       |       |-- txPower
|       |       |-- channel
|       |       |-- 11n-support
|       |       |       |-- enable
|       |       |       |-- mcs
|       |       |       |-- guard-interval
|       |       |       |-- rifs
|       |       |       |-- forty-mhz-intolerant
|       |       |       |-- phy-format
|       |       |       |-- tx-stbc
|       |       |       |-- rx-stbc
|       |       |       |-- beamforming
|       |       |       |-- tx-mcs-set
|       |       |       |-- protection
|       |       |       |-- spatial-stream
|       |       |-- 11g-support
|       |       |       |-- enable
|       |       |-- retry-limit
|       |       |       |-- short
|       |       |       |-- long
|       |       |-- threshold
|       |       |       |-- rts
|       |       |       |-- fragmentation
|       |       |-- msdu-lifetime
|       |       |       |-- tx
|       |       |       |-- rx
|       |       |-- beacon
|       |       |       |-- period
|       |       |-- cca
|       |       |       |-- mode
|       |       |       |-- threshold
|       |       |-- sds
|       |       |       |-- enable
|       |       |       |-- ampdu-control
|       |       |       |-- schedule-interval
|       |       |       |-- ac
|       |       |       |       |-- scheduler
|       |       |       |       |-- wfq-metric
|       |       |       |       |-- sq-max-length
|       |       |       |       |-- sq-drop-option
|       |       |       |       |-- token-unit
|       |       |       |       |-- fs-direction
|       |       |       |       |-- sq-retry-limit
|       |       |       |       |-- long-retry-limit
|       |       |       |       |-- short-retry-limit
|       |       |       |       |-- ampdu-tx-time-limit
|       |       |-- enable
|       |       |-- cvo
|       |       |       |-- enable
|       |       |       |-- local-call-enable
|       |       |       |-- edit-profile
|       |       |       |       |-- aifsn
|       |       |       |       |-- cw-min
|       |       |       |       |-- cw-max
|       |       |       |       |-- txop-limit
|       |       |       |       |-- ampdu-limit
|       |       |       |-- set-profile
|       |       |-- rate-control
|       |       |       |-- voice
|       |       |       |       |-- max-rate
|       |       |       |       |-- probe-interval
|       |       |       |       |-- weight
|       |       |       |       |-- threshold
|       |       |       |-- video
|       |       |       |       |-- max-rate
|       |       |       |       |-- probe-interval
|       |       |       |       |-- weight
|       |       |       |       |-- threshold
|       |       |-- antenna
|       |       |-- station-kickout
|       |-- 80211h
|       |       |-- no-possess-time
|       |       |-- channel-switch
|       |       |-- power-constraint
|       |-- alarm
|       |       |-- level
|       |       |-- group
|       |       |-- logsize
|       |       |-- logcount
|       |       |-- dump
|       |       |-- backupIP
|       |       |-- stdout
|       |       |-- current-terminal
|       |-- event-filter
|       |       |-- enable
|       |-- web-service-port
|       |-- ip
|       |       |-- dhcp
|       |       |       |-- pool
|       |       |       |       |-- network
|       |       |       |       |-- range
|       |       |       |       |-- lease
|       |       |       |       |-- domain-name
|       |       |       |       |-- dns-server
|       |       |       |       |-- default-router
|       |       |       |       |-- fix-address
|       |       |       |       |-- ntp-server
|       |       |       |       |-- user-option
|       |       |       |       |-- ping-check
|       |       |       |       |-- capwap-dhcp-option
|       |       |       |-- enable
|       |       |       |-- server-ip
|       |       |-- dhcp-proxy
|       |       |       |-- timeout
|       |       |       |-- default-dhcp-server
|       |       |       |-- enable
|       |       |-- dns
|       |       |       |-- client
|       |       |       |-- relay
|       |       |       |-- name-server
|       |       |-- igmp
|       |       |       |-- limit
|       |       |       |-- snooping
|       |       |       |-- ssm-map
|       |       |       |       |-- enable
|       |       |       |       |-- static
|       |       |-- route
|       |       |-- multicast-routing
|       |       |-- pim
|       |       |       |-- accept-register
|       |       |       |-- anycast-rp
|       |       |       |-- bsr-candidate
|       |       |       |-- cisco-register-checksum
|       |       |       |-- crp-cisco-prefix
|       |       |       |-- ignore-rp-set-priority
|       |       |       |-- jp-timer
|       |       |       |-- register-rate-limit
|       |       |       |-- register-rp-reachability
|       |       |       |-- register-source
|       |       |       |-- register-suppression
|       |       |       |-- rp-address
|       |       |       |-- rp-register-kat
|       |       |       |-- spt-threshold
|       |       |       |-- rp-candidate
|       |       |       |       |-- interval
|       |       |       |       |       |-- priority
|       |       |       |       |       |       |-- group-list
|       |       |-- nat
|       |-- access-list
|       |-- http
|       |-- https
|       |-- arp
|       |-- firewall
|       |-- wlan-arp-mode
|       |-- package
|       |       |-- upgrade
|       |-- stats-report
|       |       |-- enable
|       |       |-- upload
|       |       |-- target
|       |       |-- current-stats
|       |-- telnet-server
|       |       |-- enable
|       |       |-- port
|       |-- ssh-server
|       |       |-- enable
|       |       |-- port
|       |-- sftp-server
|       |       |-- enable
|       |       |-- chguser
|       |-- ftp-server
|       |       |-- enable
|       |       |-- port
|       |       |-- chguser
|       |-- clock
|       |       |-- set
|       |       |-- timezone
|       |-- ntp
|       |       |-- server
|       |       |       |-- enable
|       |       |-- client
|       |       |       |-- enable
|       |       |       |-- interval
|       |       |       |-- server-addr
|       |       |       |       |-- ip
|       |       |       |       |-- hostname
|       |-- syslog
|       |       |-- enable
|       |       |-- add
|       |       |-- del
|       |       |-- level
|       |-- bridge
|       |       |-- protocol
|       |       |       |-- ieee
|       |       |       |-- mstp
|       |       |       |-- rstp
|       |       |-- ageing-time
|       |       |-- address
|       |       |       |-- discard
|       |       |       |       |-- vlan
|       |       |       |-- forward
|       |       |       |       |-- vlan
|       |       |-- max-age
|       |       |-- forward-time
|       |       |-- hello-time
|       |       |-- instance
|       |       |-- max-hops
|       |       |-- spanning-tree
|       |       |       |-- enable
|       |       |       |-- errdisable-timeout
|       |       |       |       |-- enable
|       |       |       |       |-- interval
|       |       |       |-- portfast
|       |       |       |       |-- bpdu-filter
|       |       |       |       |-- bpdu-guard
|       |       |-- rapid-spanning-tree
|       |       |       |-- enable
|       |       |-- multiple-spanning-tree
|       |       |       |-- enable
|       |       |-- priority
|       |       |-- transmit-holdcount
|       |-- spanning-tree
|       |       |-- bridge
|       |       |       |-- instance
|       |       |       |       |-- vlan
|       |       |       |-- region
|       |       |       |-- revision
|       |-- vlan
|       |       |-- vlan
|       |-- interface
|       |       |-- switchport
|       |       |       |-- mode
|       |       |       |-- access
|       |       |       |-- trunk
|       |       |       |       |-- add
|       |       |       |       |-- except
|       |       |       |       |-- remove
|       |       |       |       |-- all
|       |       |       |       |-- none
|       |       |       |-- hybrid
|       |       |       |       |-- allowed
|       |       |       |       |       |-- add
|       |       |       |       |       |-- remove
|       |       |       |       |       |-- all
|       |       |       |       |       |-- none
|       |       |       |       |-- vlan
|       |       |-- static-channel-group
|       |       |-- channel-group
|       |       |-- flowcontrol
|       |       |-- storm-control
|       |       |       |-- level
|       |       |-- bridge-group
|       |       |       |-- instance
|       |       |       |       |-- path-cost
|       |       |       |       |-- priority
|       |       |       |-- priority
|       |       |       |-- path-cost
|       |       |-- mirror
|       |       |       |-- interface
|       |       |       |       |-- direction
|       |       |-- ip
|       |       |       |-- address
|       |       |       |-- igmp
|       |       |       |       |-- ra-option
|       |       |       |       |-- access-group
|       |       |       |       |-- immediate-leave
|       |       |       |       |-- last-member-query-count
|       |       |       |       |-- last-member-query-interval
|       |       |       |       |-- limit
|       |       |       |       |       |-- except
|       |       |       |       |-- mroute-proxy
|       |       |       |       |-- querier-timeout
|       |       |       |       |-- query-interval
|       |       |       |       |-- query-max-response-time
|       |       |       |       |-- robustness-variable
|       |       |       |       |-- snooping
|       |       |       |       |       |-- fast-leave
|       |       |       |       |       |-- mrouter
|       |       |       |       |       |-- querier
|       |       |       |       |       |-- report-suppression
|       |       |       |       |-- static-group
|       |       |       |       |       |-- interface
|       |       |       |       |       |-- source
|       |       |       |       |       |       |-- interface
|       |       |       |       |-- version
|       |       |       |-- pim
|       |       |       |       |-- sparse-mode
|       |       |       |       |-- bsr-border
|       |       |       |       |-- dr-priority
|       |       |       |       |-- exclude-genid
|       |       |       |       |-- hello-holdtime
|       |       |       |       |-- hello-interval
|       |       |       |       |-- neighbor-filter
|       |       |       |       |-- propagation-delay
|       |       |       |       |-- unicast-bsm
|       |       |       |-- access-group
|       |       |       |-- nat
|       |       |       |-- proxy-arp
|       |       |       |-- tcp-adjust-mss
|       |       |       |-- rip
|       |       |       |       |-- authentication
|       |       |       |       |       |-- key-chain
|       |       |       |       |       |-- mode
|       |       |       |       |       |-- string
|       |       |       |       |-- receive
|       |       |       |       |       |-- version
|       |       |       |       |-- receive-packet
|       |       |       |       |-- send
|       |       |       |       |       |-- version
|       |       |       |       |-- send-packet
|       |       |       |       |-- split-horizon
|       |       |       |-- ospf
|       |       |       |       |-- address
|       |       |       |       |       |-- authentication
|       |       |       |       |       |-- authentication-key
|       |       |       |       |       |-- cost
|       |       |       |       |       |-- database-filter
|       |       |       |       |       |-- dead-interval
|       |       |       |       |       |-- hello-interval
|       |       |       |       |       |-- message-digest-key
|       |       |       |       |       |       |-- md5
|       |       |       |       |       |-- mtu-ignore
|       |       |       |       |       |-- priority
|       |       |       |       |       |-- retransmit-interval
|       |       |       |       |       |-- transmit-delay
|       |       |       |       |-- authentication
|       |       |       |       |-- authentication-key
|       |       |       |       |-- cost
|       |       |       |       |-- database-filter
|       |       |       |       |-- dead-interval
|       |       |       |       |-- hello-interval
|       |       |       |       |-- message-digest-key
|       |       |       |       |       |-- md5
|       |       |       |       |-- mtu-ignore
|       |       |       |       |-- priority
|       |       |       |       |-- retransmit-interval
|       |       |       |       |-- transmit-delay
|       |       |       |       |-- disable
|       |       |       |       |-- mtu
|       |       |       |       |-- network
|       |       |-- shutdown
|       |       |-- traffic-shape
|       |       |-- service-policy
|       |       |-- dhcp
|       |       |       |-- server
|       |       |       |-- option-82
|       |       |-- arp-ageing-timeout
|       |       |-- speed-duplex
|       |       |-- mtu
|       |       |-- spanning-tree
|       |       |       |-- autoedge
|       |       |       |-- edgeport
|       |       |       |-- force-version
|       |       |       |-- guard
|       |       |       |-- hello-time
|       |       |       |-- instance
|       |       |       |       |-- path-cost
|       |       |       |       |-- priority
|       |       |       |       |-- restricted-role
|       |       |       |       |-- restricted-tcn
|       |       |       |-- link-type
|       |       |       |-- path-cost
|       |       |       |-- portfast
|       |       |       |       |-- bpdu-filter
|       |       |       |       |-- bpdu-guard
|       |       |       |-- priority
|       |       |       |-- restricted-role
|       |       |       |-- restricted-tcn
|       |       |       |-- transmit-holdcount
|       |-- vrrp
|       |-- router
|       |       |-- rip
|       |       |       |-- cisco-metric-behavior
|       |       |       |-- default-information
|       |       |       |-- default-metric
|       |       |       |-- distance
|       |       |       |-- distribute-list
|       |       |       |-- maximum-prefix
|       |       |       |-- neighbor
|       |       |       |-- network
|       |       |       |-- offset-list
|       |       |       |-- passive-interface
|       |       |       |-- recv-buffer-size
|       |       |       |-- redistribute
|       |       |       |       |-- metric
|       |       |       |       |-- route-map
|       |       |       |-- route
|       |       |       |-- timers
|       |       |       |       |-- basic
|       |       |       |-- version
|       |       |-- ospf
|       |       |       |-- area
|       |       |       |       |-- authentication
|       |       |       |       |-- default-cost
|       |       |       |       |-- filter-list
|       |       |       |       |-- nssa
|       |       |       |       |       |-- default-information-originate
|       |       |       |       |       |       |-- metric
|       |       |       |       |       |       |-- metric-type
|       |       |       |       |       |       |-- no-redistribution
|       |       |       |       |       |       |-- no-summary
|       |       |       |       |       |       |-- translator-role
|       |       |       |       |       |-- no-redistribution
|       |       |       |       |       |-- no-summary
|       |       |       |       |       |-- translator-role
|       |       |       |       |-- range
|       |       |       |       |-- shortcut
|       |       |       |       |-- stub
|       |       |       |       |-- virtual-link
|       |       |       |       |       |-- authentication
|       |       |       |       |       |-- authentication-key
|       |       |       |       |       |-- dead-interval
|       |       |       |       |       |-- hello-interval
|       |       |       |       |       |-- message-digest-key
|       |       |       |       |       |       |-- md5
|       |       |       |       |       |-- retransmit-interval
|       |       |       |       |       |-- transmit-delay
|       |       |       |-- auto-cost
|       |       |       |-- capability
|       |       |       |       |-- opaque
|       |       |       |-- compatible
|       |       |       |-- default-information
|       |       |       |       |-- always
|       |       |       |       |-- metric
|       |       |       |       |-- metric-type
|       |       |       |       |-- route-map
|       |       |       |-- default-metric
|       |       |       |-- distance
|       |       |       |       |-- admin
|       |       |       |       |-- ospf
|       |       |       |-- distribute-list
|       |       |       |       |-- in
|       |       |       |       |-- out
|       |       |       |-- host
|       |       |       |       |-- area
|       |       |       |-- max-concurrent-dd
|       |       |       |-- maximum-area
|       |       |       |-- neighbor
|       |       |       |       |-- cost
|       |       |       |       |-- poll-interval
|       |       |       |       |-- priority
|       |       |       |-- network
|       |       |       |       |-- area
|       |       |       |-- ospf
|       |       |       |       |-- abr-type
|       |       |       |       |-- router-id
|       |       |       |-- overflow
|       |       |       |       |-- database
|       |       |       |-- passive-interface
|       |       |       |-- redistribute
|       |       |       |       |-- metric
|       |       |       |       |-- metric-type
|       |       |       |       |-- route-map
|       |       |       |       |-- tag
|       |       |       |-- router-id
|       |       |       |-- summary-address
|       |       |       |-- timers
|       |       |       |       |-- spf
|       |       |       |       |       |-- exp
|       |       |-- vrrp
|       |       |       |-- advertisement-interval
|       |       |       |-- circuit-failover
|       |       |       |-- disable
|       |       |       |-- enable
|       |       |       |-- preempt-mode
|       |       |       |-- preempt-delay
|       |       |       |-- priority
|       |       |       |-- virtual-ip
|       |-- os-aware
|       |       |-- os-aware
|       |       |-- delete
|       |       |-- update
|       |-- ipwatch
|       |-- ftp
|       |-- stationtracking
|       |       |-- station
|       |       |-- on
|       |       |-- off
|       |-- fqm-mode
|       |       |-- access-list
|       |       |-- class-map
|       |       |       |-- match
|       |       |       |       |-- access-group
|       |       |       |       |-- class
|       |       |       |       |-- cos
|       |       |       |       |-- dst
|       |       |       |       |-- ip
|       |       |       |       |       |-- dscp
|       |       |       |       |       |-- precedence
|       |       |       |       |       |-- tos
|       |       |       |       |-- protocol
|   |   |   |   |-- src
|   |   |   |-- match-type
|   |   |-- no
|   |   |-- policy-map
|   |   |   |-- class
|   |   |   |   |-- police
|   |   |   |   |   |-- cir
|   |   |   |   |-- mark
|   |   |   |   |   |-- cos
|   |   |   |   |   |-- ip
|   |   |   |   |   |   |-- dscp
|   |   |   |   |   |   |-- precdence
|   |   |   |   |   |-- priority
|   |   |   |   |-- bandwidth
|   |   |   |   |-- shape-peak
|   |   |   |   |-- queue-limit
|   |   |-- ip
|   |   |-- time-profile
|   |   |   |-- day-start
|   |   |-- update
|   |   |   |-- access-list
|   |-- if-arbiter
|   |-- sipalg
|   |   |-- enable
|   |   |-- sip-error-resp-enable
|   |   |-- monitor-port
|   |   |-- sip-detect-long-call-enable
|   |   |-- sip-long-call-timeout
|   |-- rrm
|   |   |-- enable
|   |   |-- 80211a
|   |   |   |-- dpc
|   |   |   |   |-- enable
|   |   |   |   |-- periodic-interval
|   |   |   |   |-- rssi-threshold
|   |   |   |   |-- txPower
|   |   |   |-- dcs
|   |   |   |   |-- enable
|   |   |   |   |-- periodic-interval
|   |   |   |   |-- anchor-time
|   |   |   |   |-- interference-level-threshold
|   |   |   |   |-- channel-utilization-threshold
|   |   |   |   |-- my-utilization-threshold
|       |       |       |       |-- channel
|       |       |       |       |-- aware-option
|       |       |       |       |-- delayed-channel-change
|       |       |       |-- chdc
|       |       |       |       |-- enable
|       |       |       |       |-- statsCollectEnable
|       |       |       |       |-- statsWarningEnable
|       |       |       |       |-- statsActionEnable
|       |       |       |       |-- statsCollectInterval
|       |       |       |       |-- rssi-threshold
|       |       |       |       |-- min-failed-client-count
|       |       |       |       |-- percent-failed-client-count
|       |       |-- 80211b
|       |       |       |-- dpc
|       |       |       |       |-- enable
|       |       |       |       |-- periodic-interval
|       |       |       |       |-- rssi-threshold
|       |       |       |       |-- txPower
|       |       |       |-- dcs
|       |       |       |       |-- enable
|       |       |       |       |-- periodic-interval
|       |       |       |       |-- anchor-time
|       |       |       |       |-- interference-level-threshold
|       |       |       |       |-- channel-utilization-threshold
|       |       |       |       |-- my-utilization-threshold
|       |       |       |       |-- channel
|       |       |       |       |-- aware-option
|       |       |       |       |-- delayed-channel-change
|       |       |       |-- chdc
|       |       |       |       |-- enable
|       |       |       |       |-- statsCollectEnable
|       |       |       |       |-- statsWarningEnable
|       |       |       |       |-- statsActionEnable
|       |       |       |       |-- statsCollectInterval
|       |       |       |       |-- rssi-threshold
|       |       |       |       |-- min-failed-client-count
|       |       |       |       |-- percent-failed-client-count
|       |       |-- rf-group-name
|       |       |-- sub-channel-group
|       |       |       |-- enable
|       |       |       |-- disable
|       |       |       |-- group-name
|       |       |       |-- add-ap
|       |       |       |-- del-ap
|       |       |       |-- add-channel
|       |       |       |-- del-channel
|       |-- cluster
|       |       |-- keep-alive-interval
|       |       |-- keep-alive-retry-count
|       |       |-- enable
|       |       |-- add-apc
|       |       |-- del-apc
|       |       |-- del-apc-all
|       |-- wids
|       |       |-- enable
|       |       |-- ap-blacklist
|       |       |-- client-blacklist
|       |       |-- ssid-whitelist
|       |       |-- oui-whitelist
|       |       |-- friendlylist
|       |       |-- rogue
|       |       |       |-- expiration-timeout
|       |       |       |-- remove
|       |       |       |-- move
|       |       |       |-- modify-state
|       |       |       |-- adhoc-connection-detection
|       |       |       |-- ap
|       |       |       |       |-- ap-blacklist-check
|       |       |       |       |-- managed_ssid_invalid_security
|       |       |       |       |-- illegal-channel-detection
|       |       |       |       |-- unknownap
|       |       |       |       |       |-- managed-ssid-withauth-client-det
|       |       |       |       |       |-- wired-netwrok-detection
|       |       |       |       |-- fakeap
|       |       |       |       |       |-- managed-ssid-detection
|       |       |       |       |       |-- beacon-without-ssid-detection
|       |       |       |       |       |-- beacon-on-invalid-channel-detection
|       |       |       |       |-- managedap
|       |       |       |       |       |-- invalid-ssid-detection
|       |       |       |-- client
|       |       |       |       |-- oui-list-check
|       |       |       |       |-- auth-request-det
|       |       |       |       |-- probe-request-det
|       |       |       |       |-- deauth-request-det
|       |       |       |       |-- assoc-fail-det
|       |       |       |       |-- auth-fail-det
|       |       |       |       |-- oneXauth-fail-det
|       |       |       |       |-- webauth-fail-det
|       |       |       |       |-- exclusion-list-check
|       |       |       |       |-- allowed-limit
|       |       |       |-- add-friendly-rule
|       |       |       |-- del-friendly-rule
|       |       |       |-- modify-friendly-rule
|       |       |       |-- add-malicious-rule
|       |       |       |-- del-malicious-rule
|       |       |       |-- modify-malicious-rule
|       |       |-- channel-validation
|       |       |       |-- enable
|       |       |       |-- add
|       |       |       |-- delete
|       |-- monitor-radio
|       |       |-- scan-interval
|       |       |-- periodic-interval
|       |-- snmp
|       |       |-- community
|       |       |-- user
|       |       |-- trap
|       |       |-- trap-source-ip
|       |-- pcap
|       |       |-- mode
|       |       |-- start-service
|       |       |-- filter
|       |       |       |-- station-mac
|       |       |       |-- enable-station-mac
|       |       |       |-- ap-mac
|       |       |       |-- enable-ap-mac
|       |-- wlan-radio-service
|       |       |-- sta-idle-timeout
|       |       |-- wmm-mode
|       |       |-- dtim
|       |-- preferred-calls
|       |       |-- add
|       |       |-- del
|       |-- locationtrack
|       |       |-- autotrace
|       |       |-- algorithm
|       |       |-- enable
|       |       |-- ap
|       |       |-- station
|       |       |-- rogueap
|       |       |-- roguestation
|       |       |-- expiryhistory
|       |-- vcc
|       |       |-- scme-if
|       |       |-- add-user
|       |       |-- handover
|       |       |-- enable
|       |-- voice
|       |       |-- monitor
|       |       |       |-- enable
|       |       |       |-- interval
|       |       |       |-- fieldType
|       |       |       |       |-- ip
|       |       |       |       |-- mac
|       |       |       |       |-- user-name
|       |       |       |       |-- phone-no
|       |       |-- vqm
|       |       |       |-- enable
|       |       |       |-- connection-limit
|       |       |       |-- reporting-mode
|       |       |       |-- periodic-timer
|       |       |       |-- session-idle-timer
|       |       |       |-- rtp-port-range
|       |       |       |-- alarm
|       |       |       |       |-- enable
|       |       |       |       |-- threshold
|       |       |       |-- upload
|       |       |       |       |-- enable
|       |       |       |       |-- server
|       |       |       |       |-- interval
|       |       |       |       |-- mode
|       |       |       |       |-- user-login
|       |       |       |       |-- target-directory
|       |       |       |       |-- file-size
|       |       |       |       |-- immediate-upload
|       |       |       |-- filter
|       |       |       |       |-- prefix
|       |-- router-id
|       |-- route-map
|       |       |-- match
|       |       |       |-- interface
|       |       |       |-- ip
|    |    |    |-- metric
|    |    |    |-- route-type
|    |    |    |-- tag
|    |    |-- set
|    |    |    |-- dampening
|    |    |    |-- ip
|    |    |    |-- metric
|    |    |    |-- metric-type
|    |    |    |-- tag
```

A.2 show

```
|-- show
|       |-- band-steering
|       |-- load-balancing
|       |-- air-quality
|       |       |-- count
|       |       |       |-- interferers
|       |       |       |-- worst-interferers
|       |-- spectrum-analysis
|       |       |-- config
|       |       |       |-- ap
|       |       |-- report
|       |       |       |-- duty_cycle
|       |       |       |       |-- ap
|       |       |       |-- sample
|       |       |       |       |-- ap
|       |       |       |-- interference
|       |       |       |       |-- ap
|       |-- mgmt-users
|       |-- command-log
|       |-- cli-idle-timeout
|       |-- cli-sessions
|       |-- country
|       |       |-- global-config
|       |       |-- ap-config
|       |       |-- information
|       |-- voip
|       |       |-- config
|       |       |-- call-info
|       |-- vcc
|       |       |-- connect-status
|       |       |-- msg-counts
|       |-- 80211a
|       |       |-- cac
|       |       |       |-- configuration
|       |       |-- summary
|       |       |-- qos
|       |       |       |-- policy
|       |       |       |-- ac-profile
|       |       |       |-- edca-parameters
|       |       |       |-- radio-configuration
|       |       |-- radio-config
|       |       |-- voip-stats
```

```
|       |       |-- cvo
|       |       |       |-- profile
|       |       |       |-- config
|       |       |       |-- neighbors
|       |       |       |-- channel-info
|       |       |       |-- call-count
|       |       |       |-- heads
|       |-- 80211bg
|       |       |-- cac
|       |       |       |-- configuration
|       |       |-- summary
|       |       |-- qos
|       |       |       |-- policy
|       |       |       |-- ac-profile
|       |       |       |-- edca-parameters
|       |       |       |-- radio-configuration
|       |       |-- radio-config
|       |       |-- voip-stats
|       |       |-- cvo
|       |       |       |-- profile
|       |       |       |-- config
|       |       |       |-- neighbors
|       |       |       |-- channel-info
|       |       |       |-- call-count
|       |       |       |-- heads
|       |-- 80211h
|       |       |-- configuration
|       |       |-- prohibit-channels
|       |-- qos
|       |       |-- profile
|       |-- wlan-radio-service
|       |       |-- config
|       |       |-- msg-counts
|       |-- handover
|       |-- airmove
|       |       |-- ap
|       |       |-- group
|       |-- station
|       |       |-- stats
|       |       |       |-- management_frame
|       |       |       |       |-- all
|       |       |       |-- NCHO
|       |       |       |       |-- all
|       |       |       |-- IAHO
|       |       |       |       |-- all
|       |       |       |-- debug
|       |       |       |       |-- all
|       |       |       |-- ap-80211-stats
|       |       |-- association
|       |       |       |-- history
|       |       |-- summary
|       |       |       |-- ap
|       |       |       |-- bssid
|       |       |       |-- wlan
|       |       |-- detail
|       |       |-- data
|       |       |       |-- configuration
|       |       |       |-- wlan
|       |       |       |-- radio
|       |       |       |-- ap
|       |       |       |-- ap-packet-loss
|       |       |       |-- ap-packet-loss-raw
|       |       |       |-- device
|       |       |       |-- worst_wlan
|       |       |       |-- worst_radio
|       |       |       |-- global_stats
|       |-- system
|       |       |-- info
|       |       |-- uptime
|       |       |-- load
|       |       |-- cpu
|       |       |-- memory
|       |       |-- disk
|       |       |-- fan
|       |       |-- temp
|       |       |-- threshold
|       |       |       |-- cpu
|       |       |       |-- memory
|       |       |       |-- disk
|       |       |       |-- fan
|       |       |       |-- temp
|       |       |-- fancontrol
|       |       |-- license-key
|       |-- remote-ap-group
|       |       |-- summary
|       |       |-- user-state
|       |       |-- detail
|       |-- ap-group
|       |       |-- summary
|       |       |-- detail
|       |       |-- time-config
|       |-- ap
|       |       |-- upgrade
|       |       |       |-- summary
|       |       |       |-- list
|       |       |-- summary
|       |       |-- detail
|       |       |-- wlan-vlan
|       |       |-- stats-history
|       |       |-- if-stats
|       |       |-- join-stats
|       |       |-- capwap-stats
|       |       |-- radio-stats
|       |       |-- tech-support
|       |       |-- time-config
|       |       |-- syslog-config
|       |-- apc
|       |       |-- summary
|       |       |-- list
|       |       |-- capwap
|       |       |       |-- summary
|       |       |-- ap-if-stats
|       |-- redundancy
|       |       |-- summary
|       |       |-- priority-list
|       |-- wlan
|       |       |-- summary
|       |       |-- detail
|       |       |-- security
|       |       |       |-- summary
|       |       |       |-- detail
|       |-- vap
|       |-- if-group
|       |-- alarm
|       |       |-- info
|       |       |-- conf
|       |       |-- list
|       |       |       |-- all
|       |       |       |-- level
|       |       |       |-- group
|       |       |-- history
|       |       |       |-- all
|       |       |       |-- level
|       |       |       |-- group
|       |       |-- backup
|       |-- event
|       |-- running-config
|       |       |-- system
|       |       |-- cli-idle-timeout
|       |       |-- alarm
|       |       |-- network
|       |       |-- snmp
|       |       |-- wifim
|       |       |-- vqm
|       |       |-- voice-vqm
|       |       |-- apc
|       |       |-- capwap
|       |       |-- if-group
|       |       |-- wlan
|       |       |-- wlan-security
|       |-- tech-support
|       |       |-- version
|       |       |-- uptime
|       |       |-- system
|       |       |-- cpu
|       |       |-- load
|       |       |-- memory
|       |       |-- disk
|       |       |-- process
|       |       |-- processlog
|       |       |-- processmemory
|       |       |-- coredump
|       |       |-- crash
|       |       |-- swm-log
|       |       |-- alarm
|       |       |-- debug
|       |       |-- cluster
|       |       |-- redundancy
|       |       |-- cli-idle-timeout
|       |       |-- network
|       |       |-- snmp
|       |       |-- wifim
|       |       |-- vqm
|       |       |-- apc
|       |       |-- capwap
|       |       |-- if-group
|       |       |-- wlan
|       |       |-- wlan-security
|       |       |-- rrm
|       |       |-- alarmhistory
|       |       |-- event
|       |       |-- wids
|       |-- ip
|       |       |-- dhcp
|       |       |       |-- pool
|       |       |       |-- lease
|       |       |       |-- proxy-lease
|       |       |       |-- statistics
|       |       |       |-- process
|       |       |-- dhcp-proxy
|       |       |-- dns
|       |       |       |-- name-server
|       |       |       |-- relay
|       |       |       |       |-- cache
|       |       |       |       |-- cache-info
|       |       |-- igmp
|       |       |       |-- groups
|       |       |       |-- interface
|       |       |       |-- snooping
|       |       |       |       |-- mroute
|       |       |       |       |-- statistics
|       |       |       |-- ssm-map
|       |       |-- route
|       |       |-- interface
|       |       |-- rip
|       |       |-- protocols
|       |       |-- nat
|       |       |-- access-list
|       |       |-- filter
|       |       |-- pim
|       |       |       |-- sparse-mode
|       |       |       |       |-- bsr-router
|       |       |       |       |-- interface
|       |       |       |       |-- local-members
|       |       |       |       |-- mroute
|       |       |       |       |-- neighbor
|       |       |       |       |-- nexthop
|       |       |       |       |-- rp
|       |       |       |       |-- rp-hash
|       |       |-- ospf
|       |       |       |-- border-routers
|       |       |       |-- database
|       |       |       |       |-- adv-router
|       |       |       |       |-- asbr-summary
|       |       |       |       |-- external
|       |       |       |       |-- max-age
|       |       |       |       |-- network
|       |       |       |       |-- nssa-external
|       |       |       |       |-- opaque-area
|       |       |       |       |-- opaque-as
|       |       |       |       |-- opaque-link
|       |       |       |       |-- router
|       |       |       |       |-- self-originate
|       |       |       |       |-- summary
|       |       |       |-- neighbor
|       |       |       |-- route
|       |       |       |-- virtual-links
|       |-- access-list
|       |-- arp
|       |-- wireless-acl-list
|       |-- multi2uni-list
|       |-- interface
|       |-- vlan
|       |-- mirror
|       |-- reboot
|       |-- processes
|       |       |-- status
|       |       |-- log
|       |       |-- memory
|       |-- version
|       |-- syslog
|       |-- debug
|       |       |-- coredump
|       |       |       |-- summary
|       |       |-- reboot
|       |       |       |-- info
|       |       |       |-- summary
|       |       |       |-- export
|       |       |-- log
|       |       |       |-- all
|       |       |       |-- level
|       |       |       |-- module
|       |       |       |-- conf
|       |       |       |-- backup
|       |       |       |-- keyword
|       |       |       |-- detail
|       |       |       |       |-- all
|       |       |       |       |-- level
|       |       |       |       |-- module
|       |       |       |       |-- backup
|       |       |       |       |-- conf
|       |       |       |       |-- keyword
|       |       |       |       |-- before
|       |       |       |       |-- after
|       |       |       |       |-- start-time
|       |       |       |-- before
|       |       |       |-- after
|       |       |       |-- start-time
|       |       |-- swm-log
|       |       |-- processes
|       |       |-- apm
|       |       |       |-- msg-count
|       |       |       |-- disk-size
|       |       |       |-- timer
|       |       |       |-- test-result
|       |       |       |-- end-message
|       |       |       |-- shared-memory
|       |       |-- event
|       |-- ssh-server
|       |-- telnet-server
|       |-- ftp-server
|       |-- filter
|       |-- filter-stats
|       |-- policy-map
|       |-- class-map
|       |-- firewall
|       |-- sftp-server
|       |-- ntp
|       |-- timezone
|       |-- clock
|       |-- event-filter
|       |-- security
|       |       |-- radius-server
|       |       |       |-- config
|       |       |       |-- summary
|       |       |       |-- detail
|       |       |       |-- stats
|       |       |-- advanced
|       |       |-- hapd-stats
|       |       |-- hapd-ap-stats
|       |       |-- guestaccess
|       |       |       |-- help
|       |       |       |-- current-config
|       |       |       |-- config-user-detail
|       |       |-- captive-portal
|       |       |       |-- stats
|       |       |       |-- running-info
|       |       |       |-- config
|       |       |       |-- guest
|       |       |       |-- web-auth
|       |       |       |-- rad-msg
|       |       |       |-- rad-retrans
|       |       |       |-- failed-sta
|       |       |-- mac-filter
|       |       |       |-- summary
|       |       |       |-- detail
|       |       |-- ext-wips
|       |       |       |-- config
|       |       |       |-- list
|       |-- vrrp
|       |-- static-channel-group
|       |-- bridge
|       |-- etherchannel
|       |-- spanning-tree
|       |       |-- mst
|       |       |       |-- config
|       |       |       |-- detail
|       |       |       |       |-- interface
|       |       |       |-- instance
|       |       |       |       |-- interface
|       |       |       |-- interface
|       |       |-- interface
|       |-- sipalg
|       |       |-- configuration
|       |       |-- stats
|       |       |-- call
|       |       |       |-- summary
|       |       |       |-- detail
|       |-- rrm
|       |       |-- config-summary
|       |       |-- help
|       |       |-- neighbor-list
|       |       |-- channel-status
|       |       |-- rrm-history
|       |       |-- sub-channel-group
|       |-- locationtrack
|       |       |-- help
|       |       |-- config
|       |       |-- ap
|       |       |-- floor
|       |       |-- station
|       |       |-- rogueap
|       |       |-- roguestation
|       |-- debugging
|       |       |-- lacp
|       |-- port
|       |-- lacp
|       |-- http
|       |-- https
|       |-- snmp
|       |       |-- community
|       |       |-- user
|       |       |-- trap
|       |-- pcap
|       |       |-- current-config
|       |-- cluster
|       |       |-- config
|       |       |-- current-stats-all
|       |       |-- current-stats-apc
|       |       |-- help
|       |       |-- list-apc
|       |       |-- list-station
|       |       |-- summary-stats-all
|       |       |-- summary-stats-apc
|       |-- wids
|       |       |-- help
|       |       |-- statistics
|       |       |-- current-config
|       |       |-- lists
|       |       |       |-- ap-whitelist
|       |       |       |-- ap-blacklist
|       |       |       |-- client-whitelist
|       |       |       |-- client-blacklist
|       |       |       |-- friendlylist
|       |       |       |-- oui-list
|       |       |       |-- ssid-whitelist
|       |       |-- rogue
|       |       |       |-- ap
|       |       |       |       |-- current-config
|       |       |       |       |-- list
|       |       |       |       |-- detail
|       |       |       |-- client
|       |       |       |       |-- current-config
|       |       |       |       |-- allow-limit
|       |       |       |       |-- list
|       |       |       |       |-- detail
|       |       |       |-- adhoc
|       |       |       |       |-- list
|       |       |       |       |-- detail
|       |       |       |-- rule
|       |       |       |       |-- friendly
|       |       |       |       |-- malicious
|       |-- wips
|       |       |-- help
|       |       |-- current-config
|       |-- stats-report
|       |       |-- conf
|       |       |-- current-stats
|       |-- stationtracking
|       |       |-- station
|       |       |-- conf
|       |-- preferred-calls
|       |-- vdm
|       |       |-- config
|       |       |-- policy-for-station
|       |-- sds
|       |       |-- radio
|       |       |-- wlan
|       |-- config-files
|       |-- rate-control
|       |-- tx-power-range
|       |-- os-aware
|       |-- os-aware-all
|       |-- monitor-radio
|       |-- voice
|       |       |-- station
|       |       |       |-- summary
|       |       |       |-- detail
|       |       |       |       |-- mac
|       |       |       |       |-- ip
|       |       |       |       |-- user-name
|       |       |       |       |-- tel-no
|       |       |-- active-call
|       |       |       |-- summary
|       |       |       |-- detail
|       |       |       |       |-- mac
|       |       |       |       |-- ip
|       |       |       |       |-- user-name
|       |       |       |       |-- tel-no
|       |       |-- complete-call
|       |       |       |-- summary
|       |       |       |-- detail
|       |       |       |       |-- mac
|       |       |       |       |-- ip
|       |       |       |       |-- user-name
|       |       |       |       |-- tel-no
|       |       |-- vqm
|       |       |       |-- help
|       |       |       |-- current-config
|       |       |       |-- summary-stats
|       |       |       |-- debug-stats
|       |       |       |-- current-stats
|       |       |       |-- history-stats
|       |       |       |-- alarms
|       |       |-- statistics
|       |       |       |-- ap
|       |       |       |-- radio
|       |       |       |-- wlan
|       |       |       |-- device
|       |       |       |-- station
|       |       |-- event
|       |       |-- sipmsg-log
|       |       |-- device
|       |       |-- debug-stats
|       |-- bss-if
```

A.3 clear

```
|-- clear
|       |-- air-quality
|       |       |-- count
|       |       |       |-- interferers
|       |-- stats
|       |       |-- station
|       |       |       |-- globally
|       |       |       |-- individually
|       |-- interference
|       |       |-- report
|       |-- vap
|       |-- ip
|       |       |-- igmp
|       |       |       |-- group
|       |       |       |-- interface
|       |       |-- rip
|       |       |-- pim
|       |       |       |-- sparse-mode
|       |       |-- nat
|       |       |-- ospf
|       |-- spanning-tree
|       |       |-- bridge
|       |       |-- interface
|       |-- 80211a
|       |       |-- voip-stats
|       |-- 80211bg
|       |       |-- voip-stats
|       |-- preferred-calls
|       |-- wlan-radio-service
|       |-- vcc-msg-counts
|       |-- cli-session
|       |-- interface
|       |-- arp-cache
|       |-- voice
|       |       |-- vqm
|       |       |       |-- all
|       |       |       |-- history-stats
|       |       |       |-- summary-stats
|       |       |       |-- current-stats
|       |       |       |-- history-file
|       |       |       |-- debug-stats
|       |       |-- active-call
```

```
|       |       |-- statistics
|       |       |-- event
|       |       |-- sipmsg-log
|       |       |-- debug-stats
|       |-- sipalg
|       |       |-- stats
|       |-- pcap-stat
|       |-- security
|       |       |-- radius-server
|       |       |       |-- stats
|       |       |-- hapd-stats
|       |       |-- hapd-ap-stats
|       |       |-- captive-portal
|       |       |       |-- stats
|       |-- cluster
|       |       |-- clear-all
|       |       |-- clear-apc
|       |-- log
|       |       |-- debug
|       |       |       |-- current
|       |       |       |-- all
|       |       |       |-- detail
|       |       |       |       |-- current
|       |       |       |       |-- all
|       |       |-- alarm
|       |       |-- actalarm
|       |       |-- alarminfo
|       |-- vrrp
```

A.4 debug

```
|-- debug
|       |-- processes
|       |       |-- config
|       |-- crash
|       |       |-- erase
|       |-- igmp
|       |-- lacp
|       |-- pim
|       |       |-- sparse-mode
|       |-- fqm
|       |       |-- acl
|       |       |-- function
|       |       |-- message
|       |       |-- qos
|       |-- nsm
|       |       |-- all
|       |       |-- events
|       |       |-- kernel
|       |       |-- mcast
|       |       |-- packet
|       |-- rip
|       |       |-- all
|       |       |-- events
|       |       |-- nsm
|       |       |-- packet
|       |-- mstp
|       |       |-- all
|       |       |-- cli
|       |       |-- packet
|       |       |-- protocol
|       |       |-- timer
|       |-- vrrp
|       |-- ospf
|       |       |-- all
|       |       |-- events
|       |       |-- ifsm
|       |       |-- lsa
|       |       |-- nfsm
|       |       |-- nsm
|       |       |-- packet
|       |       |-- route
|       |-- traceroute
```

```
|       |-- tcpdump
|       |-- irfm
|       |       |-- module
|       |-- rfsgw
|       |-- wids
|       |-- locationtracking
|       |-- cluster
|       |       |-- all
|       |-- guestaccess
|       |       |-- all
|       |-- log
|       |       |-- level
|       |       |-- logsize
|       |       |-- logcount
|       |       |-- on
|       |       |-- off
|       |       |-- detail
|       |       |       |-- level
|       |       |       |-- logsize
|       |       |       |-- logcount
|       |       |       |-- on
|       |       |       |-- off
|       |       |-- mstdout
|       |       |       |-- module
|       |       |       |-- level
|       |       |       |-- on
|       |       |       |-- off
|       |-- dhcp-info
|       |-- capwap
|       |       |-- trace
|       |       |-- log
|       |       |-- status
|       |       |-- ip
|       |       |-- statistics
|       |-- sipalg
|       |       |-- enable
|       |-- apm
|       |       |-- clear
|       |       |-- block-endmsg
|       |       |-- fail-endmsg
|       |       |-- capwap-result-code
|       |       |-- event
|       |       |       |-- AP_UPGRADE_STATUS
|       |       |-- shared-memory
|       |       |       |-- clear
|       |       |       |-- add-ap
|       |       |       |-- del-ap
|       |       |       |-- findApIdListWithWlanProfileId
|       |       |       |-- findWlanIdWithApgIdAndWlanProfileId
|       |       |       |-- findWlanIdWithApIdAndWlanProfileId
|       |       |       |-- findWlanProfileIdWithApIdAndWlanId
|       |       |       |-- findWlanIdSetListWithApgId
|       |       |       |-- findWlanIdSetListWithAp
|       |       |-- wlan
|       |       |       |-- reject-probe
|       |       |       |       |-- rssi
|       |       |       |       |-- time
```

A.5 file

```
|-- file
|       |-- download
|       |-- upload
|       |-- copy
|       |-- remove
|       |-- move
|       |-- ls
|       |-- pwd
|       |-- cd
|       |-- dump
|       |-- df
|       |-- verify
|       |-- version
```

A.6 Etc

```
|-- reboot
|-- save
|       |-- local
|-- factory-reset
|-- export
|-- import
|-- ping
|-- traceroute
|-- tcpdump
|-- telnet
|-- ssh
```

ANNEX B. Open Source Announcement (WEC8500/WEC8050)

Some software components of this product incorporate source code covered under the GNU General Public License (GPL), the GNU Lesser General Public License (LGPL) and BSD License etc.

Acknowledgement:

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)

The software included in this product contains copyrighted software that is licensed under the GPL/LGPL. You may obtain the complete Corresponding Source code from us for a period of three years after our last shipment of this product by sending email to: oss.request@samsung.com

If you want to obtain the complete Corresponding Source code in the physical medium such as CD-ROM, the cost of physically performing source distribution may be charged. You may also find a copy of the source at http://www.samsungnetwork.com/Home/Opensource

This offer is valid to anyone in receipt of this information.

Below is the list of components covered under GNU General Public License, the GNU Lesser General Public License and BSD License etc.

Open Source Software	License
Apache HTTP Server	Apache License 2.0
lz4mt	BSD License
CyoEncode	BSD License
EventLog Library	BSD License
hostap-ct	BSD License
hostapd	BSD License
Libedit	BSD License

Open Source Software	License
libssh2	BSD License
Net SNMP-net-snmp	BSD License
OpenSSH	BSD License
Pure-FTPd	BSD License
Telnet	BSD License
ISC DHCP	DHCP License
Free Radius	GPL 2.0
Dproxy-Caching DNS Proxy	GPL 2.0
IP Utils	GPL 2.0
IPwatchD	GPL 2.0
NTP-The Network Time Protocol	GPL 2.0
TFTP Server and Client	GPL 2.0
Traceroute for Linux	GPL 2.0
Sys V Init	GPL 2.0
Linux Kernel	GPL 2.0
NetHogs-'net top' per process	GPL 2.0
compcache	GPL 2.0
DUMA library	GPL 2.0
GnuWin32-gzip	GPL 2.0
GNU Core Utils	GPL 2.0
ISC DHCP	ISIC License (BSD-)
FTP Lib Alt	LGPL 2.1
libnl-Netlink Library	LGPL 2.1
OSIP Library	LGPL 2.1
LIBSMI-Main	Libsmi License
libxml	libxml2 License
libxslt	MIT v2 with Ad Clause License
OpenSSL	OpenSSL Combined License
Zlib License	zlib License

Apache License

Version 2.0, January 2004
http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or
otherwise, or (ii) ownership of fifty percent (50 %) or more of the outstanding shares, or (iii) beneficial ownership of such entity. "You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License. "Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner.

For the purposes of this definition, “submitted” means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as “Not a Contribution.”

“Contributor” shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License.
Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License.
Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution.
You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

(a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

(b) You must cause any modified files to carry prominent notices stating that You changed the files; and

(c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

(d) If the Work includes a “NOTICE” text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and provide additional or different license terms and conditions use, reproduction, or distribution of Your modifications, or any such Derivative Works as a whole, provided Your use, roduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions.
Unless You explicitly state otherwise, Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks.
This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty.
Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an “AS IS” BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability.

In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability.

While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

APPENDIX: How to apply the Apache License to your work.

To apply the Apache License to your work, attach the following boilerplate notice, with the fields enclosed by brackets “[]” replaced with your own identifying information. (Don’t include the brackets!) The text should be enclosed in the appropriate comment syntax for the file format. We also recommend that a file or class name and description of purpose be included on the same “printed page” as the copyright notice for easier identification within third-party archives.

Copyright [yyyy] [name of copyright owner]

Licensed under the Apache License, Version 2.0 (the “License”); you may not use this file except in compliance with the License. You may obtain a copy of the License at

http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an “AS IS” BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

BSD 2.0 License

DHCP License

Internet Systems Consortium, Inc.
950 Charter Street
Redwood City, CA 94063
<info@isc.org>
http://www.isc.org/

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.
This General Public License applies to most of the Free Software Foundation’s software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.
For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps:
(1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software. Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software.

If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents.
We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0) This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language.
(Hereinafter, translation is included without limitation in the term "modification".)
Each licensee is addressed as "you".
Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program).
Whether that is true depends on what the Program does.

1) You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program. You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.
2) You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:
   a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.
   b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.
   c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

   These requirements apply to the modified work as a whole.

   If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

   Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

   In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.
3) You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:
   a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4) You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5) You are not required to accept this License, since you have not signed it.

However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6) Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7) If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License.
   If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.
   If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.
   It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.
   This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.
8) If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.
9) The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.
   Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and “any later version”, you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation.
   If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.
10) If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission.
    For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11) BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12) IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the “copyright” line and a pointer to where the full notice is found.

> <one line to give the program’s name and a brief idea of what it does.>
> Copyright(c) <year> <name of author>
>
> This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or(at your option) any later version.
>
> This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.
> See the GNU General Public License for more details.

```
You should have received a copy of the GNU General Public License along with this program;
if not, write to the Free Software Foundation, Inc., 51 Franklin St, Fifth Floor, Boston, MA 02110-
1301 USA.
```

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

```
Gnomovision version 69, Copyright(c) year name of author Gnomovision comes with
ABSOLUTELY NO WARRANTY; for details type ‘show w’.
This is free software, and you are welcome to redistribute it under certain conditions; type
‘show c’ for details.
```

ISIC License (BSD-)

ISIC is Copyright(c) 1999 Mike Frantzen, Chicago, IL, USA.
All rights reserved.
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1) Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2) Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

GNU LESSER GENERAL PUBLIC LICENSE

Version 2.1, February 1999
Copyright(c) 1991, 1999 Free Software Foundation, Inc.
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA
Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

[This is the first released version of the Lesser GPL. It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.]

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price.

Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code.

If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library.

Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author’s reputation will not be affected by problems that might be introduced by others.
Finally, software patents pose a constant threat to the existence of any free program.
We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.
Most GNU software, including some libraries, is covered by the ordinary GNU General Public License.
This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.
When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the “Lesser” General Public License because it does Less to protect the user’s freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs.
These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.
For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.
In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users’ freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.
The precise terms and conditions for copying, distribution and modification follow.
Pay close attention to the difference between a “work based on the library” and a “work that uses the library”.
The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0) This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called “this License”). Each licensee is addressed as “you”.

   A “library” means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

   The “Library”, below, refers to any such software library or work which has been distributed under these terms. A “work based on the Library” means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term “modification”.)

   “Source code” for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

   Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1) You may copy and distribute verbatim copies of the Library’s complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

   You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2) You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

   a) The modified work must itself be a software library.

   b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

   c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful. (For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application.

Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.) These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works.

But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it. Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library. In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3) You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices. Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4) You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5) A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a “work that uses the Library”. Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.
   However, linking a “work that uses the Library” with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a “work that uses the library”.
   The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.
   When a “work that uses the Library” uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library.
   The threshold for this to be true is not precisely defined by law.
   If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)
   Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.
6) As an exception to the Sections above, you may also combine or link a “work that uses the Library” with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer’s own use and reverse engineering for debugging such modifications.
   You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:
   a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable “work that uses the Library”, as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Use a suitable shared library mechanism for linking with the Library.
A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy. For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system.
Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7) You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8) You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9) You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10) Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11) If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all.
For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library. If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.
It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice. This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12) If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13) The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and “any later version”, you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14) If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15) BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16) IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Libraries

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that everyone can redistribute and change. You can do so by permitting redistribution under these terms (or, alternatively, under the terms of the ordinary General Public License).

To apply these terms, attach the following notices to the library. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the “copyright” line and a pointer to where the full notice is found.

> one line to give the library’s name and an idea of what it does.
> Copyright(c) year name of author
>
> This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either version 2.1 of the License, or (at your option) any later version.
>
> This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.
> See the GNU Lesser General Public License for more details.
>
> You should have received a copy of the GNU Lesser General Public License along with this library; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.

Also add information on how to contact you by electronic and paper mail.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a “copyright disclaimer” for the library, if necessary. Here is a sample; alter the names:

> Yoyodyne, Inc., hereby disclaims all copyright interest in the library ‘Frob’ (a library for tweaking knobs) written by James Random Hacker.
>
> Signature of Ty Coon, 1 April 1990 Ty Coon, President of Vice

That’s all there is to it!

libsmi license

libxml2 License

Except where otherwise noted in the source code (e.g. the files hash.c, list.c and the trio files, which are covered by a similar licence but with different Copyright notices) all the files are:

MIT v2 with Ad Clause License

LICENSE ISSUES

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License

Copyright(c) 1998-2004 The OpenSSL Project. All rights reserved.
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1) Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2) Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3) All advertising materials mentioning features or use of this software must display the following acknowledgment:
   “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)”
4) The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to endorse or promote products derived from this software without prior written permission.
   For written permission, please contact openssl-core@openssl.org.
5) Products derived from this software may not be called “OpenSSL” nor may “OpenSSL” appear in their names without prior written permission of the OpenSSL Project.
6) Redistributions of any form whatsoever must retain the following acknowledgment:
   “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)”

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT “AS IS” AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).
This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).
The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adheared to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com). Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used.

This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1) Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2) Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3) All advertising materials mentioning features or use of this software must display the following acknowledgement:
   "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)"
   The word 'cryptographic' can be left out if the rouines from the library being used are not cryptographic related:-).
4) If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED.
IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license **[including the GNU Public Licence.]**

The zlib/libpng License

Copyright(c) <year> <copyright holders>

This software is provided ‘as-is’, without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
3. This notice may not be removed or altered from any source distribution.

ANNEX C. Open Source Announcement (WEA302/WEA303/ WEA312/WEA313/WEA403/WEA412) (Highlighted- Future Release)

Some software components of this product incorporate source code covered under the GNU General Public License (GPL), the GNU Lesser General Public License (LGPL) and BSD License etc.

Acknowledgement:

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)

The software included in this product contains copyrighted software that is licensed under the GPL/LGPL. You may obtain the complete Corresponding Source code from us for a period of three years after our last shipment of this product by sending email to: oss.request@samsung.com

If you want to obtain the complete Corresponding Source code in the physical medium such as CD-ROM, the cost of physically performing source distribution may be charged. You may also find a copy of the source at http://www.samsungnetwork.com/Home/Opensource

This offer is valid to anyone in receipt of this information.

Below is the list of components covered under GNU General Public License, the GNU Lesser General Public License and BSD License etc.

Open Source Software	License
hostap-ct	BSD License
wpa_supplicant	BSD License
hostapd	BSD License
The tcpdump project	BSD License

Open Source Software	License
hostapd	BSD License
ICS DHCP	BSD License
mini_httpd-small HTTP server	BSD License
netkit-routed	BSD License
WIDE Project	BSD License
The libpcap project	BSD License
net-snmp	BSD License
OpenSSH	BSD License
Radvd	BSD License
ISC DHCP	DHCP License
RedBoot	eCos license version 2.0
Bridge-Utils	GPL 2.0
BusyBox	GPL 2.0
GNU Core Utils	GPL 2.0
Free Radius	GPL 2.0
GNU grep	GPL 2.0
buildroot	GPL 2.0
memtester	GPL 2.0
module-init-tools	GPL 2.0
mtd utils	GPL 2.0
linux net-tools	GPL 2.0
NMAP	GPL 2.0
ntpclient	GPL 2.0
procps	GPL 2.0
socat	GPL 2.0
wpa_supplicant	GPL 2.0
Sys k Logd	GPL 2.0
Sys stat	GPL 2.0
Sys V Init	GPL 2.0
GNU Term Cap	GPL 2.0
Util Linux	GPL 2.0
wireless-tools	GPL 2.0
dhcpd	GPL 2.0
Linux Kernel	GPL 2.0
GNU Wget	GPL 2.0
wput	GPL 2.0
Dnsmasq	GPL 2.0

Open Source Software	License
Ethernet bridge tables-ebtables	GPL 2.0
IGMPproxy	GPL 2.0
inadyn	GPL 2.0
iproute2	GPL 2.0
IPTables	GPL 2.0
NTFS-3G driver	GPL 2.0
NX-ROUTED	GPL 2.0
pppoe	GPL 2.0
TspctPlugin	GPL 2.0
Zebra	GPL 2.0
Netfilter	GPL 2.0
Bash	GPL 2.0
GNU awk	GPL 2.0
inetutils	GPL 2.0
GNU sed	GPL 2.0
Iperf	Iperf License
Atheros-based WiFi Hardware Abstraction Layer	Kaffe ISC License
libnl	LGPL 2.1
LZMA SDK	LGPL 2.1
OpenSSL	OpenSSL Combined License
Vim	Vim Charityware License v 5.3
zlib	zlib License

BSD 2.0 License

Copyright(c) <YEAR>, <OWNER>
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of the <ORGANIZATION> nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

DHCP License

Copyright(c) 2004 by Internet Systems Consortium, Inc. (“ISC”)
Copyright(c) 1996-2003 by Internet Software Consortium

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED “AS IS” AND ISC DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL ISC BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Internet Systems Consortium, Inc.
950 Charter Street
Redwood City, CA 94063
info@isc.org
http://www.isc.org/

Full eCos license

This is the full text of the license as found on files within eCos covered by the eCos license. It should be read in conjuction with the GNU General Public License (GPL) on which it depends.

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991
Copyright(c) 1989, 1991 Free Software Foundation, Inc.
51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.
This General Public License applies to most of the Free Software Foundation’s software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.)
You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.
For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps:
(1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software. Also, for each author’s protection and ours, we want to make certain that everyone understands that there is no warranty for this free software.

If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors’ reputations.

Finally, any free program is threatened constantly by software patents.
We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary.

To prevent this, we have made it clear that any patent must be licensed for everyone’s free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0) This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".
   Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.
1) You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.
   You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.
2) You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:
   a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.
   b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.
   c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

   These requirements apply to the modified work as a whole.
   If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.
In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3) You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:
   a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
   b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
   c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

   The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.
   If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4) You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5) You are not required to accept this License, since you have not signed it.
   However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6) Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7) If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License.
   If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.
   If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.
   It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.
   This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8) If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9) The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.
   Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation.
   If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10) If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission.
For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11) BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.
12) IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the “copyright” line and a pointer to where the full notice is found.

> <one line to give the program’s name and a brief idea of what it does.>
> Copyright(c) <year> <name of author>
>
> This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.
>
> This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.
> See the GNU General Public License for more details.
>
> You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

> Gnomovision version 69, Copyright(c) year name of author Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type ‘show w’.
> This is free software, and you are welcome to redistribute it under certain conditions; type ‘show c’ for details.

Iperf License

Iperf performance test
Mark Gates
Ajay Tirumala
Jim Ferguson
Jon Dugan
Feng Qin
Kevin Gibbs
John Estabrook
National Laboratory for Applied Network Research
National Center for Supercomputing Applications
University of Illinois at Urbana-Champaign
http://www.ncsa.uiuc.edu

GNU LESSER GENERAL PUBLIC LICENSE

Version 2.1, February 1999
Copyright(c) 1991, 1999 Free Software Foundation, Inc.
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA
Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

[This is the first released version of the Lesser GPL. It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.]

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price.

Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code.

If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library.

Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program.
We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.
Most GNU software, including some libraries, is covered by the ordinary GNU General Public License.
This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.
When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the “Lesser” General Public License because it does Less to protect the user’s freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs.
These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.
For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.
In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users’ freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.
The precise terms and conditions for copying, distribution and modification follow.
Pay close attention to the difference between a “work based on the library” and a “work that uses the library”. The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0) This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called “this License”). Each licensee is addressed as “you”.

   A “library” means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

   The “Library”, below, refers to any such software library or work which has been distributed under these terms. A “work based on the Library” means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term “modification”.)

   “Source code” for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

   Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1) You may copy and distribute verbatim copies of the Library’s complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

   You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2) You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

   a) The modified work must itself be a software library.

   b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

   c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful. (For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.) These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works.

But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it. Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library. In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3) You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices. Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy. This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4) You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5) A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a “work that uses the Library”. Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.
   However, linking a “work that uses the Library” with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a “work that uses the library”.
   The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.
   When a “work that uses the Library” uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library.
   The threshold for this to be true is not precisely defined by law.
   If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)
   Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.
6) As an exception to the Sections above, you may also combine or link a “work that uses the Library” with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer’s own use and reverse engineering for debugging such modifications.
   You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:
   a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable “work that uses the Library”, as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy. For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7) You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8) You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9) You are not required to accept this License, since you have not signed it.
However, nothing else grants you permission to modify or distribute the Library or its derivative works.
These actions are prohibited by law if you do not accept this License.
Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10) Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11) If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all.
For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library. If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.
It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice. This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12) If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13) The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.
Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation.
If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14) If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15) BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.
16) IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Libraries

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that everyone can redistribute and change. You can do so by permitting redistribution under these terms (or, alternatively, under the terms of the ordinary General Public License).

To apply these terms, attach the following notices to the library. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the “copyright” line and a pointer to where the full notice is found.

> one line to give the library’s name and an idea of what it does.
> Copyright(c) year name of author
>
> This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either version 2.1 of the License, or (at your option) any later version.
>
> This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.
> See the GNU Lesser General Public License for more details.
>
> You should have received a copy of the GNU Lesser General Public License along with this library; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.

Also add information on how to contact you by electronic and paper mail.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a “copyright disclaimer” for the library, if necessary. Here is a sample; alter the names:

> Yoyodyne, Inc., hereby disclaims all copyright interest in the library ‘Frob’ (a library for tweaking knobs) written by James Random Hacker.
>
> Signature of Ty Coon, 1 April 1990 Ty Coon, President of Vice

That’s all there is to it!

LICENSE ISSUES

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License

Copyright(c) 1998-2004 The OpenSSL Project. All rights reserved.
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1) Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2) Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3) All advertising materials mentioning features or use of this software must display the following acknowledgment:
   “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)”
4) The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to endorse or promote products derived from this software without prior written permission.
   For written permission, please contact openssl-core@openssl.org.
5) Products derived from this software may not be called “OpenSSL” nor may “OpenSSL” appear in their names without prior written permission of the OpenSSL Project.
6) Redistributions of any form whatsoever must retain the following acknowledgment:
   “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)”

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT “AS IS” AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).
This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).
The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adheared to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com). Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used.

This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1) Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2) Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3) All advertising materials mentioning features or use of this software must display the following acknowledgement:
   "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)"
   The word 'cryptographic' can be left out if the rouines from the library being used are not cryptographic related:-).
4) If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS;

OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
The license and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license **[including the GNU Public Licence.]**

VIM LICENSE

1) There are no restrictions on distributing unmodified copies of Vim except that they must include this license text. You can also distribute unmodified parts of Vim, likewise unrestricted except that they must include this license text. You are also allowed to include executables that you made from the unmodified Vim sources, plus your own usage examples and Vim scripts.
2) It is allowed to distribute a modified (or extended) version of Vim, including executables and/or source code, when the following four conditions are met:
   a) This license text must be included unmodified.
   b) The modified Vim must be distributed in one of the following five ways:
      i) If you make changes to Vim yourself, you must clearly describe in the distribution how to contact you. When the maintainer asks you (in any way) for a copy of the modified Vim you distributed, you must make your changes, including source code, available to the maintainer without fee. The maintainer reserves the right to include your changes in the official version of Vim. What the maintainer will do with your changes and under what license they will be distributed is negotiable. If there has been no negotiation then this license, or a later version, also applies to your changes. The current maintainer is Bram Moolenaar {Bram@vim.org}. If this changes it will be announced in appropriate places (most likely vim.sf.net, www.vim.org and/or comp.editors). When it is completely impossible to contact the maintainer, the obligation to send him your changes ceases. Once the maintainer has confirmed that he has received your changes they will not have to be sent again.
      ii) If you have received a modified Vim that was distributed as mentioned under a) you are allowed to further distribute it unmodified, as mentioned at I). If you make additional changes the text under a) applies to those changes.
      iii) Provide all the changes, including source code, with every copy of the modified Vim you distribute. This may be done in the form of a context diff. You can choose what license to use for new code you add. The changes and their license must not restrict others from making their own changes to the official version of Vim.
      When you have a modified Vim which includes changes as mentioned under c), you can distribute it without the source code for the changes if the following three conditions are met:

The license that applies to the changes permits you to distribute the changes to the Vim maintainer without fee or restriction, and permits the Vim maintainer to include the changes in the official version of Vim without fee or restriction.

You keep the changes for at least three years after last distributing the corresponding modified Vim. When the maintainer or someone who you distributed the modified Vim to asks you (in any way) for the changes within this period, you must make them available to him.

You clearly describe in the distribution how to contact you. This contact information must remain valid for at least three years after last distributing the corresponding modified Vim, or as long as possible.

iv) When the GNU General Public License (GPL) applies to the changes, you can distribute the modified Vim under the GNU GPL version 2 or any later version.

c) A message must be added, at least in the output of the ":version" command and in the intro screen, such that the user of the modified Vim is able to see that it was modified. When distributing as mentioned under 2) e) adding the message is only required for as far as this does not conflict with the license used for the changes.

d) The contact information as required under 2) a) and 2) d) must not be removed or changed, except that the person himself can make corrections.

3) If you distribute a modified version of Vim, you are encouraged to use the Vim license for your changes and make them available to the maintainer, including the source code. The preferred way to do this is by e-mail or by uploading the files to a server and e-mailing the URL. If the number of changes is small (e.g. a modified Makefile) e-mailing a context diff will do. The e-mail address to be used is {maintainer@vim.org}

4) It is not allowed to remove this license from the distribution of the Vim sources, parts of it or from a modified version. You may use this license for previous Vim releases instead of the license that they came with, at your option.

The zlib/libpng License

Copyright(c) <year> <copyright holders>

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
3. This notice may not be removed or altered from any source distribution.

ABBREVIATION

A

ACL	Access Control List
AES	Advanced Encryption Standard
ALG	Application Layer Gateway
AP	Access Point
APC	Access Point Controller

B

BPDU	Bridge Protocol Data Unit

C

CAC	Call Admission Control
CAPWAP	Control And Provisioning Wireless Access Point
CCM	Counter mode encryption with CBC-MAC
CCMP	Counter mode encryption with CBC-MAC Protocol
CCTV	Closed Circuit Television
CDR	Crash Detect and Report
CHDC	Coverage Hole Detection and Control
CLI	Command Line Interface
CSMA/CD	Carrier Sense Multiple Access/Collision Detect
CVO	Controlled Voice Optimization

D

DCS	Dynamic Channel Selection
DECT	Digital Enhanced Cordless Telecommunications
DFS	Dynamic Frequency Selection
DHCP	Dynamic Host Configuration Protocol
DNAT	Destination NAT
DNS	Domain Naming Service
DPC	Dynamic Power control
DSCP	Differentiated Services Code Point
DTIM	Delivery Traffic Indication Message
DTLS	Datagram Transmission Layer Security

E

EAP	Extensible Authentication Protocol
EAPOL	EAP over LANs
EDCA	Enhanced Distributed Channel Access

F

FFT	Fast Fourier Transform
FIFO	First-In-First-Out
FTP	File Transfer Protocol

G

GARP	Gratuitous Address Resolution Protocol
GbE	Giga Bit Ethernet
GI	Guard Interval

H

HO	Handover

I

IGMP	Internet Group Management Protocol
IP	Internet Protocol
IPWATCHD	IP WATCH Deamon
IV	Initial Vector

L

LACP	Link Aggregation Control Protocol
LAN	Local Area Network
LED	Light Emitting Diode
LSA	Link State Advertisement

M

MAC	Medium Access Control
MCS	Modulation and Coding Scheme
MIB	Management Information Base
MIMO	Multiple Input Multiple Output
MSTP	Multiple Spanning-Tree Protocol
MTU	Maximum Transmission Unit

N

NAT	Network Address Translation
NMS	Network Management System
NSSA	Not So Stubby Areas
NTP	Network Time Protocol

O

OKC	Opportunistic Key Caching
OSPF	Open Shortest Path First
OUI	Organizationally Unique Identifier

P

PHY	Physical layer
PIM-SM	Protocol Independent Multicast-Sparse Mode
PoE	Power over Ethernet
PMK	Pairwise Master Key
PSK	Pre-Shared Key

Q

QoS	Quality of Service

R

RADIUS	Remote Authentication Dial-In User Service
RF	Radio Frequency
RPM	Revolution Per Minute
RRM	Radio Resource Management
RSSI	Received Signal Strength Indication
RSTP	Rapid Spanning-Tree Protocol
RTP	Real-time Transport Protocol

S

SDS	Samsung Downlink Scheduler
SIP	Session Initiation Protocol
SNAT	Source NAT
SNMP	Simple Network Management Protocol
SNR	Signal to Noise Ratio
SSH	Secure Shell
SSID	Service Set Identifier
STP	Signaling Transfer Point

T

TBTT	Target Beacon Transmission Times
TKIP	Temporal Key Integrity Protocol

U

USB	Universal Serial Bus
UTC	Coordinated Universal Time
UTP	Unshielded Twisted Pair

V

VAP	Virtual Access Point
VATS	Voice-Aware Traffic Scheduling
VLAN	Virtual Local Area Network
VoIP	Voice over IP
VPN	Virtual Private Network
VQM	Voice Quality Monitoring
VRRP	Virtual Router Redundancy Protocol

W

WAN	Wide Area Network
WDS	Wireless Distribution Service
WEM	Wireless Enterprise WLAN Manager (Future Release)
WEP	Wired Equivalent Privacy
WES	Wireless Enterprise Security
Wi-Fi	Wireless Fidelity
WIDS	Wireless Intrusion Detection System
WLAN	Wireless Local Area Network
WMM	WiFi Multimedia
WPA	Wi-Fi Protected Access
WPA2	Wi-Fi Protected Access Version 2

WEC8500/WEC8050 (APC)

Operation Manual