SIEMENS

SCALANCE W1750D UI

Configuration Manual

Continued on next page

09/2018

C79000-G8976-C451-03

Siemens AG
Division Process Industries and Drives
Postfach 48 48
90026 NÜRNBERG
DEUTSCHLAND

Dokument-Bestellnummer: C79000-G8976-C451-03
℗ 09/2018 Änderungen vorbehalten

SCALANCE W1750D UI

Configuration Manual

Continued

Continued on next page

Siemens AG
Division Process Industries and Drives
Postfach 48 48
90026 NÜRNBERG
DEUTSCHLAND

Dokument-Bestellnummer: C79000-G8976-C451-02
℗ 07/2018 Änderungen vorbehalten

SCALANCE W1750D UI

Configuration Manual

Legal information

Warning notice system

This manual contains notices you have to observe in order to ensure your personal safety, as well as to prevent damage to property. The notices referring to your personal safety are highlighted in the manual by a safety alert symbol, notices referring only to property damage have no safety alert symbol. These notices shown below are graded according to the degree of danger.

⚠ DANGER

indicates that death or severe personal injury **will** result if proper precautions are not taken.

⚠ WARNING

indicates that death or severe personal injury **may** result if proper precautions are not taken.

⚠ CAUTION

indicates that minor personal injury can result if proper precautions are not taken.

NOTICE

indicates that property damage can result if proper precautions are not taken.

If more than one degree of danger is present, the warning notice representing the highest degree of danger will be used. A notice warning of injury to persons with a safety alert symbol may also include a warning relating to property damage.

Qualified Personnel

The product/system described in this documentation may be operated only by **personnel qualified** for the specific task in accordance with the relevant documentation, in particular its warning notices and safety instructions. Qualified personnel are those who, based on their training and experience, are capable of identifying risks and avoiding potential hazards when working with these products/systems.

Proper use of Siemens products

Note the following:

⚠ WARNING

Siemens products may only be used for the applications described in the catalog and in the relevant technical documentation. If products and components from other manufacturers are used, these must be recommended or approved by Siemens. Proper transport, storage, installation, assembly, commissioning, operation and maintenance are required to ensure that the products operate safely and without any problems. The permissible ambient conditions must be complied with. The information in the relevant documentation must be observed.

Trademarks

All names identified by ® are registered trademarks of Siemens AG. The remaining trademarks in this publication may be trademarks whose use by third parties for their own purposes could violate the rights of the owner.

Disclaimer of Liability

We have reviewed the contents of this publication to ensure consistency with the hardware and software described. Since variance cannot be precluded entirely, we cannot guarantee full consistency. However, the information in this publication is reviewed regularly and any necessary corrections are included in subsequent editions.

Siemens AG
Division Process Industries and Drives
Postfach 48 48
90026 NÜRNBERG
DEUTSCHLAND

C79000-G8976-C451-02
℗ 08/2018 Subject to change

Table of contents

About this guide

1

This User Guide describes the features supported by SCALANCE W and provides detailed instructions for setting up and configuring the SCALANCE W network.

Intended Audience

This guide is intended for administrators who configure and use APs.

Related Documents

In addition to this document, the SCALANCE W product documentation includes the following:

- Access Point Installation Guides
- Quick Start Guide
- CLI Function Manual

Conventions

The following conventions are used throughout this manual to emphasize important concepts:

Table 1- 1 Typographical Conventions

Style Type	Description
Italics	This style is used to emphasize important terms and to mark the titles of books.
`System items`	This fixed-width font depicts the following: • Sample screen output • System prompts • Filenames, software devices, and specific commands when mentioned in the text.
Commands	In the command examples, this style depicts the keywords that must be typed exactly as shown.
<Arguments>	In the command examples, italicized text within angle brackets represents items that you should replace with information appropriate to your specific situation. For example: `# send` *<text message>* In this example, you would type “send” at the system prompt exactly as shown, followed by the text of the message you wish to send. Do not type the angle brackets.

Style Type	Description
`[Optional]`	Command examples enclosed in brackets are optional. Do not type the brackets.
`{Item A | Item B}`	In the command examples, items within curled braces and separated by a vertical bar represent the available choices. Enter only one choice. Do not type the braces or bars.

Service & Support

In addition to the product documentation, also check out the comprehensive online information platform of Siemens Industry Online Support at the following Internet address: (https://support.industry.siemens.com/cs/de/en/)

Apart from news, there you will also find:

- Project information: Manuals, FAQs, downloads, application examples etc.
- Contacts, Technical Forum
- The option to submit a support query (https://support.industry.siemens.com/My/ww/en/requests):
- Our service offer:

  Right across our products and systems, we provide numerous services that support you in every phase of the life of your machine or system - from planning and implementation to commissioning, through to maintenance and modernization.

You will find contact data on the Internet at the following address:

https://www.automation.siemens.com/aspa_app/?ci=yes&lang=en

Security information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens' products and solutions constitute one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.

For additional information on industrial security measures that may be implemented, please visit https://www.siemens.com/industrialsecurity

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customers' exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under: https://www.siemens.com/industrialsecurity

Security recommendations 2

To prevent unauthorized access, note the following security recommendations.

General

- You should make regular checks to make sure that the device meets these recommendations and/or other security guidelines.
- Evaluate your plant as a whole in terms of security. Use a cell protection concept with suitable products (https://www.industry.siemens.com/topics/global/en/industrial-security/pages/default.aspx).
- When the internal and external network are disconnected, an attacker cannot access internal data from the outside. Therefore operate the device only within a protected network area.
- For communication via non-secure networks use additional devices with VPN functionality to encrypt and authenticate the communication.
- Terminate management connections correctly (WBM, Telnet, SSH etc.).

Physical access

- Restrict physical access to the device to qualified personnel.

Software (security functions)

- Keep the software up to date. Check regularly for security updates of the product. You will find information on this on the Internet pages "Industrial Security (https://www.siemens.com/industrialsecurity)".
- Inform yourself regularly about security advisories and bulletins published by Siemens ProductCERT (https://www.siemens.com/cert/en/cert-security-advisories.htm).
- Only activate protocols that you really require to use the device.
- Use the security functions such as address translation with NAT (Network Address Translation) or NAPT (Network Address Port Translation) to protect receiving ports from access by third parties.
- Restrict access to the device with a firewall or rules in an access control list (ACL - Access Control List).
- If RADIUS authentication is via remote access, make sure that the communication is within the secured network area or is via a secure channel.

- The option of VLAN structuring provides good protection against DoS attacks and unauthorized access. Check whether this is practical or useful in your environment.
- Enable logging functions. Use the central logging function to log changes and access attempts centrally. Check the logging information regularly.
- Configure a Syslog server to forward all logs to a central location.
- Use WPA2/ WPA2-PSK with AES to protect the WLAN-Software

Passwords

- Define rules for the use of devices and assignment of passwords.
- Regularly update passwords and keys to increase security.
- Change all default passwords for users before you operate the device.
- Only use passwords with a high password strength. Avoid weak passwords for example password1, 123456789, abcdefgh.
- Make sure that all passwords are protected and inaccessible to unauthorized personnel.
- Do not use the same password for different users and systems or after it has expired.

Keys and certificates

- This section deals with the security keys and certificates you require to set up HTTPS (Hypertext Transfer Protocol Secure).
- We strongly recommend that you create your own HTTPS certificates and make them available. There are preset certificates and keys on the device. The preset and automatically created HTTPS certificates are self-signed. We recommend that you use HTTPS certificates signed either by a reliable external or by an internal certification authority. The HTTPS certificate checks the identity of the device and controls the encrypted data exchange. You can install the HTTPS certificate via the SCALANCE W UI, see "Uploading Certificate".
- Handle user-defined private keys with great caution if you use user-defined SSH or SSL keys.
- Use the certification authority including key revocation and management to sign the certificates.
- Verify certificates and fingerprints on the server and client to avoid "man in the middle" attacks.
- We recommend that you use certificates with a key length of 2048 bits.
- Change keys and certificates immediately, if there is a suspicion of compromise.

Secure/non-secure protocols

- Avoid and disable non-secure protocols, for example Telnet and TFTP. For historical reasons, these protocols are still available, however not intended for secure applications. Use non-secure protocols on the device with caution.
- The following protocols provide secure alternatives:
  - SNMPv1/v2 → SNMPv3

    Check whether use of SNMPv1 is necessary. SNMPv1 is classified as non-secure. Use the option of preventing write access. The product provides you with suitable setting options. If SNMP is enabled, change the community names. If no unrestricted access is necessary, restrict access with SNMP. Use SNMPv3 in conjunction with passwords.
  - HTTP → HTTPS
  - Telnet → SSH
  - SNTP → NTP
  - Use secure protocols when access to the device is not prevented by physical protection measures.
- To prevent unauthorized access to the device or network, take suitable protective measures against non-secure protocols.
- If you require non-secure protocols and services, operate the device only within a protected network area.
- Restrict the services and protocols available to the outside to a minimum.

Available protocols per port

The following list provides you with an overview of the open ports on this device. The table includes the following columns:

- Protocol

  All protocols that the device supports.
- Port number

  Port number assigned to the protocol.
- Port status
  - Open: The port is always open and cannot be closed.
- Factory setting
  - Open: The factory setting of the port is "Open".
  - Closed: The factory setting of the port is "Closed".
- Authentication

  Specifies whether or not the protocol is authenticated.

Protocol	Port number	Port status	Factory setting of the port	Authentication
Air Monitor	UDP/1144	open	close	yes
Airgroup	UDP/53536	open	close	yes
Airgroup Master to slave	UDP/53535	open	close	no
Bootps	UDP/67	open	open	no
Captive portal	TCP/8080	open	open	yes
DHCP	UDP/1067	open	open	no
	UDP/68	open	close	no
	UDP/4011	open	close	no
Dnsmasq	UDP/one port in range 3000-3020	open	open	no
DTLS	UDP/4433	open	close	yes
HTTP	TCP/80	open	open	yes
	TCP/4343	open	open	yes
HTTPS	TCP/443	open	open	yes
	TCP/43430	open	close	yes
mDNS	UDP/5999	open	close	no
	UDP/5353	open	close	no
NTP	UDP/123	open	close	no
Proprietary	UDP/8209	open	close	no
	UDP/4434	open	open	no
	UDP/8211	open	open	no
Dynamic dns	UDP/5363	open	open	yes
Proprietary(dTable)	UDP/3799	open	close	no
	UDP/8612	open	open	no
RADIUS	UDP/1892	open	close	no
	UDP/2629	open	open	no
	UDP/1812	open	close	no
	UDP/2083	open	close	no
	UDP/1616	open	open	no
Radius-terms	UDP/2628	open	open	yes
SSH	TCP/22	open	open	yes
	TCP/2322	open	open	yes
Syslog	UDP/514	open	close	no
Telnet	TCP/23	open	close	yes

Protocol	Port number	Port status	Factory setting of the port	Authentication
SNMPv1	UDP/161	open	open	no
	UDP/one Port in range 49152-65535	open	close	no
SNMPv3	UDP/161	open	open	yes
	UDP/one Port in range 49152-65535	open	close	yes

2.1

About SCALANCE W 3

3.1 Overview

SCALANCE W is a simple, easy to deploy turnkey WLAN solution consisting of one or more SCALANCE W Access Points. An Ethernet port with routable connectivity to the Internet or a self-enclosed network is used for deploying an SCALANCE W Wireless Network. An AP can be installed at a single site or deployed across multiple geographically dispersed locations. Designed specifically for easy deployment and proactive management of networks, SCALANCE W is ideal for small customers or remote locations without requiring any on-site IT administrator.

An AP cluster consists of slave APs and a master AP in the same VLAN, as they communicate with broadcast messages. A virtual controller is a combination of the whole cluster, as the slave APs and Master AP coordinate to provide a controllerless SCALANCE W solution. In a SCALANCE W deployment scenario, the first AP that comes up becomes the master AP. All other APs joining the cluster after that AP, become the slave APs.

In a SCALANCE W deployment scenario, only the first AP or the master AP needs to be configured. The other APs download configurations from the first AP that is configured. The SCALANCE W solution constantly monitors the network to determine the AP that must function as a master AP at a given time. The master AP may change as necessary from one AP to another without impacting network performance.

3.2 SCALANCE W UI

The SCALANCE W User Interface (UI) provides a standard web-based interface that allows you to configure and monitor a Wi-Fi network. SCALANCE W is accessible through a standard web browser from a remote management console or workstation and can be launched using the following browsers:

- Microsoft Internet Explorer 11 or earlier
- Apple Safari 6.0 or later
- Google Chrome 23.0.1271.95 or later
- Mozilla Firefox 17.0 or later

If the SCALANCE W UI is launched through an unsupported browser, a warning message is displayed along with a list of recommended browsers. However, the users are allowed to login using the **Continue login** link on the **Login** page.

Note

To view the SCALANCE W UI, ensure that JavaScript is enabled on the web browser.

Note

The SCALANCE W UI logs out automatically if the window is inactive for 15 minutes.

3.3 SCALANCE W CLI

The SCALANCE W CLI is a text-based interface that is accessible through an SSH session.

SSH access requires that you configure an IP address and a default gateway on the AP and connect the AP to your network. This is typically performed when the SCALANCE W network on an AP is set up.

Setting up an AP

4

4.1 Setting up a SCALANCE W Network

Before installing an AP:

- Ensure that you have an Ethernet cable of the required length to connect an AP to the home router.
- Ensure that you have one of the following power sources:

  IEEE 802.3af/at-compliant PoE source. The PoE source can be any power source equipment switch or a midspan power source equipment device.
- AP power adapter kit.

To set up the SCALANCE W network, perform the following procedures

1. Connecting an AP (Page 29)
2. Assigning an IP address to the AP (Page 30)

4.1.1 Connecting an AP

Based on the type of the power source used, perform one of the following steps to connect an AP to the power source:

1. PoE switch—Connect the Ethernet 0 port of the AP to the appropriate port on the PoE switch.
2. PoE midspan—Connect the Ethernet 0 port of the AP to the appropriate port on the PoE midspan.
3. AC to DC power adapter—Connect the 12V DC power jack socket to the AC to DC power adapter

4.1.2 Assigning an IP address to the AP

The AP needs an IP address for network connectivity. When you connect an AP to a network, it receives an IP address from a DHCP server.

To obtain an IP address for an AP:

1. Ensure that the DHCP service is enabled on the network.
2. Connect the Ethernet 0 port of AP to a switch or router using an Ethernet cable.
3. Connect the AP to a power source. The AP receives an IP address provided by the switch or router.

Note

If there is no DHCP service on the network, the AP can be assigned a static IP address. If a static IP is not assigned, the AP obtains an IP automatically within the 169.254 subnet.

Assigning a Static IP

To assign a static IP to an AP:

1. Connect a terminal, PC, or workstation running a terminal emulation program to the **Console** port on the AP.
2. Turn on the AP. An autoboot countdown prompt that allows you to interrupt the normal startup process and access **apboot** is displayed.
3. Press **Enter** key before the timer expires. The AP goes into the **apboot** mode.
4. In the **apboot** mode, execute the following commands to assign a static IP to the AP

```
Hit <Enter> to stop autoboot: 0
apboot>
apboot> setenv ipaddr 192.0.2.0
apboot> setenv netmask 255.255.255.0
apboot> setenv gatewayip 192.0.2.2
apboot> save
Saving Environment to Flash...

Un-Protected 1 sectors
.done
Erased 1 sectors
Writing
```

5. Use the `printenv` command to view the configuration.

```
apboot> printenv
```

4.2 Provisioning an AP

4.2.1 ZTP of APs

ZTP eliminates the traditional method of deploying and maintaining devices and allows you to provision new devices in your network automatically, without manual intervention. Following are the ZTP methods for SCALANCE W.

4.2.2 NTP Server and AP Synchronization

In order for ZTP to be successful, the timezone of the AP must be in synchronization with the NTP server.

Note

To facilitate ZTP using the AMP or Activate, you must configure the firewall and wired infrastructure to either allow the NTP traffic to pool.ntp.org, or provide alternative NTP servers under DHCP options. For more information on configuring an NTP server, see NTP Server (Page 73).

In a scenario where the NTP server is unreachable, the connection between the AP and Activate will fall back to the unsecured status. The NTP client process running in the back end will continuously attempt to reconnect to the NTP server until a secure connection is established. The NTP client process receives a response from the NTP server on successfully establishing a connection and notifies the CLI process which runs a series of checks to ensure the NTP server is reachable.

Connecting to a Provisioning Wi-Fi Network

The APs boot with factory default configuration and try to provision automatically. If the automatic provisioning is successful, the SCALANCE W SSID will not be available. If AirWave and Activate are not reachable and the automatic provisioning fails, the SCALANCE W SSID becomes available and the users can connect to a provisioning network by using the SCALANCE W SSID.

To connect to a provisioning Wi-Fi network:

1. Ensure that the client is not connected to any wired network.
2. Connect a wireless-enabled client to a provisioning Wi-Fi network: for example, scalance.

3. If the Windows operating system is used:
   - Click the wireless network connection icon in the system tray. The **Wireless Network Connection** window is displayed.
   - Click the SCALANCE W network and then click **Connect**.
4. If the Mac operating system is used:
   - Click the **AirPort** icon. A list of available Wi-Fi networks is displayed.
   - Click the SCALANCE W network

Note

The SCALANCE W SSIDs are broadcast in 2.4 GHz only.

AP Cluster

APs in the same VLAN automatically find each other and form a single functioning network managed by a virtual controller.

Note

Moving an AP from one cluster to another requires a factory reset of the AP.

Disabling the Provisioning Wi-Fi Network

The provisioning network is enabled by default. SCALANCE W provides the option to disable the provisioning network through the console port. Use this option only when you do not want the default SSID SCALANCE W to be broadcast in your network.

To disable the provisioning network:

1. Connect a terminal, PC, or workstation running a terminal emulation program to the **Console** port on the AP.
2. Configure the terminal or terminal emulation program to use the following communication settings:

Baud Rate	Data Bits	Parity	Stop Bits	Flow Control
9600	8	None	1	None

3. Turn on the AP. An autoboot countdown prompt that allows you to interrupt the normal startup process and access apboot is displayed.

4. Click Enter key before the timer expires. The AP goes into the apboot mode through console.
5. In the apboot mode, execute the following commands to disable the provisioning network:

```
apboot> factory_reset

apboot> setenv disable_prov_ssid 1

apboot> saveenv

apboot> reset
```

4.2.3 Provisioning APs through Airwave

AirWave is a powerful platform and easy-to-use network operations system that manages wireless, wired, and remote access networks, as well as wired and wireless infrastructures from a wide range of third- party manufacturers. With its easy-to-use interface, AirWave provides real-time monitoring, proactive alerts, historical reporting, as well as fast and efficient troubleshooting. It also offers tools that manage RF coverage, strengthen wireless security, and demonstrate regulatory compliance.

4.3 Logging in to the SCALANCE W UI

Launch a web browser and enter http://direct.siemens.com. In the login screen, enter the following credentials:

- Username — admin
- Password — admin

When you use a provisioning Wi-Fi network to connect to the Internet, all browser requests are directed to the SCALANCE W UI. For example, if you enter www.example.com in the address bar, you are directed to the SCALANCE W UI. You can change the default login credentials after the first login.

Note

If an AP does not obtain an IP address, it assigns itself 169.x.x.x as the IP address. In this case, DNS requests from clients on a provisioning SSID will not receive a response because of lack of network connectivity. Hence, automatic redirection to the SCALANCE W UI http://direct.scalance.com will fail.

In such a case, you must manually open http://direct.scalance.com on your browser to access the SCALANCE W SCALANCE W UI.

Regulatory Domains

The IEEE 802.11, 802.11b, 802.11g, or 802.11n Wi-Fi networks operate in the 2.4 GHz spectrum and IEEE 802.11a or 802.11n operate in the 5 GHz spectrum. The spectrum is divided into channels. The 2.4 GHz spectrum is divided into 14 overlapping, staggered 20 MHz wireless carrier channels. These channels are spaced 5 MHz apart. The 5 GHz spectrum is divided into more channels. The channels that can be used in a particular country vary based on the regulations of that country.

The initial Wi-Fi setup requires you to specify the country code for the country in which the AP operates. This configuration sets the regulatory domain for the radio frequencies that the APs use. Within the regulated transmission spectrum, a HT 802.11ac, 802.11a, 802.11b, 802.11g, or 802.11n radio setting can be configured. The available 20 MHz, 40 MHz, or 80 MHz channels are dependent on the specified country code.

You cannot change a country code for APs in regulatory domains such as Japan. However, for AP-US and AP-RW variants, you can select from the list of supported regulatory domains. If the supported country code is not in the list, contact your Siemens Support team to know if the required country code is supported and obtain the software that supports the required country code.

NOTICE

Country code assignments

Improper country code assignments can disrupt wireless transmissions. Most countries impose penalties and sanctions on operators of wireless networks with devices set to improper country codes

To view the country code information, run the **show country-codes** command.

NOTICE

National approvals

When you select a country, keep in mind the national approvals for the product. The current status can be found on the Internet at the following address:

https://www.siemens.com/wireless-approvals

Specifying Country Code

The **Country Code** window is displayed for the AP-US and AP-RW variants when you login to the AP UI for the first time. The **Please Specify the Country Code** drop-down list displays only the supported country codes. Select a country code from the list and click **OK**. The AP operates in the selected country code domain.

Note

Country code once set, cannot be changed in the SCALANCE W UI. It can be changed only by using the **virtual-controller- country** command in the SCALANCE W CLI.

Note

Slave APs obtain country code configuration settings from the master AP.

You can also view the list of supported country codes for the AP-US and AP-RW variants by using the **show country-codes** command.

4.4 Accessing the SCALANCE W CLI

SCALANCE W supports the use of CLI for scripting purposes. When you make configuration changes on a master AP in the CLI, all associated APs in the cluster inherit these changes and subsequently update their configurations. By default, you can access the CLI from the serial port or from an SSH session. You must explicitly enable Telnet access on the AP to access the CLI through a Telnet session.

For information on enabling SSH and Telnet access to the AP CLI, see Terminal access (Page 73).

Connecting to a CLI Session

On connecting to a CLI session, the system displays its host name followed by the login prompt. Use the administrator credentials to start a CLI session. For example:

```
User: admin
```

If the login is successful, the privileged command mode is enabled and a command prompt is displayed. For example:

```
(AP)#
```

The privileged EXEC mode provides access to **show**, **clear**, **ping**, **traceroute** and **commit** commands. The configuration commands are available in the config mode. To move from Privileged EXEC mode to the Configuration mode, enter the following command at the command prompt:

```
(AP)# configure terminal
```

The configure terminal command allows you to enter the basic configuration mode and the command prompt is displayed as follows:

```
(AP)(config)#
```

The SCALANCE W CLI allows CLI scripting in several other subcommand modes to allow the users to configure individual interfaces, SSIDs, access rules, and security settings.

You can use the question mark (?) to view the commands available in a privileged EXEC mode, configuration mode, or subcommand mode.

Note

Although automatic completion is supported for some commands such as **configure terminal**, the complete **exit** and **end** commands must be entered at command prompt.

Applying Configuration Changes

Each command processed by the virtual controller is applied on all the slaves in a cluster. The changes configured in a CLI session are saved in the CLI context. The CLI does not support the configuration data exceeding the 4K buffer size in a CLI session. Therefore, it is recommended that you configure fewer changes at a time and apply the changes at regular intervals.

To apply and save the configuration changes at regular intervals, execute the following command in the privileged EXEC mode:

```
(AP)# commit apply
```

To apply the configuration changes to the cluster without saving the configuration, execute the following command in the privileged EXEC mode:

```
(AP)# commit apply no-save
```

To view the changes that are yet to be applied, execute the following command in the privileged EXEC mode:

```
(AP)# show uncommitted-config
```

To revert to the earlier configuration, execute the following command in the privileged EXEC mode.

```
(AP)# commit revert
```

Example:

To apply and view the configuration changes:

```
(AP)(config)# rf dot11a-radio-profile

(AP)# show uncommitted-config
```

Using Sequence-Sensitive Commands

The SCALANCE W CLI does not support positioning or precedence of sequence-sensitive commands. Therefore, it is recommended that you remove the existing configuration before adding or modifying the configuration details for sequence-sensitive commands. You can either delete an existing profile or remove a specific configuration by using the **no** commands.

The following table lists the sequence-sensitive commands and the corresponding **no** commands to remove the configuration:

Table 4- 1 *Sequence-Sensitive Commands*

<table>
<tr><th>Sequence-Sensitive Command</th><th>Corresponding no command</th></tr>
<tr><td>opendns <username <password></td><td>no opendns</td></tr>
<tr><td>rule <dest> <mask> <match> <protocol> <start-port> <end-port> {permit | deny | src-nat | dst-nat {<IP- address> <port> | <port>}}[<option1....option9>]</td><td>no rule <dest> <mask> <match> <protocol> <start-port> <end-port> {permit | deny | src-nat | dst-nat}</td></tr>
<tr><td>mgmt-auth-server <auth-profile-name></td><td>no mgmt-auth-server <auth-profile- name></td></tr>
<tr><td>set-role <attribute>{{equals| not-equals | starts-with | ends-with | contains} <operator> <role> | value-of}</td><td>no set-role <attribute>{{equals | not-equals | starts-with | ends-with | contains} <operator>| value-of} no set-role</td></tr>
<tr><td>set-vlan <attribute>{{equals | not-equals | starts- with | ends-with | contains} <operator> <VLAN-ID> | value-of}</td><td>no set-vlan <attribute>{{equals | not-equals | starts-with | ends-with | contains} <operator> | value-of} no set-vlan</td></tr>
<tr><td>auth-server <name></td><td>no auth-server <name></td></tr>
</table>

Banner and Login session Configuration using CLI

The text banner can be displayed at the login prompt when users are on a management (Telnet or SSH) session of the CLI, and the management session can remain active even when there is no user activity involved.

The **banner** command defines a text banner to be displayed at the login prompt of a CLI. SCALANCE W supports up to 16 lines text, and each line accepts a maximum of 255 characters including spaces.

To configure a banner:

```
(AP)(config)# banner motd <motd_text>
```

To display the banner:

```
(AP)# show banner
```

The **loginsession** command configures the management session (Telnet or SSH) to remain active without any user activity.

To define a timeout interval:

```
(AP) (config) #loginsession timeout <val>
```

<val> can be any number of minutes from 5 to 60, or any number of seconds from 1 to 3600. You can also specify a timeout value of 0 to disable CLI session timeouts. The users must re-login to the AP after the session times out. The session does not time out when the value is set to 0.

4.5 AP Degraded State

The following conditions may cause an AP to prevent users from logging in to the SCALANCE W UI and CLI. In most cases, the AP will display the error message **Warning: CLI Module is running in a degraded state. Some commands will not function.**

1. When the AP cannot be a master AP because it has no IP address, and does not have an uplink connection.
2. When the AP is unable to join the cluster because of a missing country code, image, or incorrect regulatory hardware.
3. When the AP has been denied permission to the existing cluster based on the allowed AP whitelist or the auto-join configuration present in the cluster.
4. In a mixed class network, when the slave APs join the master AP with a different software version, causing the image sync from the cloud or AirWave to fail.

Additionally, the following console messages indicate other error conditions:

- **4-0 Authentication server failure**: Incorrect username or password.
- **5-0 Authentication server timeout** - no response from RADIUS server.
- **7-0**: Indicates PAPI errors within the AP. The AP log messages provide details on the error condition. Consult Technical Support for further assistance.
- **8-0**: Indicates an authentication failure or an incomplete synchronization of a swarm configuration.

An example of one of the above mentioned console messages is **Internal error 7-0, please contact support**.

Automatic Retrieval of Configuration 5

5.1 Managed Mode Operations

APs support managed mode operations to retrieve the configuration file from a server through the FTP or FTPS, and automatically update the AP configuration.

The server details for retrieving configuration files are stored in the basic configuration of the APs. The basic configuration of an AP includes settings specific to an AP, for example, host name, static IP, and radio configuration settings. When an AP boots up, it performs a GET operation to retrieve the configuration (.cfg) file from the associated server using the specified download method.

After the initial configuration is applied to the APs, the configuration can be changed at any point. You can configure a polling mechanism to fetch the latest configuration by using an FTP or FTPS client periodically. If the remote configuration is different from the one running on the AP and if a difference in the configuration file is detected by the AP, the new configuration is applied. At any given time, APs can fetch only one configuration file, which may include the configuration details specific to an AP. For configuring polling mechanism and downloading configuration files, the users are required to provide credentials (username and password). However, if automatic mode is enabled, the user credentials required to fetch the configuration file are automatically generated. To enable automatic configuration of the APs, configure the managed mode command parameters.

5.2 Prerequisites

Perform the following checks before configuring the managed mode command parameters:

- When the APs are in the managed mode, ensure that the APs are not managed by AirWave.

5.3 Configuration Managed Mode Parameters

To enable the automatic configuration, perform the steps described in the following table:

Table 5- 1 Managed Mode Commands

Steps		Command
1	Start a CLI session to configure the managed-mode profile for automatic configuration.	`(AP)(config)# managed-mode-profile`

2	Enable automatic configuration
	Or
	Specify the user credentials.
		`(AP)(managed-mode-profile)# automatic`
		Or
		`(AP)(managed-mode-profile)# username <username>`
		`(AP)(managed-mode-profile)# password <password>`
		NOTE: If the automatic mode is enabled, the user credentials are automatically generated based on AP MAC address.

3	Specify the configuration file.	`(AP)(managed-mode-profile)# config-filename<file_name>` Filename—Indicates filename in the alphanumeric format. Ensure that configuration file name does not exceed 40 characters.
4	Specify the configuration file download method.	`(AP)(managed-mode-profile)# download-method <ftp|ftps>` You can use either FTP or FTPS for downloading configuration files.
5	Specify the name of the server or the IP address of the server from which the configuration file must be downloaded.	`(AP)(managed-mode-profile)# server <server_name>`
6	Configure the day and time at which the APs can poll the configuration files from the server.	`(AP) (managed-mode-profile)# sync-time day <dd> hour <hh> min <mm> window <window>` Based on the expected frequency of configuration changes and maintenance window, you can set the configuration synchronization timeline. • `day <dd`>—Indicates day, for example to configure Sunday as the day, specify 01. To configure the synchronization period as everyday, specify 00. • `hour <hh>`—Indicates hour within the range of 0–23. • `min <mm>`—Indicates minutes within the range of 0–59. • `window <hh>`—Defines a window for synchronization of the configuration file. The default value is 3 hours.
7	Configure the time interval in minutes between two retries, after which APs can retry downloading the configuration file.	`(AP)(managed-mode-profile)# retry-poll-period <seconds>` **NOTE:** Specify the retry interval in seconds within the range of 5–60 seconds. The default retry interval is 5 seconds.

8	Apply the configuration changes.	`(AP)(managed-mode-profile)# end`
		`(AP)# commit apply`

If you want to apply the configuration immediately and do not want to wait until next configuration retrieval attempt, execute the following command:

```
(AP)# managed-mode-sync-server
```

Example

To configure managed mode profile:

```
(AP)(config)# managed-mode-profile
```

5.4 Verifying the Configuration

To verify if the automatic configuration functions, perform the following checks:

1. Verify the status of configuration by running the following commands at the command prompt:

   ```
   (AP)# show managed-mode config
   ```

   ```
   (AP)# show managed-mode status
   ```

2. Verify the status of download by running the following command at the command prompt:

   ```
   (AP)# show managed-mode logs
   ```

If the configuration settings retrieved in the configuration file are incomplete, APs reboot with the earlier configuration.

SCALANCE W User Interface 6

6.1 Login Screen

The SCALANCE W login page allows you to perform the following tasks:

- View SCALANCE W Network Connectivity summary
- View the SCALANCE W UI in a specific language
- Log in to the SCALANCE W UI

Viewing Connectivity Summary

The login page also displays the connectivity status to the SCALANCE W network. The users can view a summary that indicates the status of the Internet availability, uplink, cellular modem and signal strength, VPN, and AirWave configuration details before logging in to the SCALANCE W UI.

Language

The **Language** drop-down list contains the available languages and allows users to select their preferred language before logging in to the SCALANCE W UI. A default language is selected based on the language preferences in the client desktop operating system or browser. If SCALANCE W cannot detect the language, then **English** is used as the default language.

You can also select the required language option from the **Languages** drop-down list located on the SCALANCE W main window.

Logging into the SCALANCE W UI

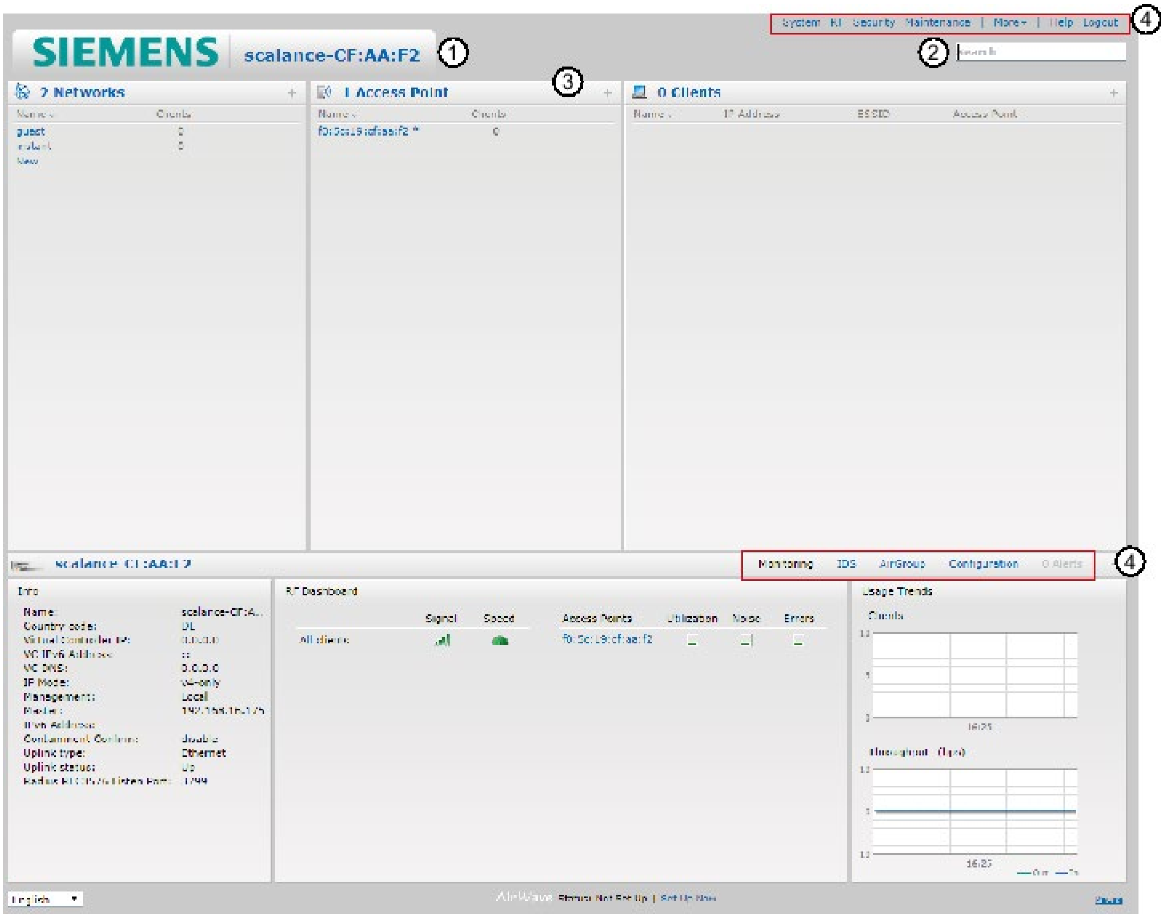
To log in to the SCALANCE W UI, enter the following credentials:

- Username — admin
- Password — admin

The SCALANCE W UI main window is displayed.

6.2 Main Window

After you log in to SCALANCE W, the UI main window is displayed



Info

Name: scalance-CF:A...
Country code: DL
Virtual Controller IP: 0.0.0.0
VC IPv6 Address: ::
VC DNS: 0.0.0.0
IP Mode: v4-only
Management: Local
Master: 192.168.16.175
IPv6 Address:
Containment Control: disable
Uplink type: Ethernet
Uplink status: Up

Figure 6-1 SCALANCE W Main Window

The main window consists of the following elements:

- ① Banner (Page 47)
- ② Search Text Box (Page 47)
- ③ Tabs (Page 47)
- ④ Links (Page 50)
- Views (Page 72)

6.2.1 Banner

The banner is a horizontal gray rectangle that appears on the SCALANCE W main window. It displays the company name, logo, and the virtual controller name.

6.2.2 Search Text Box

Administrators can search for an AP, client, or a network in the **Search** text box. When you type a search text, the search function suggests matching keywords and allows you to automatically complete the search text entry.

6.2.3 Tabs

The SCALANCE W main window consists of the following tabs:

- Network Tab (Page 47)— Provides information about the network profiles configured in the SCALANCE W network.
- Access Points Tab (Page 48)— Provides information about the APs configured in the SCALANCE W network.
- Clients Tab (Page 49)— Provides information about the clients in the SCALANCE W network.

Each tab appears in a compressed view by default. The number of networks, APs, or clients in the network precedes the corresponding tab names. The individual tabs can be expanded or collapsed by clicking the tabs. The list items in each tab can be sorted by clicking the triangle icon next to the heading labels.

6.2.3.1 Network Tab

This tab displays a list of Wi-Fi networks that are configured in the SCALANCE W network. The network names are displayed as links. The expanded view displays the following information about each WLAN SSID:

- **Name** — Name of the network.
- **Clients** — Number of clients that are connected to the network.
- **Type** — Type of network such as Employee, Guest, or Voice.
- **Band** — Band in which the network is broadcast: 2.4 GHz band, 5 GHz band, or both.
- **Authentication Method** — Authentication method required to connect to the network.
- **Key Management** — Authentication key type.
- **IP Assignment** — Source of IP address for the client.
- **Zone** — AP zone configured on the SSID.

To add a wireless network profile, click the **New** link on the **Network** tab. To edit, click the **edit** link that is displayed on clicking the network name in the **Network** tab. To delete a network, click the **x** link.
For more information on the procedure to add or modify a wireless network, see Wireless Network Profiles (Page 95).

6.2.3.2 Access Points Tab

If the Auto-Join Mode feature is enabled, a list of enabled and active APs in the SCALANCE W network is displayed on the **Access Points** tab. The AP names are displayed as links. If the Auto Join Mode feature is disabled, the **New** link is displayed. Click this link to add a new AP to the network. If an AP is configured and not active, its MAC Address is displayed in red.

The expanded view of the **Access Points** tab displays the following information about each AP:

- **Name**—Name of the AP. If the AP functions as a master AP in the network, the asterisk sign "*" is displayed next to the AP.
- **IP Address**—IP address of the AP.
- **Mode**—Mode of the AP.
  - **Access**—In this mode, the AP serves clients and scans the home channel for spectrum analysis while monitoring channels for rogue APs in the background.
  - **Monitor** — In this mode, the AP acts as a dedicated AM, scanning all channels for rogue APs and clients.
- **Spectrum**—When enabled, the AP functions as a dedicated full-spectrum RF monitor, scanning all channels to detect interference from neighboring APs or non-Wi-Fi devices such as microwaves and cordless phones. When Spectrum is enabled, the AP does not provide access services to clients.
- **Clients**—Number of clients that are currently associated to the AP.
- **Type**—Model number of the AP.
- **Mesh Role**—Role of the AP as a mesh portal or mesh point.
- **Zone**—AP zone.
- **Serial number**—Serial number of the device.
- **Channel**—Channel on which the AP is currently broadcast.
- **Power (dB)**—Maximum transmission Effective Isotropic Radiated Power (EIRP) of the radio.
- **Utilization (%)**—Percentage of time that the channel is utilized.
- **Noise (dBm)**—Noise floor of the channel.

An **edit** link is displayed on clicking the AP name. For details on editing AP settings, see Customizing AP Settings (Page **Fehler! Textmarke nicht definiert.**).

6.2.3.3 Clients Tab

This tab displays a list of clients that are connected to the SCALANCE W network. The client names are displayed as links. The expanded view displays the following information about each client:

- **Name**—Username of the client or guest users if available.
- **IP Address**—IP address of the client.
- **MAC Address**—MAC address of the client.
- **OS**—Operating system that runs on the client.
- **ESSID**—ESSID to which the client is connected.
- **Access Point**—AP to which the client is connected.
- **Channel**—The client operating channel.
- **Type**—Type of the Wi-Fi client.
- **Role**—Role assigned to the client.
- **Signal**—Current signal strength of the client, as detected by the AP.
- **Speed (mbps)**—Current speed at which data is transmitted. When the client is associated with an AP, it constantly negotiates the speed of data transfer. A value of 0 means that the AP has not heard from the client for some time.

6.2.4 Links

The following links allow you to configure various features for the SCALANCE W network:

- New Version Available (Page **Fehler! Textmarke nicht definiert.**)
- System (Page 51)
- RF (Page 52)
- Security (Page 52)
- Maintenance (Page 53)
- More (Page 54)
- Help (Page 56)
- Logout (Page 56)
- Monitoring (Page 56)
- Client Match (Page 66)
- AppRF (Page 66)
- Spectrum (Page 67)
- Alerts (Page 68)
- IDS (Page 70)
- AirGroup (Page 71)
- Configuration (Page 71)
- AirWave Setup (Page 71)
- Pause/Resume (Page 72)

Each of these links is explained in the subsequent sections.

6.2.4.1 System

This link displays the **System** window. The **System** window consists of the following tabs:

Note

Use the **Show/Hide Advanced** option of the **System** window to view or hide the advanced options.

- **General**—Allows you to configure, view, or edit the Name, IP address, NTP Server, and other AP settings for the virtual controller.
- **Admin**—Allows you to configure administrator credentials for access to the virtual controller management UI. You can also configure AirWave in this tab. For more information on management interface and AirWave configuration, see Managing AP Users (Page 173) and Managing an AP from AirWave (Page 385), respectively.
- **Uplink**—Allows you to view or configure uplink settings. See Uplink Configuration (Page 395) for more information.
- **L3 Mobility**—Allows you to view or configure the Layer-3 mobility settings. See Configuring Layer-3 Mobility (Page 422) for more information.
- **Enterprise Domains**—Allows you to view or configure the DNS domain names that are valid in the enterprise network. See Configuring Enterprise Domains (Page 233) for more information.
- **Monitoring**—Allows you to view or configure the following details:
  - **Syslog**—Allows you to view or configure Syslog server details for sending syslog messages to the external servers. See Configuring a Syslog Server (Page 443) for more information.
  - **TFTP Dump**—Allows you to view or configure a TFTP dump server for core dump files. See Configuring TFTP Dump Server (Page 445) for more information.
  - **SNMP**—Allows you to view or configure SNMP agent settings. See Configuring SNMP (Page 439) for more information.

- **WISPr**—Allows you to view or configure the WISPr settings. See Configuring WISPr Authentication (Page 212) for more information.
- **Proxy**—Allows you to configure HTTP proxy on an AP. See Configuring HTTP Proxy on an AP (Page **Fehler! Textmarke nicht definiert.**).
- **Time Based Services**—Allows you to configure a time profile which can be assigned to the SSID configured on the AP. See Configuring Time-Based Services (Page 265) (Page 265)

6.2.4.2 RF

The **RF** link displays a window for configuring ARM and Radio features.

- **ARM**—Allows you to view or configure channel and power settings for all the APs in the network. For information on ARM configuration, see ARM Overview (Page 321).
- **Radio**—Allows you to view or configure radio settings for 2.4 GHz and the 5 GHz radio profiles. For information on Radio, see Configuring Radio Settings (Page 330).

6.2.4.3 Security

The **Security** link displays a window with the following tabs:

- **Authentication Servers**—Use this tab to configure an external RADIUS server for a wireless network. For more information, see Configuring an External Server for Authentication (Page 188).
- **Users for Internal Server**—Use this tab to populate the system’s internal authentication server with users. This list is used by networks for which per-user authorization is specified using the internal authentication server of the virtual controller. For more information on users, see Managing AP Users (Page 173).
- **Roles** —Use this tab to view the roles defined for all the Networks. The Access Rules part allows you to configure permissions for each role. For more information, see Configuring User Roles (Page 237) and Configuring ACL Rules for Network Services (Page 220).
- **Blacklisting**—Use this tab to blacklist clients. For more information, see Blacklisting Clients (Page 213).
- **Firewall Settings**—Use this tab to enable or disable ALG supporting address and port translation for various protocols and to configure protection against wired attacks. For more information, see Configuring ALG Protocols (Page 225) and Configuring Firewall Settings for Protection from ARP Attacks (Page 226).
- **Inbound Firewall**—Use this tab to enhance the inbound firewall by allowing the configuration of inbound firewall rules, management subnets, and restricted corporate access through an uplink switch. For more information, see Managing Inbound Traffic (Page 228).
- **Walled Garden**—Use this tab to allow or prevent access to a selected list of websites. For more information, see Configuring Walled Garden Access (Page 169).
- **External Captive Portal**—Use this tab to configure external captive portal profiles. For more information, see Configuring External Captive Portal for a Guest Network (Page 162).

- **Custom Blocked Page URL**—Use this tab to create a list of URLs that can be blocked using an ACL rule. For more information, see Creating Custom Error Page for Web Access Blocked by AppRF Policies (Page 233).

6.2.4.4 Maintenance

The **Maintenance** link displays a window that allows you to maintain the Wi-Fi network. The **Maintenance** window consists of the following tabs:

- **About** — Displays the name of the product, build time, AP model name, the SCALANCE W version, website address of Siemens, and copyright information.
- **Configuration** — Displays the following details:
  - **Current Configuration** — Displays the current configuration details.
  - **Clear Configuration** — Allows you to clear the current configuration details of the network. Select the **Remove all configurations including per-AP settings and certificates** checkbox to remove the per-AP settings and certificates as well.

Note

The **Remove all configurations including per-AP settings and certificates** option is applicable only to clear configurations. It is not applicable to backup and restore configurations.

  - **Backup Configuration** — Allows you to back up local configuration details. The backed up configuration data is saved in the file named **backup.cfg**.
  - **Restore Configuration** —Allows you to restore the backed up configuration. After restoring the configuration, the AP must be rebooted for the changes to take effect.

- **Certificates**—Displays information about the certificates installed on the AP. You can also upload new certificates to the AP database, see Uploading Certificates (Page 216).
- **Firmware**—Displays the current firmware version and provides various options to upgrade to a new firmware version.
- **Reboot**—Displays the APs in the network and provides an option to reboot the required AP or all APs. See Upgrading an AP (Page **Fehler! Textmarke nicht definiert.**).
- **Convert**—Provides an option to convert an AP to a Mobility Controller managed Remote AP or Campus AP, or to the default virtual controller mode. For more information, see Converting an AP to a Remote AP and Campus AP (Page 434).

6.2.4.5 More

The **More** link allows you to select the following options:

- VPN
- IDS
- Wired
- Services
- DHCP Server
- Support

VPN

The **VPN** window allows you to define communication settings with a controller or a third party VPN concentrator. See VPN Configuration (Page 273) for more information. The following figure shows an example of the IPsec configuration options available in the **VPN** window:

IDS

The **IDS** window allows you to configure wireless intrusion detection and protection levels. The following figures show the **IDS** window:

For more information on wireless intrusion detection and protection, see Detecting and Classifying Rogue APs (Page 409).

Wired

The **Wired** window allows you to configure a wired network profile. See Wired Profiles (Page 125) for more information.

Services

The **Services** window allows you to configure services such as AirGroup, RTLS, and OpenDNS. The Services window consists of the following tabs:

- **AirGroup** — Allows you to configure the AirGroup and AirGroup services. For more information, see Configuring AirGroup (Page 351).
- **RTLS** — Allows you to integrate AMP or third-party RTLS such as Aeroscout RTLS with SCALANCE W. For more information, see Configuring an AP for RTLS Support (Page 361). The RTLS tab also allows you to integrate AP with the ALE. For more information about configuring an AP for ALE integration, see Configuring an AP for Analytics and Location Engine Support (Page 362).
- **OpenDNS** — Allows you to configure support for OpenDNS business solutions, which require an OpenDNS (www.opendns.com) account. The OpenDNS credentials are used by SCALANCE W and AirWave to filter content at the enterprise level. For more information, see Configuring OpenDNS Credentials (Page 367).
- **CALEA** — Allows you to configure support for CALEA server integration, thereby ensuring compliance with Lawful Intercept and CALEA specifications. For more information, see CALEA Integration and Lawful Intercept Compliance (Page 372).
- **Network Integration** — Allows you to configure an AP for integration with Palo Alto Networks Firewall and XML API server. For more information on AP integration with PAN, see Integrating an AP with Palo Alto Networks Firewall (Page 367) and Integrating an AP with an XML API Interface (Page 369).

DHCP Server

The **DHCP Servers** window allows you to configure various DHCP modes. For more information, see DHCP Configuration (Page 253).

Support

The **Support** link consists of the following details:

- **Command**—Allows you to select a support command for execution.
- **Target**—Displays a list of APs in the network.
- **Run**—Allows you to execute the selected command for a specific AP or all APs and view logs.
- **Auto Run**—Allows you to configure a schedule for automatic execution of a support command for a specific AP or all APs.
- **Filter**—Allows you to filter the contents of a command output.
- **Clear**—Clears the command output that is displayed after a command is executed.
- **Save**—Allows you to save the support command logs as an HTML or text file.

For more information on support commands, see Running Debug Commands (Page 446).

6.2.4.6 Help

The **Help** link allows you to view a short description or definition of the selected terms in the UI windows or the dialog boxes.

To activate the context-sensitive help:

1. Click the **Help** link available above the Search bar on the SCALANCE W main window.
2. Click any text or term displayed in green italics to view its description or definition.
3. To disable the help mode, click **Done**.

6.2.4.7 Logout

The **Logout** link allows you to log out of the SCALANCE W UI.

6.2.4.8 Monitoring

The **Monitoring** link displays the Monitoring pane for the SCALANCE W network. Use the down arrow located to the right side of these links to compress or expand the Monitoring pane.

The Monitoring pane consists of the following sections:

- Info
- RF Dashboard
- RF Trends
- Usage Trends
- Mobility Trail

Info

The **Info** section displays the configuration informatio of the virtual controller by default. On selecting the **Network View** tab, the monitoring pane displays configuration information of the selected network. Similarly, if the **Access Point** or the **Client** view, this section displays the configuration information of the selected AP or the client.

Table 6- 1 *Contents of the Info Section in the SCALANCE W Main Window*

Name	Description
Info section in the **Virtual Controller** view	The **Info** section in the **Virtual Controller** view displays the following information: • **Name**—Displays the virtual controller name. • **Country Code**—Displays the Country in which the virtual controller is operating. • **Virtual Controller IP address**—Displays the IP address of the virtual controller. • **VC DNS**—Displays the DNS IP address configured for the virtual controller. • **Management**—Indicates if the AP is managed locally or through AirWave I. • **Master**—Displays the IP address of the AP acting as virtual controller. • **OpenDNS Status**—Displays the OpenDNS status. If the OpenDNS status indicates **Not Connected**, ensure that the network connection is up and appropriate credentials are configured for **OpenDNS**. • **MAS integration**—Displays the status of the Mobility Access Switch integration feature. • **Uplink type**—Displays the type of uplink configured of the AP, for example, Ethernet or 3G. • **Uplink status**—Indicates the uplink status. • **Blacklisted clients**—Displays the number of blacklisted clients. • **Internal RADIUS Users**—Displays the number of internal RADIUS users. • **Internal Guest Users**—Displays the number of internal guest users. • **Internal User Open Slots**—Displays the available slots for user configuration as supported by the AP model.
Info section in the **Network** view	The **Info** section in the **Network** view displays the following information: • **Name**—Displays the name of the network. • **Status**—Displays the status of the network. • **Type**—Displays the type of network, for example, Employee, Guest, or Voice. • **VLAN**—Displays VLAN details. • **IP Assignment**—Indicates if the AP clients are assigned IP address from the network that the virtual controller is connected to, or from an internal autogenerated IP scope from the virtual controller. • **Access**—Indicates the level of access control configured for the network. • **WMM DSCP**—Displays WMM DSCP mapping details. • **Security level**—Indicates the type of user authentication and data encryption configured for the network. The **info** section for WLAN SSIDs also indicates status of captive portal and CALEA ACLs and provides a link to upload certificates for the internal server. For more information, see Uploading Certificates (Page 216).

Name	Description
Info section in the **Access Point** view	The **Info** section in the **Access Point** view displays the following information: • **Name**—Displays the name of the selected AP. • **IP Address**—Displays the IP address of the AP. • **Mode**—Displays the mode in which the AP is configured to operate. • **Spectrum**—Displays the status of the spectrum monitor. • **Clients**—Number of clients associated with the AP. **Type**—Displays the model number of the AP. • **Zone**—Displays AP zone details. • **CPU Utilization**—Displays the CPU utilization in percentage. • **Memory Free**—Displays the memory availability of the AP in MB. • **Serial number**—Displays the serial number of the AP. • **MAC**—Displays the MAC address. • **From Port**—Displays the port from where the slave AP is learned in hierarchy mode.
Info section in the **Client** view	The **Info** section in the **Client** view displays the following information: • **Name**—Displays the name of the client. • **IP Address**—Displays the IP address of the client. • **MAC Address**—Displays MAC address of the client. • **OS**—Displays the operating system that is running of the client. • **ESSID**—Indicates the network to which the client is connected. • **Access Point**—Indicates the AP to which the client is connected. • **Channel**—Indicates the channel that is currently used by the client. • **Type**—Displays the channel type on which the client is broadcasting. • **Role**—Displays the role assigned to the client.

RF Dashboard

The **RF Dashboard** section lists the APs that exceed the utilization, noise, or error threshold. It also shows the clients with low speed or signal strength in the network and the RF information for the AP to which the client is connected.

The AP names are displayed as links. When an AP is clicked, the AP configuration information is displayed in the Info section and the RF Dashboard section is displayed on the SCALANCE W main window.

The following table describes the icons available on the RF Dashboard pane::

Table 6- 2 *RF Dashboard Icons*

Icon number	Name	Description
1	Signal	Displays the signal strength of the client. Signal strength is measured in decibels. Depending of the signal strength of the client, the color of the lines of the Signal icon changes in the following order: • Green— Signal strength is more than 20 dB. • Orange — Signal strength is between 15 dB and 20 dB. • Red — Signal strength is less than 15 dB. To view the signal graph for a client, click the signal in conext to the client in the **Signal** column.
2	Speed	Displays the data transfer speed of the client. Depending on the data transfer speed of the client, the color of the Speed icon changes in the following order: • Green—Data transfer speed is more than 50% of the maximum speed supported by the client. • Orange—Data transfer speed is between 25% and 50% of the maximum speed supported by the client. • Red—Data transfer speed is less than 25% of the maximum speed supported by the client. To view the data transfer speed graph of a client, click the speed icon corresponding to the client name in the **Speed** column.
3	Utilization	Displays the noise floor details for the APs. Noise is measured in decibels/meter. Depending on the percentage of noise floor utilization, the color of the lines on the Utilization icon changes in the following order: • Green—Utilization is less than 50%. • Orange—Utilization is between 50% and 75%. • Red—Utilization is more than 75%. To view the utilization graph of an AP, click the Utilization icon next to the AP in the **Utilization** column.

Icon number	Name	Description
4	Noise	Displays the noise floor details for the APs. Noise is measured in decibel per meter. Depending on the noise floor, the color of the lines on the Noise icon changes in the following order: • Green—Noise floor is more than -87 dBm. • Orange—Noise floor is between -80 dBm and -87 dBm. • Red—Noise floor is less than -80 dBm. To view the noise floor graph of an AP, click the Noise icon next to the AP in the **Noise** column.
5	Errors	Displays the errors for the APs. Depending on the errors, color of the lines on the Errors icon changes in the following order: • Green— Errors are less than 5000 frames per second. • Orange — Errors are between 5000 and 10,000 frames per second. • Red — Errors are more than 10000 frames per second.

RF Trends

The **RF Trends** section displays the graphs for the selected AP and the client. To view the details on the graphs, click the graphs and hover the mouse on a data point.

The following table describes the RF trends graphs available in the Client view:

Table 6- 3 *Client View—RF Trends Graphs and Monitoring Procedures*

Graph Name	Description	Monitoring Procedure
Signal	The Signal graph shows the signal strength of the client for the last 15 minutes. It is measured in dB. To see an enlarged view, click the graph. The enlarged view provides Last, Minimum, Maximum, and Average signal statistics of the client for the last 15 minutes. To see the exact signal strength at a particular time, move the cursor over the graph line.	To monitor the signal strength of the selected client for the last 15 minutes: 1. Log in to the SCALANCE W UI. The Virtual Controller view is displayed. This is the default view. 2. On the **Clients** tab, click the IP address of the client for which you want to monitor the signal strength. 3. Study the Signal graph in the RF Trends pane. For example, the graph shows that signal strength for the client is 54.0 dB at 12:23 hours.
Frames	The Frames graph shows the In and Out frame rate per second of the client for the last 15 minutes. It also shows data for the Retry In and Retry Out frames. • Outgoing frames — Outgoing frame traffic is displayed in green. It is show above the median line. • Incoming frames — Incoming frame traffic is displayed in blue. It is show below the median line. • Retry Out — Retries for the outgoing frames are displayed above the median line in black . • Retry In— Retries for the incoming frames are displayed below the median line in red. To see an enlarged view, click the graph. The enlarged view provides Last, Minimum, Maximum, and Average statistics for the In, Out, Retries In, and Retries Out frames. To see the exact frames at a particular time, move the cursor over the graph line.	To monitor the In and Out frame rate per second and retry frames for the In and Out traffic, for the last 15 minutes: 1. Log in to the SCALANCE W UI. The Virtual Controller view is displayed. This is the default view. 2. On the **Clients** tab, click the IP address of the client for which you want to monitor the frames. 3. Study the Frames graph in the RF Trends pane. For example, the graph shows 4.0 frames per second for the client at 12:27 hours.

Graph Name	**Description**	**Monitoring Procedure**
Speed	The Speed graph shows the data transfer speed for the client. Data transfer is measured in Mbps To see an enlarged view, click the graph. The enlarged view shows Last, Minimum, Maximum, and Average statistics of the client for the last 15 minutes. To see the exact speed at a particular time, move the cursor over the graph line.	To monitor the speed for the client for the last 15 minutes: 1. Log in to the SCALANCE W UI. The Virtual Controller view is displayed. This is the default view. 2. On the **Clients** tab, click the IP address of the client for which you want to monitor the speed. 3. Study the Speed graph in the RF Trends pane. For example, the graph shows that the data transfer speed at 12:26 hours is 240 Mbps.
Throughput	The Throughput Graph shows the throughput of the selected client for the last 15 minutes. • Outgoing traffic — Throughput for the outgoing traffic is displayed in green. It is shown above the median line. • Incoming traffic — Throughput for the incoming traffic is displayed in blue. It is shown below the median line. To see an enlarged view, click the graph. The enlarged view shows Last, Minimum, Maximum, and Average statistics for the incoming and outgoing traffic throughput of the client for the last 15 minutes. To see the exact throughput at a particular time, move the cursor over the graph line.	To monitor the errors for the client for the last 15 minutes: 1. Log in to the SCALANCE W UI. The Virtual Controller view is displayed. This is the default view. 2. In the **Clients** tab, click the IP address of the client for which you want to monitor the throughput. 3. Study the Throughput graph in the RF Trends pane. For example, the graph shows 1.0 Kbps outgoing traffic throughput for the client at 12:30 hours.

Usage Trends

The **Usage Trends** section displays the following graphs:

- **Clients** — In the default view, the Clients graph displays the number of clients that were associated with the virtual controller in the last 15 minutes. In Network view or the Access Point view, the graph displays the number of clients that were associated with the selected network or AP in the last 15 minutes.
- **Throughput** —In the default view, the Throughput graph displays the incoming and outgoing throughput traffic for the virtual controller in the last 15 minutes. In the Network view or the Access Point view, the graph displays the incoming and outgoing throughput traffic for the selected network or AP in the last 15 minutes.

The following table describes the graphs displayed in the Network view:

Table 6- 4 *Network View—Graphs and Monitoring Procedures*

Graph Name	Description	Monitoring Procedure
Clients	The Clients graph shows the number of clients associated with the network for the last 15 minutes. To see an enlarged view, click the graph. • The enlarged view provides Last, Minimum, Maximum, and Average statistics for the number of clients associated with the virtual controller for the last 15 minutes. • To see the exact number of clients in the SCALANCE W network at a particular time, move the cursor over the graph line.	To check the number of clients associated with the network for the last 15 minutes: 1. Log in to the SCALANCE W UI. The Virtual Controller view is displayed. This is the default view. 2. On the **Network** tab, click the network for which you want to check the client association. 3. Study the Clients graph in the **Usage Trends** pane. For example, the graph shows that one client is associated with the selected network at 12:00 hours.
Throughput	The Throughput graph shows the throughput of the selected network for the last 15 minutes. • Outgoing traffic — Throughput for the outgoing traffic is displayed in green. Outgoing traffic is shown above the median line. • Incoming traffic — Throughput for the incoming traffic is displayed in blue. Incoming traffic is shown below the median line. To see an enlarged view, click the graph • The enlarged view provides Last, Minimum, Maximum, and Average statistics for the incoming and outgoing traffic throughput of the network for the last 15 minutes. To see the exact throughput of the selected network at a particular time, move the cursor over the graph line.	To check the throughput of the selected network for the last 15 minutes, 1. Log in to the SCALANCE W UI. The Virtual Controller view is displayed. This is the default view. 2. On the **Network** tab, click the network for which you want to check the client association. 3. Study the Throughput graph in the **Usage Trends** pane. For example, the graph shows 22.0 Kbps incoming traffic throughput for the selected network at 12:03 hours.

The following table describes the graphs displayed in the Network view:

Table 6- 5 *Access Point View—Usage Trends and Monitoring Procedures*

Graph Name	Description	Monitoring Procedure
Neighboring APs	The Neighboring APs graph shows the number of APs detected by the selected AP: • Valid APs: An AP that is part of the enterprise providing WLAN service. • Interfering APs: An AP that is seen in the RF environment but is not connected to the network. • Rogue APs: An unauthorized AP that is plugged into the wired side of the network. To see the number of different types of neighboring APs for the last 15 minutes, move the cursor over the respective graph lines.	To check the neighboring APs detected by the AP for the last 15 minutes: 1. Log in to the SCALANCE W UI. The Virtual Controller view is displayed. This is the default view. 2. On the **Access Points** tab, click the AP for which you want to monitor the client association. Study the Neighboring APs graph in the **Overview** section. For example, the graph shows that 148 interfering APs are detected by the AP at 12:04 hours.
CPU Utilization	The CPU Utilization graph displays the utilization of CPU for the selected AP. To see the CPU utilization of the AP, move the cursor over the graph line.	To check the CPU utilization of the AP for the last 15 minutes: • Log in to the SCALANCE W UI. The Virtual Controller view is displayed. This is the default view. • On the **Access Points** tab, click the AP for which you want to monitor the client association. • Study the CPU Utilization graph in the **Overview** pane. For example, the graph shows that the CPU utilization of the AP is 30% at 12:09 hours.
Neighboring Clients	The Neighboring Clients graph shows the number of clients not connected to the selected AP, but heard by it. • Any client that successfully authenticates with a valid AP and passes encrypted traffic is classified as a valid client. • Interfering: A client associated to any AP and is not valid is classified as an interfering client. To see the number of different types of neighboring clients for the last 15 minutes, move the cursor over the respective graph lines.	To check the neighboring clients detected by the AP for the last 15 minutes, 1. Log in to the SCALANCE W UI. The Virtual Controller view is displayed. This is the default view. 2. On the **Access Points** tab, click the AP for which you want to monitor the client association. 3. Study the Neighboring Clients graph in the **Overview** pane. For example, the graph shows that 20 interfering clients were detected by the AP at 12:15 hours.

Graph Name	Description	Monitoring Procedure
Memory free (MB)	The Memory free graph displays the memory availability of the AP in MB. To see the free memory of the AP, move the cursor over the graph line.	To check the free memory of the AP for the last 15 minutes: 1. Log in to the SCALANCE W UI. The Virtual Controller view is displayed. This is the default view. 2. On the **Access Points** tab, click the AP for which you want to monitor the client association. 3. Study the Memory free graph in the **Overview** pane. For example, the graph shows that the free memory of the AP is 64 MB at 12:13 hours.
Clients	The Clients graph shows the number of clients associated with the selected AP for the last 15 minutes. To see an enlarged view, click the graph. The enlarged view provides Last, Minimum, Maximum, and Average statistics for the number of clients associated with the AP for the last 15 minutes. To see the exact number of clients associated with the selected AP at a particular time, move the cursor over the graph line.	To check the number of clients associated with the AP for the last 15 minutes: 1. Log in to the SCALANCE W UI. The Virtual Controller view is displayed. This is the default view. 2. On the **Access Points** tab, click the AP for which you want to monitor the client association. 3. Study the Clients graph. For example, the graph shows that six clients are associated with the AP at 12:11 hours.
Throughput	The Throughput graph shows the throughput for the selected AP for the last 15 minutes. • Outgoing traffic—Throughput for the outgoing traffic is displayed in green. It is shown above the median line. • Incoming traffic—Throughput for the incoming traffic is displayed in blue. It is shown below the median line. To see an enlarged view, click the graph. • The enlarged view provides Last, Minimum, Maximum, and Average statistics for the incoming and outgoing traffic throughput of the AP for the last 15 minutes. To see the exact throughput of the selected AP at a particular time, move the cursor over the graph line.	To check the throughput of the selected AP for the last 15 minutes: 1. Log in to the SCALANCE W UI. The Virtual Controller view is displayed. This is the default view. 2. On the **Access Points** tab, click the AP for which you want to monitor the throughput. 3. Study the Throughput graph. For example, the graph shows 44.03 Kbps incoming traffic throughput at 12:08 hours.

Mobility Trail

The **Mobility Trail** section displays the following mobility trail information for the selected client:

- **Association Time**—The time at which the selected client was associated with a particular AP. The SCALANCE W UI shows the client and AP association over the last 15 minutes.
- **Access Point**—The AP name with which the client was associated

Note

Mobility information about the client is reset each time it roams from one AP to another.

6.2.4.9 Client Match

If Client Match is enabled, the **Client Match** link provides a graphical representation of radio map view of an AP and the client distribution on an AP radio.

On clicking an access point in the **Access Points** tab and the **Client Match** link, a stations map view is displayed and a graph is drawn with real-time data points for the AP radio. If the AP supports dual-band, you can toggle between 2.4 GHz and 5 GHz links in the Client Match graph area to view the data. When you hover the mouse on the graph, details such as RSSI, Client Match status, and the client distribution on channels are displayed.

On clicking a client in the **Clients** tab and the **Client Match** link, a graph is drawn with real-time data points for an AP radio map. When you hover the mouse on the graph, details such as RSSI, channel utilization details, and client count on each channel are displayed.

6.2.4.10 AppRF

The **AppRF** link displays the application traffic summary for APs and client devices. The **AppRF** link in the activity panel is displayed only if **AppRF visibility** is enabled in the **System** window. For more information on application visibility and AppRF charts, see Application Visibility (Page 335).

6.2.4.11 Spectrum

The spectrum link (in **Access Point** view) displays the spectrum data that is collected by a hybrid AP or by an AP that has enabled spectrum monitor. The spectrum data is not reported to the virtual controller.

The spectrum link displays the following:

- **Device list**—The device list display consists of a device summary table and channel information for active non Wi-Fi devices currently seen by a spectrum monitor or a hybrid AP radio.
- **Channel Utilization and Monitoring**—This chart provides an overview of channel quality across the spectrum. It shows channel utilization information such as channel quality, availability, and utilization metrics as seen by a spectrum monitor for the 2.4 GHz and 5 GHz radio bands. The first bar for each channel represents the percentage of airtime used by non-Wi-Fi interference and Wi-Fi devices. The second bar indicates the channel quality. A higher percentage value indicates better quality.
- **Channel Details**—When you move your mouse over a channel, the channel details or the summary of the 2.4 GHz and 5 GHz channels as detected by a spectrum monitor are displayed. You can view the aggregate data for each channel seen by the spectrum monitor radio, including the maximum AP power, interference, and the SNIR. Spectrum monitors display spectrum analysis data seen on all channels in the selected band, and hybrid APs display data from the single channel that they are monitoring.

For more information on spectrum monitoring, see Spectrum Monitor (Page 425).

6.2.4.12 Alerts

Alerts are generated when a user encounters problems while accessing or connecting to a network. The alerts that are generated can be categorized as follows:

- 802.11-related association and authentication failure alerts
- 802.1X-related mode and key mismatch, server, and client time-out failure alerts
- IP-address-related failures — Static IP address or DHCP-related alerts.

The **Alerts** link displays the following types of alerts:

- Client Alerts
- Active Faults
- Fault History

Table 6- 6 Types of Alerts

Type of Alert	Description	Information Displayed
Client Alerts	The alert type, **Client Alerts**, occur when clients are connected to the SCALANCE W network.	The alert type, **Client Alert** displays the following information: • **Timestamp** — Displays the time at which the client alert was recorded. • **MAC address** — Displays the MAC address of the client that caused the alert. • **Description** — Provides a short description of the alert. • **Access Points** — Displays the IP address of the SCALANCE W • AP to which the client is connected. • **Details** — Provides complete details of the alert.
Active Faults	The **Active Faults** alerts occur in the event of a system fault.	The **Active Faults** alerts consists of the following information: • **Time** — Displays the system time when an event occurs. • **Number** — Indicates the number of sequence. • **Description** — Displays the event details.
Fault History	The **Fault History** alerts display the historic system faults.	The **Fault History** alert displays the following information: • **Time** — Displays the system time when an event occurs. • **Number** — Indicates the number of sequence. • **Cleared by** — Displays the module which cleared this fault. • **Description** — Displays the event details.

The following table displays a list of alerts that are generated in the AP network:

Table 6- 7 *Alerts List*

Description Code	Description	Details	Corrective Actions
100101	Internal error	The AP has encountered an internal error for this client.	Contact the Siemens customer support team.
100102	Unknown SSID in association request	The AP cannot allow this client to associate because the association request received contains an unknown SSID.	Identify the client and check its Wi- Fi driver and manager software.
100103	Mismatched authentication/ encryption setting	The AP cannot allow this client to associate because its authentication or encryption settings do not match AP's configuration.	Ascertain the correct authentication or encryption settings and try to associate again.
100104	Unsupported 802.11 rate	The AP cannot allow this client to associate because it does not support the 802.11 rate requested by this client.	Check the configuration on the AP to see if the desired rate can be supported.
100105	Maximum capacity reached on AP	The AP has reached maximum capacity and cannot accommodate any more clients.	Consider expanding capacity by installing additional APs or balance load by relocating APs.
100206	Invalid MAC Address	The AP cannot authenticate this client because its MAC address is not valid.	This condition may be indicative of a misbehaving client. Try to locate the client device and check its hardware and software.
100307	Client blocked due to repeated authentication failures	The AP is temporarily blocking the 802.1X authentication request from this client because the credentials provided have been rejected by the RADIUS server too many times.	Identify the client and check its 802.1X credentials.
100308	RADIUS server connection failure	The AP cannot authenticate this client using 802.1X because the RADIUS server did not respond to the authentication request. If the AP is using the internal RADIUS server, it is recommend to check the related configuration as well as the installed certificate and passphrase.	If the AP is using the internal RADIUS server, Siemens recommends checking the related configuration as well as the installed certificate and passphrase. If the AP is using an external RADIUS server, check if there are any issues with the RADIUS server and try connecting again.
100309	RADIUS server authentication failure	The AP cannot authenticate this client using 802.1X, because the RADIUS server rejected the authentication credentials (for example, password) provided by the client.	Ascertain the correct authentication credentials and log in again.
100410	Integrity check failure in encrypted message	The AP cannot receive data from this client because the integrity check of the received message (MIC) has failed. Recommend checking the encryption setting on the client and on the AP.	Check the encryption setting on the client and on the AP.

Description Code	Description	Details	Corrective Actions
100511	DHCP request timed out	This client did not receive a response to its DHCP request in time. Recommend checking the status of the DHCP server in the network.	Check the status of the DHCP server in the network.
101012	Wrong Client VLAN	VLAN mismatch between the AP and the upstream device. Upstream device can be upstream switch or RADIUS server.	

6.2.4.13 IDS

The **IDS** link displays a list of foreign APs and foreign clients that are detected in the network. It consists of the following sections:

- **Foreign Access Points Detected**—Lists the APs that are not controlled by the virtual controller.

  The following information is displayed for each foreign AP:

  - **MAC address**—Displays the MAC address of the foreign AP.
  - **Network**—Displays the name of the network to which the foreign AP is connected.
  - **Classification**—Displays the classification of the foreign AP, for example, Interfering AP or Rogue AP.
  - **Channel**—Displays the channel in which the foreign AP is operating.
  - **Type**—Displays the Wi-Fi type of the foreign AP.
  - **Last seen**—Displays the time when the foreign AP was last detected in the network.
  - **Where**—Provides information about the AP that detected the foreign AP. Click the push pin icon to view the information.
- **Foreign Clients Detected**— Lists the clients that are not controlled by the virtual controller.

  The following information is displayed for each foreign client:

  - **MAC address**—Displays the MAC address of the foreign client.
  - **Network**—Displays the name of the network to which the foreign client is connected.
  - **Classification**—Displays the classification of the foreign client: Interfering client.
  - **Channel**—Displays the channel in which the foreign client is operating.
  - **Type**—Displays the Wi-Fi type of the foreign client.
  - **Last seen**—Displays the time when the foreign client was last detected in the network.
  - **Where**—Provides information about the AP that detected the foreign client. Click the Push Pin icon to view the information.

For more information on the intrusion detection feature, see Intrusion Detection (Page 409).

6.2.4.14 AirGroup

This **AirGroup** link provides an overall view of your AirGroup configuration. Click each parameter to view or edit the settings.

- **MAC**—Displays the MAC address of the AirGroup servers.
- **IP**—Displays the IP address of the AirGroup servers.
- **Host Name**—Displays the machine name or host name of the AirGroup servers.
- **Service**— Displays the type of services such as AirPlay or AirPrint.
- **VLAN**—Displays VLAN details of the AirGroup servers.
- **Wired/Wireless**—Displays if the AirGroup server is connected through a wired or wireless interface.
- **Role**—Displays the user role if the server is connected through 802.1X authentication. If the server is connected through phase-shift keying or open authentication, this parameter is blank.
- **Group**—Displays the group.
- **CPPM**—By clicking this, you get details of the registered rules in ClearPass Policy Manager for this server.
- **MDNS Cache**—By clicking this, you receive MDNS record details of a particular server.

6.2.4.15 Configuration

The **Configuration** link provides an overall view of your virtual controller, APs, and WLAN SSID configuration.

6.2.4.16 Airwave Setup

AirWave is a solution for managing rapidly changing wireless networks. When enabled, AirWave allows you to manage the SCALANCE W network. For more information on AirWave, see Managing an AP from AirWave (Page 385).

The AirWave status is displayed below the virtual controller section of the SCALANCE W main window. If the AirWave status is **Not Set Up**, click the **Set Up Now** link to configure AirWave. The **System > Admin** window is displayed.

6.2.4.17 Pause/Resume

The **Pause/Resume** link is located on the SCALANCE W main window.

The SCALANCE W UI is automatically refreshed every 15 seconds by default. Click the **Pause** link to pause the automatic refreshing of the SCALANCE W UI after every 15 seconds. When the automatic refreshing is paused, the **Pause** link changes to **Resume**. Click the **Resume** link to resume automatic refreshing.

Automatic refreshing allows you to get the latest information about the network and network elements. You can use the **Pause** link when you want to analyze or monitor the network or a network element, and therefore do not want the UI to refresh.

6.2.5 Views

Depending on the link or tab that is clicked, SCALANCE W displays information about the virtual controller, Wi-Fi networks, APs, or the clients in the Info section. The views on the SCALANCE W main window are classified as follows:

- **Virtual Controller** view—The virtual controller view is the default view. This view allows you to monitor the SCALANCE W network.
- The following SCALANCE W UI elements are available in this view:
  - **Tabs**—Networks, Access Points, and Clients. For detailed information on the tabs, see Tabs (Page 47).
  - **Links**—Monitoring, Client Alerts, and IDS. The Spectrum link is visible if you have configured the AP as a spectrum monitor. These links allow you to monitor the SCALANCE W network. For more information on these links, see Monitoring (Page 56), IDS (Page 70), Alerts (Page 68) and Spectrum Monitor (Page 67).
- **Network** view—The Network view provides information that is necessary to monitor a selected wireless network. All Wi-Fi networks in the SCALANCE W network are listed in the **Network** tab. Click the name of the network that you want to monitor.
- SCALANCE W Access Point view—The SCALANCE W Access Point view provides information that is necessary to monitor a selected AP. All APs in the SCALANCE W network are listed in the **Access Points** tab. Click the name of the AP that you want to monitor.
- **Client** view—The Client view provides information that is necessary to monitor a selected client. In the Client view, all the clients in the SCALANCE W network are listed in the **Clients** tab. Click the IP address of the client that you want to monitor.

For more information on the graphs and the views, see Monitoring (Page 56).

Initial Configuration Tasks 7

7.1 Configuring System Parameters

This section describes how to configure the system parameters of an AP. To configure system parameters:

1. Select **System**.

Table 7- 1 System Parameters

Parameter	Description	CLI Configuration
Name	Name of the AP.	`(AP)# name <name>`
System location	Physical location of the AP.	`(AP)# (config)# sysloca- tion<location-name>`

Virtual Controller IP	This parameter allows you to specify a single static
	IP address that can be used to manage a multi- AP SCALANCE W network. This IP address is automatically provisioned on a shadow interface on the AP that takes the role of a virtual controller. When an AP becomes a virtual controller, it sends three ARP messages with the static IP address and its MAC address to update the network ARP cache.
		`(AP)(config)`
		`# virtual- controller-ip <IP- address>`

Allow IPv6 Management	Select the check box to enable IPv6 configuration	

Virtual Controller IPv6	This parameter is used to configure the IPv6 address.	`(AP)(config)`
		`# virtual- controller- ipv6 <ipv6 address>`

Uplink switch native VLAN	This parameter notifies the AP about the native-VLAN of the upstream switch to which the AP is connected. The parameter stops the AP from sending out tagged frames to clients connected with the SSID that has the same VLAN as the native VLAN of the upstream switch, to which the AP is connected. By default, the AP considers the uplink switch native VLAN value as 1.	`(AP)(config)`
		`# enet-vlan <vlan- ID>`

Parameter	Description	CLI Configuration

Dynamic Proxy	This parameter allows you to enable or disable the dynamic proxy for RADIUS and TACACS servers.
	• Dynamic RADIUS proxy—When dynamic RADIUS proxy is enabled, the virtual controller network will use the IP address of the virtual controller for communication with external RADIUS servers. Ensure that you set the virtual controller IP address as a NAS client in the RADIUS server if Dynamic RADIUS proxy is enabled.
	• Dynamic TACACS proxy—When enabled, the virtual controller network will use the IP address of the virtual controller for communication with external TACACS servers. The IP address is chosen based on one of the following rules:
	– If a VPN tunnel exists between the AP and the TACACS server, then the IP address of the tunnel interface will be used.
	– If a virtual controller IP address is configured, the same will be used by the virtual controller network to communicate with the external TACACS server.
	– If a virtual controller IP is not configured, then the IP address of the bridge interface is used.
	NOTE: When dynamic-tacacs-proxy is enabled on the AP, the TACACS server cannot identify the slave AP that generates the TACACS traffic as the source IP address is changed.
		To enable dynamic RADIUS proxy:
		`(AP)(config)`
		`# dynamic-radius- proxy`
		To enable TACACS proxy:
		`(AP)(config)`
		`# dynamic-tacacs- proxy`

MAS Integration	Select **Enabled**/**Disabled** from the **MAS integration** drop-down list to enable or disable the LLDP protocol for Mobility Access Switch integration. With this protocol, APs can instruct the Mobility Access Switch to turn off ports where rogue access points are connected, as well as take actions such as increasing PoE priority and automatically configuring VLANs on ports where SCALANCE W access points are connected.	`(AP)(config)`
		`# mas-integration`

Parameter	**Description**	**CLI Configuration**

NTP Server	This parameter allows you to configure NTP server. To facilitate communication between various elements in a network, time synchronization between the elements and across the network is critical. Time synchronization allows you to:
	• Trace and track security gaps, monitor network usage, and troubleshoot network issues.
	• Validate certificates.
	• Map an event on one network element to a corresponding event on another.
	• Maintain accurate time for billing services and similar tasks.
	NTP helps obtain the precise time from a server and regulate the local time in each network element. Connectivity to a valid NTP server is required to synchronize the AP clock to set the correct time. If NTP server is not configured in the AP network, an AP reboot may lead to variation in time data.
	By default, the AP tries to connect to **pool.ntp.org** to synchronize time. The NTP server can also be provisioned through the DHCP option 42. If the NTP server is configured, it takes precedence over the DHCP option 42 provisioned value. The NTP server provisioned through the DHCP option 42 is used if no server is configured. The default server **pool.ntp.org** is used if no NTP server is configured or provisioned through DHCP option 42.
	NOTE: To facilitate ZTP using the AMP, you must configure the firewall and wired infrastructure to either allow the NTP traffic to pool.ntp.org, or provide alternative NTP servers under DHCP options.
		To configure an NTP server:
		`(AP)(config)`
		`# ntp-server <name>`

Timezone	Timezone in which the AP must operate. You can also enable DST on APs if the time zone you selected supports the DST. When enabled, the DST ensures that the APs reflect the seasonal time changes in the region they serve.	To configure timezone:
		`(AP)(config)`
		`# clock timezone <name> <hour-offset><minute-offset>`
		To configure DST:
		`AP)(config)# clock summer-time <timezone> recurring <start-week> <start- day> <start-month>`
		`<start-hour> <end-week> <end-day> <end-month> <end-hour>`

Preferred Band	The preferred band for the AP.
	NOTE: Reboot the AP after modifying the radio profile for changes to take effect.
		`(AP)(config)`
		`# rf-band <band>`

AppRF Visibility	Select one of the following options from the **AppRF visibility** drop-down list.
	• **App**—Displays only inbuilt DPI data.
	• **WebCC**—Displays the DPI data hosted on the cloud.
	• **All**—Displays both App and WebCC DPI data.
	• **None**—Does not display any AppRF content.
		`(AP)(config)`
		`# dpi`

Parameter	Description	CLI Configuration

URL Visibility	Select **Enabled** or **Disabled** from the **URL visibility** drop-down list.	`(AP)(config)`
		`# url-visibility`

Cluster security	Select **Enabled** to ensure that the control plane messages between access points are secured. This option is disabled by default.
	NOTE: The Cluster security setting can be enabled only if the default NTP server or a static NTP server is reachable.
		`(AP)(config)`
		`# cluster-security`

Virtual Controller network settings	If the virtual controller IP address is in the same subnet as the AP, ensure that you select **Custom** from the **Virtual Controller network settings** drop-down list and configure the following details:
	• **Virtual Controller Netmask**—Enter subnet mask details.
	• **Virtual Controller Gateway**—Enter a gateway address.
	• **Virtual Controller DNS**—If the DNS IP address is configured for a master AP, the DNS IP settings are synchronized for all APs in an AP cluster.
	– If the DNS IP address is configured for an AP as part of the per AP setting (**Edit Access Point > General**), it takes precedence over the virtual controller DNS IP address defined in the **System > General** window.
	– If the APs are not explicitly assigned a DNS IP address, the DNS IP address defined in **System > General** takes precedence.
	– If the DNS IP address is not defined for APs or virtual controller, the DNS address dynamically assigned from the DHCP server is used.
	• **Virtual Controller VLAN**—Ensure that the VLAN defined for the virtual controller is not the same as the native VLAN of the AP.
	virtual controller VLAN, gateway, and subnet mask details.
		`(AP)(config)`
		`# virtual- controller-dnsip`
		`<addr>`
		`(AP)(config)`
		`# virtual- controller-vlan`
		`<vcvlan> <vcmask>`
		`<vcgw>`

Auto join mode	The Auto-Join feature allows APs to automatically discover the virtual controller and join the network. The Auto-Join feature is enabled by default. If the Auto-Join feature is disabled, a link is displayed in the **Access Points** tab indicating that there are new APs discovered in the network. Click this link if you want to add these APs to the network. When Auto-Join feature is disabled, the inactive APs are displayed in red.	To disable auto-join mode:
		`(AP)(config)`
		`# no allow-new-aps`
		To enable auto-join mode:
		`(AP)(config)`
		`# allow-new-aps`

Terminal access	When terminal access is enabled, you can access the AP CLI through SSH.
	The terminal access is enabled by default.
		`(AP)(config)`
		`# terminal-access`

Console access	When enabled, you can access the AP through the console port.	`(AP)(config)`
		`# console`

Telnet server	To start a Telnet session with the AP CLI, enable access to the Telnet server.	`(AP)(config)`
		`# telnet-server`

Parameter	Description	CLI Configuration

LED display	LED display status of the AP. To enable or disable LED display for all APs in a cluster, select **Enabled** or **Disabled**, respectively.
	NOTE: The LEDs are always enabled during the AP reboot.
		`(AP)(config)`
		`# led-off`

Extended SSID	**Extended SSID** is enabled by default in the factory
	default settings of APs. This disables mesh in the factory default settings.
	APs support up to 14 SSIDs when Extended SSID is disabled and up to 16 SSIDs with Extended SSID enabled.
		`(AP)(config)`
		`# extended-ssid`

Deny inter user bridging	If you have security and traffic management policies defined in upstream devices, you can disable bridging traffic between two clients connected to the same AP on the same VLAN. When inter user bridging is denied, the clients can connect to the Internet but cannot communicate with each other, and the bridging traffic between the clients is sent to the upstream device to make the forwarding decision. This global parameter overwrites all the options available in an SSID profile. For example, when this parameter is enabled, all the SSIDs deny client-to-client bridging traffic.
	By default, the **Deny inter user bridging** parameter is disabled.
		`(AP)(config)`
		`# deny-inter-user-bridging`
		To disable inter-user bridging for the WLAN SSID clients:
		`(AP)(config)`
		`# wlan ssid-profile <ssid-profile>`
		`(AP)(SSID Profile <ssid-profile>)# deny- inter-user-bridging`

Deny local routing	If you have security and traffic management policies defined in upstream devices, you can disable routing traffic between two clients connected to the same AP on different VLANs. When local routing is disabled, the clients can connect to the Internet but cannot communicate with each other, and the routing traffic between the clients is sent to the upstream device to make the forwarding decision. This global parameter overwrites all the options in an SSID profile. For example, when this parameter is enabled, all the SSIDs deny client-to-client local traffic.
	By default, the **Deny local routing** parameter is disabled.
		`(AP)(config)`
		`# deny-local-routing`

Parameter	Description	CLI Configuration

Dynamic CPU Utilization	APs perform various functions such as wired and wireless client connectivity and traffic flows, wireless security, network management, and location tracking. If an AP is overloaded, it prioritizes the platform resources across different functions.
	Typically, the APs manage resources automatically in real time. However, under special circumstances, if dynamic resource management needs to be enforced or disabled altogether, the dynamic CPU management feature settings can be modified.
	To configure dynamic CPU management, select any of the following options from **DYNAMIC CPU UTILIZATION**.
	• **Automatic**—When selected, the CPU management is enabled or disabled automatically during runtime. This decision is based on real-time load calculations taking into account all different functions that the CPU needs to perform. This is the default and recommended option.
	• **Always Disabled in all APs**—When selected, this setting disables CPU management on all APs, typically for small networks. This setting protects user experience.
	• **Always Enabled in all APs**—When selected, the client and network management functions are protected. This setting helps in large networks with high client density.
		`(AP)(config)`
		`# dynamic-cpu-mgmt`

7.2 Changing Password

You can update your password details by using the SCALANCE W UI or the CLI.

In the SCALANCE W UI

To change the admin user password:

1. Navigate to **System > Admin**.
2. Under **Local**, provide a new password that you would like the admin users to use.
3. Click **OK**.

In the CLI

To change the admin user password:

```
(AP)(config)# mgmt-user <username> [password]
```

Hashing of Management User Password

All the management user passwords can be stored and displayed as hash instead of plain text. Hashed passwords are more secure as they cannot be converted back to plain text format.

This setting is enabled by default on factory reset APs running SCALANCE W6.5.1.0-4.3.1 onwards, and is applicable to all APs in the cluster.

Hashing of the management user password can be configured by using either the SCALANCE W UI or the CLI.

In the SCALANCE W UI

To set the management password in hash format:

1. Navigate to **System > Admin**.
2. Click the **show advanced options** link.
3. Select the **Hash Management Password** check box. This will enable the hashing of the management user password.

The check box will appear grayed out after this setting is enabled, as this setting cannot be reversed.

In the CLI

The following example enables the hashing of a management user password:

```
(AP)(config)# hash-mgmt-password
```

The following example adds a management user with read-only privilege:

```
(AP)(config)# hash-mgmt-user john password cleartext password01 usertype read-only
```

The following examples removes a management user with read-only privilege:

```
(AP)(config)# no hash-mgmt-user read-onl
```

Upgrading an AP

8

8.1 Upgrading an AP and an Image Sever

SCALANCE W supports mixed AP class deployment with all APs as part of the same virtual controller cluster.

Image Management Using AirWave

If the multiclass AP network is managed by AirWave, image upgrades can only be done through the AirWave WebUI. The AP images for different classes must be uploaded on the AMP server. When new APs joining the network need to synchronize their software with the version running on the virtual controller, and if the new AP belongs to a different class, the image file for the new AP is provided by AirWave. If AirWave does not have the appropriate image file, the new AP cannot join the network.

Note

The virtual controller communicates with the AirWave server if AirWave is configured. If AirWave is not configured on the AP, the image is requested from the Image server.

Configuring HTTP Proxy on an AP

If your network requires a proxy server for Internet access, ensure that you configure the HTTP proxy on the AP to download the image from the cloud server. The **Username** and **Password** configuration is supported only for cloud services. After setting up the HTTP proxy settings, the AP connects to the AMP, OpenDNS, or web content classification server through a secure HTTP connection. You can also exempt certain applications from using the HTTP proxy (configured on an AP) by providing their host name or IP address under exceptions.

In the SCALANCE W UI

To configure the HTTP proxy settings:

4. Navigate to **System** > **Proxy**. The Proxy configuration window is displayed.

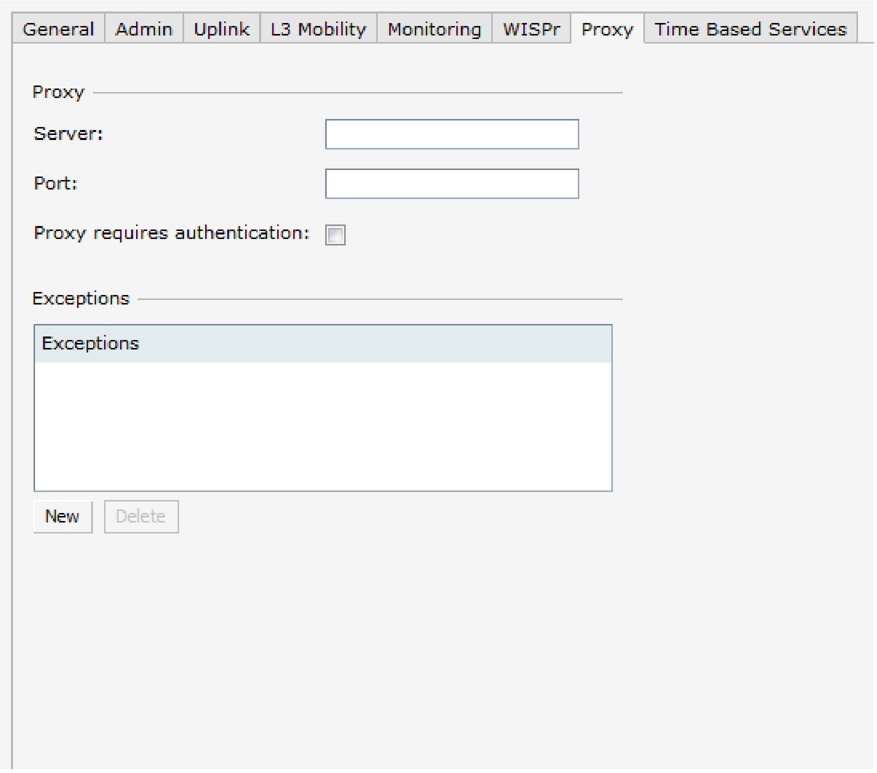


Figure 1-1 Proxy Configuration Window

5. Enter the HTTP proxy server IP address in the **Server** text box.
6. Enter the port number in the **Port** text box.
7. If you want to set an authentication username and password for the proxy server, select the **Proxy requires authentication** checkbox. Enter a username in the **Username** text box.
8. Enter a password in the **Password** text box.
9. If you do not want the HTTP proxy to be applied for a particular host, click **New** to enter that IP address or domain name of that host in the

   Exceptions section.

In the CLI

To configure the HTTP proxy settings:

```
(AP)(conf)#proxy server 192.0.2.1 8080 example1 user123

(AP)(conf)# proxy exception 192.0.2.2

(AP)(conf)# end

(AP)(conf)# commit apply
```

8.2 Upgrading an AP Image Manually

In the SCALANCE W UI:

The following procedure describes how to manually check for a new firmware image version and obtain an image file:

10. Navigate to **Maintenance** > **Firmware**.
11. Under **Manual** section, perform the following steps:
12. Select the Image file option.
13. Select the **Image URL** option. Select this option to obtain an image file from a HTTP, TFTP, or FTP URL.
    – HTTP - http://<IP-address>/<image-file>. For example, http://<IP-address>/Siemens_Hercules_8.3.0.1_xxxx
    – TFTP - tftp://<IP-address>/<image-file>. For example, tftp://<IP-address>/Siemens_Hercules_8.3.0.1_xxxx
    – FTP - ftp://<IP-address>/<image-file>. For example, ftp://<IP-address>/Siemens_Hercules_8.3.0.1_xxxx
    – FTP - ftp://<user name:password>@<IP-address>/<image-file>. For example, ftp://<aruba:123456>@<IP-addressSiemens_Hercules_8.3.0.1_xxxx

    Note

    The FTP server supporsts both **anonymous** and **username:password** login methods.

    Note

    Multiclass APs can be upgraded only in the URL format, not in the local image file format.

14. Clear the **Reboot all APs after upgrade** check box if required. This check box is selected by default to allow the APs to reboot automatically after a successful upgrade. To reboot the AP at a later time, clear the **Reboot all APs after upgrade** check box.
15. Click **Upgrade Now** to upgrade the AP to the newer version

In the CLI

To upgrade an image using a HTTP, TFTP, or FTP URL:

```
(AP)# upgrade-image <ftp/tftp/http-URL>
```

To upgrade an image by using the username and password in the FTP URL :

```
(AP)# upgrade-image ftp://Aruba:123456@192.0.2.7/Siemens_Hercules_8.3.0.1_xxxx
```

To upgrade an image without rebooting the AP:

```
(AP)# upgrade-image2-no-reboot <ftp/tftp/http-URL>
```

To view the upgrade information:

```
(AP)# show upgrade info Image Upgrade Progress

----------------------

Mac IP Address AP Class Status Image Info Error Detail

--- --------- -------- ------ ---------- ------------

d8:c7:c8:c4:42:98 10.17.101.1 Hercules image-ok image file none Auto reboot :enable

Use external URL :disable
```

8.3 Impact Classify Media Flag on SCALANCE W Release

SCALANCE W 8.3.0.1

Classify media flag is no longer supported from SCALANCE W 8.3.0.1 onwards. However, media classification continues to take effect without this flag. RTP or RTCP sessions are automatically subjected to media monitoring and media classification. If the criteria for session prioritization is met, the session is automatically prioritized with the right priority and flags.

Note

Media monitoring cannot be disabled from SCALANCE W 8.3.0.1 onwards.

SCALANCE W 6.5.x.x

The release supports classify media flag as an option in the access rule. When the flag is enabled in a TCP 443 or TCP 5061 session, and a control session of the TCP port hits the datapath, media monitoring starts taking effect. The subsequent RTP or RTCP sessions undergo media monitoring. Based on various criteria, the sessions are prioritized. When the classify media flag is removed from the control sessions (TCP 5061 or TCP 443 for Skype and TCP 5060 for Jabber), media monitoring no longer happens; hence no prioritization takes place

8.4 Impact of Classify Media Flag After an Upgrade or Downgrade

Upgrade from SCALANCE W 6.5.x.x to SCALANCE W 8.3.x.x

If an ACL is running SCALANCE W 6.5.x.x and classify media flag is enabled, then the classify media flag is removed from SCALANCE W 8.3.x.x. If the APs are managed by AirWave or any other cloud server, ensure to remove classify media by creating a new template, before upgrading to SCALANCE W 8.3.0.0.

Else, the configuration is not applied to APs.

The following examples describe the impact of the classify media flag on APs running SCALANCE W 6.5.x.x and SCALANCE W 8.3.x.x:

In SCALANCE W 6.5.x.x

```
(AP)(config)# wlan access-rule ms4b

(AP)(Access Rule "ms4b")# index 2

(AP)(Access Rule "ms4b")# rule any any match tcp 5061 5061 permit classify-media
```

In SCALANCE W 8.3.x.x

```
(AP)(config)# wlan access-rule ms4b

(AP)(Access Rule "ms4b")# index 2

(AP)(Access Rule "ms4b")# rule any any match tcp 5061 5061 permit
```

Downgrade from SCALANCE W 8.3.x.x to SCALANCE W 6.5.x.x

Because SCALANCE W 8.3.x.x does not support the classify media flag, if you downgrade from SCALANCE W 8.3.x.x to an earlier release, the media classification flag must be added manually to every control session, in order to enable media classification for a pecific application.

VLAN Configuration 9

VLAN configuration is required for networks with more devices and broadcast traffic on a WLAN SSID or wired profile. Based on the network type and its requirements, you can configure the VLANs for a WLAN SSID or wired port profile.

For more information on VLAN configuration for a WLAN SSID and wired port profile, see Configuring VLAN Settings for a WLAN SSID Profile (Page 101) and Configuring VLAN for a Wired Profile (Page 127) , respectively.

9.1 VLAN Pooling

In a single AP cluster, a large number of clients can be assigned to the same VLAN. Using the same VLAN for multiple clients can lead to a high level of broadcasts in the same subnet. To manage the broadcast traffic, you can partition the network into different subnets and use L3-mobility between those subnets when clients roam. However, if a large number of clients need to be in the same subnet, you can configure VLAN pooling, in which each client is randomly assigned a VLAN from a pool of VLANs on the same SSID. Thus, VLAN pooling allows automatic partitioning of a single broadcast domain of clients into multiple VLANs.

9.2 Uplink VLAN Monitoring and Detection on Upstream Devices

If a client connects to an SSID or a wired interface with VLAN that is not allowed on the upstream device, the client will not be assigned an IP address and thus cannot connect to the Internet. In such a scenario, the SCALANCE W UI displays an alert. To prevent this issue from recurring, ensure that there is no mismatch in the VLAN configuration.

IPv6 Support 10

10.1 IPv6 Notation

IPv6 is the latest version of Internet Protocol (IP) that is suitable for large-scale IP networks. IPv6 supports a 128-bit address to allow 2128, or approximately 3.4×1038 addresses while IPv4 supports only 232 addresses.

The IP address of the IPv6 host is always represented as eight groups of four hexadecimal digits separated by colons. For example `2001:0db8:0a0b:12f0:0000:0000:0000:0001`. However, the IPv6 notation can be abbreviated to compress one or more groups of zeroes or to compress leading or trailing zeroes.

The following examples show various representations of the address

```
2001:0db8:0a0b:12f0:0000:0000:0000:0001
```

- Valid format—`2001:db8:a0b:12f0::0:0:1`
- Invalid format—`2001:db8:a0b:12f0::::0:1`. The `"::"` sign appears only once in an address.
- With leading zeros omitted—`2001:db8:a0b:12f0:0:0:0:1`
- Switching from upper to lower case—`2001:DB8:A0B:12f0:0:0:0:1`

IPv6 uses a "/" notation which describes the number of bits in netmask as in IPv4.

```
2001:db8::1/128 - Single Host
```

```
2001:db8::/64 - Network
```

10.2 Enabling IPv6 Support for AP Configuration

APs support IPv6 address mode for the following features:

- Supported IP modes
- Configuring IPv6 Address for an AP
- RADIUS over IPv6
- SNMP Over IPv6
- SNTP Over IPv6

Supported IP modes

SCALANCE W supports two modes of IP address configuration:

- V4-only—The AP would allow IPv6 clients to pass-through just like the previous SCALANCE W release.
- V4-prefer—Supports both IPv4 and IPv6 addresses. If the AP gets both IPv4 and IPv6 responses for a DNS query, then the AP would prefer the IPv4 DNS address instead of the IPv6 DNS address.

When the IP mode is set to v4-prefer mode, the AP derives a link local IPv6 address and attempts to acquire a routable IPv6 address by monitoring RA packets. AP assigns itself to both SLAAC and DHCPv6 client address. APs also support IPv6 DNS server addresses and use these for DNS resolution.

In the CLI:

To enable IPv4 mode or dual stack mode:

```
(AP)(config)# ip-mode {v4-only|v4-prefer}
```

Configuring IPv6 Address for an AP

You can enable the IPv6 mode on the AP and also configure a virtual controller IPv6 address using the SCALANCE W UI or the CLI:

In the SCALANCE W UI:

To enable IPv6 and configure virtual controller IPv6 address:

1. Go to the **System** link, directly above the Search bar in the SCALANCE W UI.
2. Under **General**, select the **Allow IPv6 Management** check box.
3. Enter the IP address in the **Virtual Controller IPv6** address text box.
4. Click **OK**.

In the CLI:

To configure an IPv6 address for an AP:

```
(AP)(config)# virtual-controller-ipv6 <ipv6 address> (
```

Note

The virtual controller IPv6 address can be configured only after enabling the v4-prefer mode in the SCALANCE W CLI.

RADIUS over IPv6

With the address mode set to v4-prefer, the AP supports an IPv6 IP address for the RADIUS server. The authentication server configuration can also include the NAS IPv6 address (that defaults to the routable IPv6 address when not configured). RADIUS server supports hostname configuration using IP or FQDN configurations also.

To configure an IPv6 address for the RADIUS server:

```
(AP)(config)# wlan auth-server radiusIPv6

(AP)(Auth Server "radiusIPv6")# ip <host>

(AP)(Auth Server "radiusIPv6")# nas-ip <ip_ipv6>
```

SNMP Over IPv6

In this release, you can configure a community string to authenticate messages sent between the virtual controller and the SNMP agent, where the IPv6 address will be used as the virtual controller address. For more information on configuring SNMP parameters, see Configuring SNMP (Page 439).

To view the SNMP configuration:

```
AP)# show running-config|include snmp

snmp-server community e96a5ff136b5f481b6b55af75d7735c16ee1f61ba082d7ee

snmp-server host 2001:470:20::121 version 2c siemens-string inform
```

SNTP Over IPv6

To view the SNTP configuration:

```
(AP)# show running-config|include ntp ntp-server 2001:470:20::121
```

10.3 Firewall Support for IPv6

For a given client, a single ACL is used to firewall both IPv4 and IPv6 rules. A rule **any any match any any any permit** in the access rule configuration will expand to two different ACL entries:

- any any any P6
- any any any P4

Similarly, if any IPv6 specific rule is added. For example, if any DHCPv6 or FTPv6 rule is added, the ACE would be expanded as follows:

any 2002::/64 17 0-65535 546-547 6—*destined to network 2002::/64 DHCPv6 is denied*.

any 2001::10/128 6 0-65535 20-21 6—*destined to host 2001::10 FTP is denied*.

For all ACLs the AP will have an implicit IPv4 and IPv6 **allow all** acl rule.

10.4 Debugging Commands

Use the following commands to troubleshoot issues pertaining to IPv6 configuration:

- `show ipv6 interface brief` and `show ipv6 interface details`— displays the configured IPv6 address, and any duplicate addresses.
- `show ipv6 route`—displays the IPv6 routing information.
- `show datapath ipv6 session`—displays IPv6 sessions.
- `show datapath ipv6 user`—displays IPv6 client details.
- `show clients` and `show clients debug`—displays the details about AP clients.

Wireless Network Profiles 11

11.1 Configuring Wireless Network Profiles

During start up, a wireless client searches for radio signals or beacon frames that originate from the nearest AP. After locating the AP, the following transactions take place between the client and the AP:

1. Authentication—The AP communicates with a RADIUS server to validate or authenticate the client.
2. Connection—After successful authentication, the client establishes a connection with the AP.

Network Types

SCALANCE W wireless networks are categorized as:

- **Employee network**—An Employee network is a classic Wi-Fi network. This network type is used by the employees in an organization and it supports passphrase-based or 802.1X-based authentication methods. Employees can access the protected data of an enterprise through the employee network after successful authentication. The employee network is selected by default during a network profile configuration.
- **Voice network**—This Voice network type allows you to configure a network profile for devices that provide only voice services—for example, devices such as handsets or applications that require voice traffic prioritization.
- **Guest network**—The Guest wireless network is created for guests, visitors, contractors, and any non- employee users who use the enterprise Wi-Fi network. The virtual controller assigns the IP address for the guest clients. Captive portal or passphrase-based authentication methods can be set for this wireless network. Typically, a guest network is an unencrypted network. However, you can specify the encryption settings when configuring a guest network.

Note

When a client is associated to the Voice network, all data traffic is marked and placed into the high-priority queue in the QoS.

To configure a new wireless network profile, complete the following procedures:

1. Configuring WLAN Settings (Page 96)
2. Configuring VLAN Settings (Page 101)
3. Configuring Security Settings (Page 104)
4. Configuring Access Rules for a Network (Page 111)

11.1.1 Configuring WLAN Settings for an SSID Profile

You can configure WLAN settings using the SCALANCE W UI or the CLI.

In the SCALANCE W UI

To configure WLAN settings:

1. On the **Network** tab of the SCALANCE W main window, click the **New** link. The **New WLAN** window is displayed.
2. Enter a name that uniquely identifies a wireless network in the **Name (SSID)** text box.

Note

The SSID name must be unique and may contain any special character except for ' and **".**

3. Based on the type of network profile, select any of the following options under **Primary usage**:
   - **Employee**
   - **Voice**
   - **Guest**
4. Click the **Show advanced options** link. The advanced options for configuration are displayed. Specify the following parameters as require:

Parameter	Description
Broadcast filtering	Select any of the following values: • **All**—When set to **All**, the AP drops all broadcast and multicast frames except DHCP and ARP, IGMP group queries, and IPv6 neighbor discovery protocols. • **ARP**—When set to **ARP**, the AP drops all broadcast and multicast frames except DHCP and ARP, IGMP group queries, and IPv6 neighbor discovery protocols; additionally, it converts ARP requests to unicast and send frames directly to the associated client. The broadcast filtering option is set to **ARP** by default when an SSID profile is created. • **Unicast-ARP-Only**—When set to **Unicast-ARP-Only**, the AP allows all broadcast and multicast frames as it is, however the ARP requests are converted to unicast frames and sends them to the associated clients. • **Disabled**—When set to **Disabled**, all broadcast and multicast traffic is forwarded to the wireless interfaces.

Parameter	Description
Multicast transmission optimization	Select **Enabled** if you want the AP to select the optimal rate for sending broadcast and multicast frames based on the lowest of unicast rates across all associated clients. When this option is enabled, multicast traffic can be sent at up to 24 Mbps. The default rate of sending frames for 2.4 GHz is 1 Mbps and that for 5 GHz is 6 Mbps. This option is disabled by default.
Dynamic multicast optimization	Select **Enabled** to allow the AP to convert multicast streams into unicast streams over the wireless link. Enabling Dynamic Multicast Optimization (DMO) enhances the quality and reliability of streaming video, while preserving the bandwidth available to the non-video clients. **NOTE:** When you enable DMO on multicast SSID profiles, ensure that the DMO feature is enabled on all SSIDs configured in the same VLAN.
DMO channel utilization threshold	Specify a value to set a threshold for DMO channel utilization. With DMO, the AP converts multicast streams into unicast streams as long as the channel utilization does not exceed this threshold. The default value is 90% and the maximum threshold value is 100%. When the threshold is reached or exceeds the maximum value, the AP sends multicast traffic over the wireless link.
Transmit Rates	Specify the following parameters: • **2.4 GHz**—If the 2.4 GHz band is configured on the AP, specify the minimum and maximum transmission rate. The default value for minimum transmission rate is 1 Mbps and maximum transmission rate is 54 Mbps. • **5 GHz**—If the 5 GHz band is configured on the AP, specify the minimum and maximum transmission rate. The default value for minimum transmission rate is 6 Mbps and maximum transmission rate is 54 Mbps.
Band	Select a value to specify the band at which the network transmits radio signals. You can set the band to **2.4 GHz**, **5 GHz**, or **All**. The **All** option is selected by default.
DTIM interval	The **DTIM interval** indicates the delivery traffic indication message (DTIM) period in beacons, which can be configured for every WLAN SSID profile. The DTIM interval determines how often the AP should deliver the buffered broadcast and multicast frames to associated clients in the power save mode. The default value is 1, which means the client checks for buffered data on the AP at every beacon. You can also configure a higher DTIM value for power saving.
Min RSSI probe request	Sets a minimum received signal strength indication (RSSI) threshold for probe requests.
Min RSSI auth request	Sets a minimum RSSI threshold for authentication requests.
Very high throughput	Enables the VHT function on AP devices that support VHT. For 802.11acAPs, the VHT function is enabled by default. However, you can disable the VHT function if you want the 802.11ac APs to function as 802.11n APs. If VHT is configured or disabled on an SSID, the changes will apply only to the SSID on which it is enabled or disabled.
Zone	Specify the zone for the SSID. When the zone is defined in SSID profile and if the same zone is defined on an AP, the SSID is created on that AP. For more information on configuring zone details, see Configuring Zone Settings on an AP (Page **Fehler! Textmarke nicht definiert.**).

Parameter	Description
Time Range	Click **Edit**, select a Time Range Profile from the list and specify if the profile must be enabled or disabled for the SSID, and then click **OK**.
Bandwidth Limits	Select the required options under **Bandwidth Limits**: • **Airtime**—Select this check box to specify an aggregate amount of airtime that all clients in this network can use for sending and receiving data. Specify the airtime percentage. • **Each radio**—Select this check box to specify an aggregate amount of throughput that each radio is allowed to provide for the connected clients. • **Downstream** and **Upstream**—Specify the downstream and upstream rates within a range of 1 to 65,535 Kbps for the SSID users. If the assignment is specific for each user, select the **Per user** check box.
Wi-Fi Multimedia (WMM) traffic management	Configure the following options for WMM traffic management. WMM supports voice, video, best effort, and background access categories. To allocate bandwidth for the following types of traffic, specify a percentage value under **Share**. To configure Differentiated Service Code Point (DSCP) mapping, specify a value under **DSCP Mapping**. • **Background WMM**—For background traffic such as file downloads or print jobs. • **Best effort WMM**—For best effort traffic such as traffic from legacy devices or traffic from applications or devices that do not support QoS. • **Video WMM**—For video traffic generated from video streaming. • **Voice WMM**—For voice traffic generated from the incoming and outgoing voice communication. For more information on WMM traffic and DSCP mapping, see Wi-Fi Multimedia Traffic Management (Page 343).
	For voice traffic and Spectra link Voice Prioritization, configure the following parameters: • **Traffic Specification (TSPEC)**—To prioritize time-sensitive traffic such as voice traffic initiated by the client, select the **Traffic Specification (TSPEC)** check box. • **TSPEC Bandwidth**—To reserve bandwidth, set the TPSEC bandwidth to the desired value within the range of 200–600,000 Kbps. The default value is 2000 Kbps. • **Spectra link Voice Protocol (SVP)**—Select the check box to prioritize voice traffic for SVP handsets.

Parameter	Description
Content filtering	Select **Enabled** to route all DNS requests for the non-corporate domains to OpenDNS on this network.
Inactivity timeout	Specify an interval for session timeout in seconds, minutes, or hours. If a client session is inactive for the specified duration, the session expires and the user is required to log in again. You can specify a value within the range of 60–86,400 seconds (24 hours) for a client session. The default value is 1000 seconds.
Deauth Inactive Clients	Select **Enabled** to allow the AP to send a deauthentication frame to the inactive client and clear client entry.
SSID	Select the **Hide** check box if you do not want the SSID (network name) to be visible to users. Select the **Disable** check box if you want to disable the SSID. On selecting this, the SSID will be disabled, but will not be removed from the network. By default, all SSIDs are enabled.
Out of service (OOS)	Enable or disable the SSID based on the following OOS states of the AP: • VPN down • Uplink down • Internet down • Primary uplink down The network will be out of service when selected event occurs and the SSID is enabled or disabled as per the configuration settings applied. For example, if you select the VPN down option from the drop-down list and set the status to enabled, the SSID is enabled when the VPN connection is down and is disabled when the VPN connection is restored.
OOS time (global)	Configure a hold time interval in seconds within a range of 30–300 seconds, after which the out-of-service operation is triggered. For example, if the VPN is down and the configured hold time is 45 seconds, the effect of this out-of-service state impacts the SSID availability after 45 seconds.
Max clients threshold	Specify the maximum number of clients that can be configured for each BSSID on a WLAN. You can specify a value within the range of 0–255. The default value is 64. **NOTE:** When the **Max clients threshold** parameter is configured, the value is applicable to every AP in a cluster.
SSID Encoding	To encode the SSID, select UTF-8. By default, the SSIDs are not encoded. **NOTE:** When a wireless SSID is encoded, by default, UTF-8 is added to the access rules that are active on the SSID. However this does not apply for the access rules that are configured separately for the SSID. UTF-8 is not supported for wired networks.
Deny inter user bridging	When enabled, the bridging traffic between two clients that are connected to the same SSID on the same VLAN is disabled. The clients can connect to the Internet, but cannot communicate with each other, and the bridging traffic between the clients is sent to the upstream device to make the forwarding decision.
ESSID	Enter the ESSID. If the value defined for ESSID value is not the same as the profile name, the SSIDs can be searched based on the ESSID value and not by its profile name.

5. Click **Next** to configure VLAN settings.

   For more information, see Configuring VLAN Settings for a WLAN SSID Profile (Page 101).

In the CLI

To configure WLAN settings for an SSID profile:

```
(AP)(config)# wlan ssid-profile <name>
(AP)(SSID Profile <name>)# essid <ESSID-name>
(AP)(SSID Profile <name>)# type {<Employee>|<Voice>|<Guest>}
(AP)(SSID Profile <name>)# broadcast-filter {All|ARP|Unicast-ARP-Only|Disabled}
(AP)(SSID Profile <name>)# dtim-period <number-of-beacons>
(AP)(SSID Profile <name>)# multicast-rate-optimization
(AP)(SSID Profile <name>)# dynamic-multicast-optimization
(AP)(SSID Profile <name>)# dmo-channel-utilization-threshold
(AP)(SSID Profile <name>)# a-max-tx-rate <rate>
(AP)(SSID Profile <name>)# a-min-tx-rate <rate>
(AP)(SSID Profile <name>)# g-max-tx-rate <rate>
(AP)(SSID Profile <name>)# g-min-tx-rate <rate>
(AP)(SSID Profile <name>)# zone <zone>
(AP)(SSID Profile <name>)# bandwidth-limit  <limit>
(AP)(SSID Profile <name>)# per-user-bandwidth-limit <limit>
(AP)(SSID Profile <name>)# air-time-limit <limit>
(AP)(SSID Profile <name>)# wmm-background-dscp <dscp>
(AP)(SSID Profile <name>)# wmm-background-share <share>
(AP)(SSID Profile <name>)# wmm-best-effort-dscp <dscp>
(AP)(SSID Profile <name>)# wmm-best-effort-share <share>
(AP)(SSID Profile <name>)# wmm-video-dscp <dscp>
(AP)(SSID Profile <name>)# wmm-video-share <share>
(AP)(SSID Profile <name>)# wmm-voice-dscp <dscp>
(AP)(SSID Profile <name>)# wmm-voice-share <share>
(AP)(SSID Profile <name>)# rf-band {<2.4>|<5>|<all>}
(AP)(SSID Profile <name>)# content-filtering
(AP)(SSID Profile <name>)# mfp-capable
(AP)(SSID Profile <name>)# mfp-required
(AP)(SSID Profile <name>)# hide-ssid
(AP)(SSID Profile <name>)# out-of-service <def> <name>
(AP)(SSID Profile <name>)# time-range <profile name> {<Enable>|<Disable>}
(AP)(SSID Profile <name>)# inactivity-timeout <interval>
(AP)(SSID Profile <name>)# local-probe-req-thresh <threshold>
(AP)(SSID Profile <name>)# max-clients-threshold <number-of-clients>
```

Temporal Diversity and Maximum Retries using CLI

When clients are not responding to 802.11 packets with the **temporal-diversity** parameter disabled, which is the default setting, APs can attempt only hardware retries. But if this parameter is enabled when the clients are not responding to 802.11 packets, APs can perform two hardware retries. When the hardware retry attempts fail, APs can perform software retries.

The **max-retries** parameter indicates the maximum number of attempts the AP performs when clients are not responding to 802.11 packets. By default, the AP attempts a maximum of eight retries when clients are not responding to 802.11 packets.

The following example shows the configuration of **temporal-diversity** and **max-retries** in a WLAN SSID profile:

```
(AP) (config) # wlan ssid-profile Name

(AP) (SSID Profile "Name") # temporal-diversity

(AP) (SSID Profile "Name") # max-retries 3
```

11.1.2 Configuring VLAN Settings for a WLAN SSID Profile

If you are creating a new SSID profile, complete the WLAN Settings procedure before configuring the VLAN. For more information, see Configuring WLAN Settings for an SSID Profile (Page 96).

You can configure VLAN settings for an SSID profile using the SCALANCE W UI or the CLI.

In the SCALANCE W UI

To configure VLAN settings for an SSID:

1. On the **Network** tab of the SCALANCE W main window, click the **New** link.
2. On the **VLAN** tab.
3. Select any for the following options for **Client IP assignment**.
   – **Virtual Controller assigned**—On selecting this option, the wired client obtains the IP address from the virtual controller. When this option is used, the source IP address is translated to the physical IP address of the master AP for all client traffic that goes through this interface. The virtual controller can also assign a guest VLAN to the client.
   – **Network assigned**—On selecting this option, the IP address is obtained from the network.

4. Based on the type of client IP assignment mode selected, you can configure the VLAN assignment for clients as described in the following table:

Client IP Assignment	Client VLAN Assignment
Virtual Controller assigned	If **Virtual Controller assigned** is selected for client IP assignment, the virtual controller creates a private subnet and VLAN on the AP for the wireless clients. The NAT for all client traffic that goes out of this interface is carried out at the source. This setup eliminates the need for complex VLAN and IP address management for a multisite wireless network. On selecting this option, the following client VLAN assignment options are displayed: • **Default**—When selected, the default VLAN as determined by the virtual controller is assigned for clients. • **Custom**—When selected, you can specify a custom VLAN assignment option. You can select an existing DHCP scope for client IP and VLAN assignment or you can create a new DHCP scope by selecting **New**. For more information on DHCP scopes (Page 253).
Network assigned	If **Network assigned** is selected, you can specify any of the following options for the **Client VLAN assignment**. • **Default**—On selecting this option, the client obtains the IP address in the same subnet as the APs. By default, the client VLAN is assigned to the native VLAN on the wired network. • **Static**—On selecting this option, you need to specify any one of the following: a single VLAN, a comma separated list of VLANS, or a range of VLANs for all clients on this network. Select this option for configuring VLAN pooling. • **Dynamic**—On selecting this option, you can assign the VLANs dynamically from a DHCP server. To create VLAN assignment rules, click **New** to assign the user to a VLAN. In the **New VLAN Assignment Rule** window, enter the following information: – **Attribute**—Select an attribute returned by the RADIUS server during authentication. – **Operator**—Select an operator for matching the string. – **String**—Enter the string to match . – **VLAN**—Enter the VLAN to be assigned.

5. Click **Next** to configure security settings for the Employee network. For more information, see Configuring Security Settings for a WLAN SSID Profile (Page 104).

In the CLI

To manually assign VLANs for WLAN SSID users:

```
(AP)(config)# wlan ssid-profile <name>

(AP)(SSID Profile <name>)# vlan <vlan-ID>
```

To create a new VLAN assignment rule:

```
(AP)(config)# wlan ssid-profile <name>

(AP)(SSID Profile <name>)# set-vlan <attribute> {{contains|ends-with|equals|matches-
regular-expression|not-equals|starts-with} <operand> <vlan>|value-of}
```

Enforcing DHCP

You can configure a WLAN SSID profile to enforce DHCP on AP clients. When DHCP is enforced:

- A layer-2 user entry is created when a client associates with an AP.
- The client DHCP state and IP address are tracked.
- When the client obtains an IP address from DHCP, the DHCP state changes to complete.
- If the DHCP state is complete, a layer-3 user entry is created.
- When a client roams between the APs, the DHCP state and the client IP address will be synchronized with the new AP.

By default, enforcing DHCP feature is disabled. To enforce DHCP:

```
(AP)(config)# wlan ssid-profile <name>

(AP)(SSID Profile <name>)# enforce-dhcp

(AP)(SSID Profile <name>)# end

(AP)# commit apply
```

11.1.3 Configuring Security Settings for a WLAN SSID Profile

This section describes the procedure for configuring security settings for an Employee or Voice network. For information on guest network configuration, see Captive Portal for Guest Access (Page 139).

Note

If you are creating a new SSID profile, configure the WLAN and VLAN settings before defining security settings. For more information, see Configuring WLAN Settings for an SSID Profile (Page 96) and Configuring VLAN Settings for a WLAN SSID Profile (Page 101).

Configuring Security Settings for an Employee or Voice Network

You can configure security settings for an Employee or Voice network by using the SCALANCE W UI or the CLI.

In the SCALANCE W UI

To configure security settings for an Employee or Voice network:

1. On the **Network** tab of the SCALANCE W main window, click the **New** link.
2. Click the **Security** tab.
3. Specify any of the following types of security levels by moving the slider to a desired level:
   - **Enterprise**—On selecting the enterprise security level, the authentication options applicable to the enterprise network are displayed.
   - **Personal**—On selecting the personal security level, the authentication options applicable to the personalized network are displayed.
   - **Open**—On selecting the open security level, the authentication options applicable to an open network are displayed.

   The default security setting for a network profile is **Personal**.

4. Based on the security level selected, specify the following parameters.

Parameter	**Description**	**Security Level**
Key Management	Click the **Enterprise** security level, select any of the following options from the **Key management** drop-down list: • WPA-2 Enterprise • WPA Enterprise • Both (WPA-2 & WPA) • Dynamic WEP with 802.1X—If you do not want to use a session key from the RADIUS server to derive pairwise unicast keys, set **Session Key for LEAP** to **Enabled**. This is required for old printers that use dynamic WEP through LEAP authentication. The **Session Key for LEAP** feature is set to **Disabled** by default.	Applicable to **Enterprise** and **Personal** security levels only. For the **Open** security level, no encryption settings are required.
	For the **Personal** security level, select any of the following encryption keys from the **Key management** drop-down list. • WPA-2 Personal • WPA-Personal (Both TKIP and AES Encryption) • WPA-Personal (TKIP Encryption only) • WPA-Personal (AES Encryption only) • Both (WPA-2 & WPA) • Static WEP If a WPA-2, WPA encryption, or Both (WPA-2&WPA) is selected, configure the passphrase: 1. Select a passphrase format from the **Passphrase format** drop-down list. The options available are 8–63 alphanumeric characters and 64 hexadecimal characters. 2. Enter a passphrase in the **Passphrase** text box and reconfirm. **NOTE:** The **Passphrase** may contain any special character except for **".** For **Static WEP**, specify the following parameters: 1. Select an appropriate value for **WEP key size** from the WEP key size drop-down list. You can specify 64-bit or 128-bit . 2. Select an appropriate value for Tx key from the **Tx Key** drop-down list. You can specify **1**, **2**, **3**, or **4**. 3. Enter an appropriate **WEP key** and reconfirm.	

Parameter	**Description**	**Security Level**
Termination	To terminate the EAP portion of 802.1X authentication on the AP instead of the RADIUS server, set **Termination** to **Enabled**. Enabling **Termination** can reduce network traffic to the external RADIUS server by terminating the authorization protocol on the AP. By default, for 802.1X authorization, the client conducts an EAP exchange with the RADIUS server, and the AP acts as a relay for this exchange. When **Termination** is enabled, the AP by itself acts as an authentication server and terminates the outer layers of the EAP protocol, only relaying the innermost layer to the external RADIUS server. It can also reduce the number of exchange packets between the AP and the authentication server. **NOTE:** SCALANCE W supports the configuration of primary and backup authentication servers in an EAP termination-enabled SSID. **NOTE:** If you are using LDAP for authentication, ensure that AP termination is configured to support EAP.	**Enterprise** security level
Authentication server 1 and Authentication server 2	Select any of the following options from the **Authentication server 1** drop- down list: • Select an authentication server from the list if an external server is already configured. To modify the server parameters, click **Edit**. • Select **New** to add a new server. For information on configuring external servers, see Configuring an External Server for Authentication (Page 188). • To use an internal server, select **Internal server** and add the clients that are required to authenticate with the internal RADIUS server. Click the **Users** link to add the users. For information on adding a user, see Managing AP Users. If an external server is selected, you can also configure another authentication server.	**Enterprise**, **Personal**, and **Open** security levels.
Load balancing	Set this to **Enabled** if you are using two RADIUS authentication servers, so that the load across the two RADIUS servers is balanced. For more information on the dynamic load balancing mechanism, see Dynamic Load Balancing between Two Authentication Servers (Page 187).	**Enterprise**, **Personal**, and **Open** security levels.

Parameter	Description	Security Level
Reauth interval	Specify a value for **Reauth interval**. When set to a value greater than zero, APs periodically reauthenticate all associated and authenticated clients. The following list provides descriptions for three reauthentication interval configuration scenarios: • When Reauth interval is configured on an SSID performing L2 authentication (MAC or 802.1X authentication)—When reauthentication fails, the clients are disconnected. If the SSID is performing only MAC authentication and has a pre-authentication role assigned to the client, the client will get a post-authentication role only after a successful reauthentication. If reauthentication fails, the client retains the pre- authentication role. • When Reauth interval is configured on an SSID performing both L2 and L3 authentication (MAC with captive portal authentication)—When reauthentication succeeds, the client retains the role that is already assigned. If reauthentication fails, a pre-authentication role is assigned to the client. • When Reauth interval is configured on an SSID performing only L3 authentication (captive portal authentication)—When reauthentication succeeds, a pre-authentication role is assigned to the client that is in a post-authentication role. Due to this, the clients are required to go through captive portal to regain access.	**Enterprise**, **Personal**, and **Open** security levels.
Blacklisting	To enable blacklisting of the clients with a specific number of authentication failures, select **Enabled** from the **Blacklisting** drop-down list and specify a value for **Max authentication failures**. The users who fail to authenticate the number of times specified in **Max authentication failures** are dynamically blacklisted.	**Enterprise**, **Personal**, and **Open** security levels.
Accounting	Select any of the following options: • To enable accounting, select **Use authentication servers** from the **Accounting** drop-down list. On enabling the accounting function, APs post accounting information to the RADIUS server at the specified **Accounting interval**. • To use a separate server for accounting, select **Use separate servers**. The accounting server is distinguished from the authentication server specified for the SSID profile. • To disable the accounting function, select **Disabled**.	**Enterprise**, **Personal**, and **Open** security levels.

Parameter	Description	Security Level
Authentication survivability	To enable authentication survivability, set **Authentication survivability** to **Enabled**. Specify a value in hours for **Cache timeout (global)** to set the duration after which the authenticated credentials in the cache must expire. When the cache expires, the clients are required to authenticate again. You can specify a value within a range of 1–99 hours and the default value is 24 hours. **NOTE:** The authentication survivability feature requires ClearPass Policy Manager 6.0.2 or later, and is available only when the **New** server option is selected. On setting this parameter to **Enabled**, SCALANCE W authenticates the previously connected clients using EAP-PEAP authentication even when connectivity to ClearPass Policy Manager is temporarily lost. The Authentication survivability feature is not applicable when a RADIUS server is configured as an internal server.	**Enterprise** security level
MAC authentication	To enable MAC-address-based authentication for **Personal** and **Open** security levels, set **MAC authentication** to **Enabled**. For **Enterprise** security level, the following options are available: • **Perform MAC authentication before 802.1X**—Select this check box to use 802.1X authentication only when the MAC authentication is successful. • **MAC authentication fail-thru**—On selecting this check box, the 802.1X authentication is attempted when the MAC authentication fails.	**Enterprise**, **Personal**, and **Open** security levels.
Delimiter character	Specify a character (for example, colon or dash) as a delimiter for the MAC address string. When configured, the AP will use the delimiter in the MAC authentication request. For example, if you specify colon as the delimiter, MAC addresses in the xx:xx:xx:xx:xx:xx format are used. If the delimiter is not specified, the MAC address in the xxxxxxxxxxxx format is used. **NOTE:** This option is available only when MAC authentication is enabled.	**Enterprise**, **Personal**, and **Open** security levels.
Uppercase support	Set to **Enabled** to allow the AP to use uppercase letters in MAC address string for MAC authentication. **NOTE:** This option is available only if MAC authentication is enabled.	**Enterprise**, **Personal**, and **Open** security levels.
Upload Certificate	Click **Upload Certificate** and browse to upload a certificate file for the internal server. For more information on certificates, see Uploading Certificates (Page 216).	**Enterprise**, **Personal**, and **Open** security levels

Parameter	Description	Security Level
Fast Roaming	You can configure the following fast roaming options for the WLAN SSID: • **Opportunistic Key Caching**: You can enable **Opportunistic Key Caching** (OKC) when **WPA-2 Enterprise** and **Both (WPA2 & WPA)** encryption types are selected. If OKC is enabled, a cached pairwise master key (PMK) is used when the client roams to a new AP. This allows faster roaming of clients without the need for a complete 802.1X authentication. • **802.11r**: Selecting this check box enables fast BSS transition. The Fast BSS Transition mechanism minimizes the delay when a client transitions from one BSS to another within the same cluster. This option is available only when WPA-2 Enterprise and WPA-2 personal encryption keys are selected. • **802.11k**: Selecting this check box enables 802.11k roaming on the SSID profile. The 802.11k protocol enables APs and clients to dynamically measure the available radio resources. When 802.11k is enabled, APs and clients send neighbor reports, beacon reports, and link measurement reports to each other. • **802.11v**: Selecting this check box enables the 802.11v-based BSS transition. 802.11v standard defines mechanisms for wireless network management enhancements and BSS transition management. It allows client devices to exchange information about the network topology and RF environment. The BSS transition management mechanism enables an AP to request a voice client to transition to a specific AP, or suggest a set of preferred APs to a voice client, due to network load balancing or BSS termination. It also helps the voice client identify the best AP to transition to as they roam.	**Enterprise**, **Personal**, and **Open** security levels.

5. Click **Next** to configure access rules. For more information, see Configuring Access Rules for a WLAN SSID Profile. (Page 111)

In the CLI

To configure enterprise security settings for the Employee and Voice users:

```
(AP)(config)# wlan ssid-profile <name>

(AP)(SSID Profile <name>)# opmode {wpa2-aes|wpa-tkip,wpa2-aes|dynamic-wep}

(AP)(SSID Profile <name>)# leap-use-session-key

(AP)(SSID Profile <name>)# termination

(AP)(SSID Profile <name>)# auth-server <server-name>

(AP)(SSID Profile <name>)# external-server

(AP)(SSID Profile <name>)# server-load-balancing

(AP)(SSID Profile <name>)# blacklist

(AP)(SSID Profile <name>)# mac-authentication

(AP)(SSID Profile <name>)# l2-auth-failthrough

(AP)(SSID Profile <name>)# auth-survivability

(AP)(SSID Profile <name>)# radius-accounting

(AP)(SSID Profile <name>)# radius-accounting-mode {user-association|user-
authentication}

(AP)(SSID Profile <name>)# radius-interim-accounting-interval <minutes>

(AP)(SSID Profile <name>)# radius-reauth-interval <minutes>

(AP)(SSID Profile <name>)# max-authentication-failures <number>

(AP)(SSID Profile <name>)# no okc-disable

(AP)(SSID Profile <name>)# dot11r

(AP)(SSID Profile <name>)# dot11k

(AP)(SSID Profile <name>)# dot11v
```

To configure personal security settings for the Employee and Voice users:

```
(AP)(config)# wlan ssid-profile <name>

(AP)(SSID Profile <name>)# opmode {wpa2-psk-aes|wpa-tkip|wpa-psk-tkip|wpa-psk-
tkip,wpa2-psk-aes|static-wep}

(AP)(SSID Profile <name>)# mac-authentication

(AP)(SSID Profile <name>)# auth-server <server-name>

(AP)(SSID Profile <name>)# external-server

(AP)(SSID Profile <name>)# server-load-balancing

(AP)(SSID Profile <name>)# blacklist

(AP)(SSID Profile <name>)# max-authentication-failures <number>

(AP)(SSID Profile <name>)# radius-accounting

(AP)(SSID Profile <name>)# radius-accounting-mode {user-association|user-
authentication}
```

```
(AP)(SSID Profile <name>)# radius-interim-accounting-interval <minutes>

(AP)(SSID Profile <name>)# radius-reauth-interval <minutes>
```

To configure open security settings for Employee and Voice users of a WLAN SSID profile:

```
(AP)(config)# wlan ssid-profile <name>

(AP)(SSID Profile <name>)# opmode opensystem

(AP)(SSID Profile <name>)# mac-authentication

(AP)(SSID Profile <name>)# auth-server <server-name>

(AP)(SSID Profile <name>)# external-server

(AP)(SSID Profile <name>)# server-load-balancing

(AP)(SSID Profile <name>)# blacklist

(AP)(SSID Profile <name>)# max-authentication-failures <number>

(AP)(SSID Profile <name>)# radius-accounting

(AP)(SSID Profile <name>)# radius-accounting-mode {user-association|user-
authentication}

(AP)(SSID Profile <name>)# radius-interim-accounting-interval <minutes>

(AP)(SSID Profile <name>)# radius-reauth-interval <minutes>
```

11.1.4 Configuring Access Rules for a WLAN SSID Profile

This section describes the procedure for configuring security settings for Employee and Voice networks only. For information on guest network configuration, see Captive Portal for Guest Access (Page 139).

Note

If you are creating a new SSID profile, complete the WLAN settings and configure VLAN and security parameters, before defining access rules. For more information, see Configuring WLAN Settings for an SSID Profile (Page 96), Configuring VLAN Settings for a WLAN SSID Profile (Page 101) and Configuring Security Settings for a WLAN SSID Profile. (Page 104)

You can configure up to 128 access rules for an Employee, Voice , or Guest network using the SCALANCE W UI or the CLI.

In the SCALANCE W UI

To configure access rules for an Employee or Voice network:

1. In the Access Rules tab, set the slider to any of the following types of access control:

- **Unrestricted**—Select this option to set unrestricted access to the network.
- **Network-based**—Set the slider to **Network-based** to set common rules for all users in a network. The **Allow any to all destinations** access rule is enabled by default. This rule allows traffic to all destinations.

  To define an access rule:

  – Click **New**.

  – Select appropriate options in the **New Rule** window.

  – Click **OK**.
- **Role-based**—Select this option to enable access based on user roles. For role-based access control:

  – Create a user role if required. For more information, see Configuring User Roles.

  – Create access rules for a specific user role. For more information, see Configuring ACL Rules for Network Services (Page 220). You can also configure an access rule to enforce captive portal authentication for an SSID that is configured to use 802.1X authentication method. For more information, see Configuring Captive Portal Roles for an SSID (Page 167).

  – Create a role assignment rule. For more information, see Configuring Derivation Rules (Page 240).

2. Click **Finish**.

In the CLI

To configure access control rules for a WLAN SSID:

```
(AP)(config)# wlan access-rule <name>

(AP)(Access Rule <name>)# rule <dest> <mask> <match> {<protocol> <start-port> <end-
port> {permit|deny|src-nat [vlan <vlan_id>|tunnel]|dst-nat{<IP-address>
<port>|<port>}}| app

<app> {permit|deny}| appcategory <appgrp>|webcategory <webgrp> {permit|deny}|
webreputation

<webrep> [<option1....option9>]
```

To configure access control rules based on the SSID:

```
(AP)(config)# wlan ssid-profile <name>

(AP)(SSID Profile <name>)# set-role-by-ssid
```

To configure role assignment rules:

```
(AP)(config)# wlan ssid-profile <name>
```

```
(AP)(SSID Profile <name>)# set-role <attribute>{{equals|not-equals|starts-with|ends-
with|contains|matches-regular-expression}<operator><role>|value-of}
```

To configure a pre-authentication role:

```
(AP)(config)# wlan ssid-profile <name>
```

```
(AP)(SSID Profile <name>)# set-role-pre-auth <role>
```

To configure machine and user authentication roles:

```
(AP)(config)# wlan ssid-profile <name>
```

```
(AP)(SSID Profile <name>)# set-role-machine-auth <machine_only> <user_only>
```

To configure unrestricted access:

```
(AP)(config)# wlan ssid-profile <name>
```

```
(AP)(SSID Profile <name>)# set-role-unrestricted
```

Example

The following example configures access rules for the wireless network:

```
(AP)(config)# wlan access-rule WirelessRule
```

11.1.5 SSID and VLAN Configuration

You can set a unique SSID and also configure a unique a VLAN for each AP in a cluster. Clients will be able to connect to the defined SSIDs and can configure the defined VLANs in the AP cluster.

You can configure the SSID and VLAN settings by using the SCALANCE W CLI.

In the CLI

The following command is used to configure SSID and VLAN settings in a WLAN profile:

```
(AP)(config)# wlan ssid-profile TechPubsAP
```

```
(AP)(SSID Profile "TechPubsAP")# essid $per-ap-ssid
```

```
(AP)(SSID Profile "TechPubsAP")# vlan $per-ap-vlan
```

To configure SSID settings:

```
(AP)# per-ap-ssid pcap
```

To configure VLAN settings:

```
(AP)# per-ap-vlan 123
```

To verify the SSID and VLAN configurations:

```
(AP)# show ap-env

Antenna Type:Internal

Need USB field:Yes

per_ap_ssid:pcap

per_ap_vlan:123

installation_type:indoor

uap_controller_less:1

flex_radio_mode:2.4ghz

ap2xx_prestandard_poeplus_detection:1
```

Note

For information on configuring a native VLAN on a wired profile, see Configuring VLAN for a Wired Profile (Page 127).

11.2 Configuring Fast Roaming for Wireless Clients

11.2.1 Opportunistic Key Caching

SCALANCE W now supports OKC-based roaming. In OKC-based roaming, the AP stores one PMK per client, which is derived from the last 802.1X authentication completed by the client in the network. The cached PMK is used when a client roams to a new AP. This allows faster roaming of clients between the APs in a cluster, without requiring a complete 802.1X authentication.

Note

OKC roaming (when configured in the 802.1X Authentication profile) is supported on WPA-2 clients. If the wireless client (the 802.1X supplicant) does not support this feature, a complete 802.1X authentication is required whenever a client roams to a new AP

Configuring an AP for OKC Roaming

You can enable OKC roaming for WLAN SSID by using the SCALANCE W UI or the CLI.

In the SCALANCE W UI

1. Navigate to the WLAN wizard.
2. Go to **Network > New** OR Go to **Network > WLAN SSID** and click **edit**.
3. Click the **Security** tab.

4. Move the slider to the **Enterprise** security level. On selecting the Enterprise security level, the authentication options applicable to the Enterprise network are displayed,
5. Select the **WPA-2 Enterprise** or **Both (WPA-2 & WPA)** option from the **Key management** drop-down list. When any of these encryption types is selected, **Opportunistic Key Caching OKC** is enabled by default.
6. Click **Next** and then click **Finish**.

In the CLI

To disable OKC roaming on a WLAN SSID:

```
(AP)(config)# wlan ssid-profile <name>

(AP)(SSID Profile "<name>")# opmode {wpa2-aes|wpa-tkip,wpa-aes,wpa2-tkip,wpa2-aes}

(AP)(SSID Profile "<name>")# okc-disable
```

To enable OKC roaming on a WLAN SSID:

```
(AP)(config)# wlan ssid-profile <name>

(AP)(SSID Profile "<name>")# opmode {wpa2-aes| wpa-tkip,wpa-aes,wpa2-tkip,wpa2-aes} (

AP)(SSID Profile "<name>")# no okc-disable
```

11.2.2 Fast BSS Transition (802.11r Roaming)

802.11r is a roaming standard defined by IEEE. When enabled, 802.11r reduces roaming delay by pre- authenticating clients with multiple target APs before a client roams to an AP. With 802.11r implementation, clients pre-authenticate with multiple APs in a cluster.

As part of the 802.11r implementation, SCALANCE W supports the Fast BSS Transition protocol. The Fast BSS Transition mechanism reduces client roaming delay when a client transitions from one BSS to another within the same cluster. This minimizes the time required to resume data connectivity when a BSS transition happens

Note

Fast BSS Transition is operational only if the wireless client supports 802.11r standard. If the client does not support 802.11r standard, it falls back to the normal WPA-2 authentication method.

Configuring an AP for 802.11r support

You can configure 802.11r support for a WLAN SSID by using the SCALANCE W UI or the CLI.

In the SCALANCE W UI

1. Navigate to the WLAN wizard.
2. Go to **Network > New** OR Go to **Network > WLAN SSID** and click **edit**.
3. Click the **Security** tab.

4. Under **Fast Roaming**, select the **802.11r** check box.
5. Click **Next** and then click **Finish**.

In the CLI

To enable 802.11r roaming on a WLAN SSID:

```
(AP)(config)# wlan ssid-profile <name>

(AP)(SSID Profile <name>)# dot11r
```

Example

```
(AP)(config)# wlan ssid-profile dot11r-profile

(AP)(SSID Profile "dot11r-profile")# dot11r
```

Mobility Domain Identifier

In a network of standalone APs within the same management VLAN, 802.11r roaming does not work. This is because the mobility domain identifiers do not match across APs. They are auto-generated based on a virtual controller key. SCALANCE W introduces an option for users to set a mobility domain identifier for 802.11r SSIDs. For standalone APs in the same management VLAN, 802.11r roaming works only when the mobility domain identifier is configured with the same value.

You can configure a mobility domain identifier by using the SCALANCE W UI or the CLI.

In the SCALANCE W UI

1. Navigate to the WLAN wizard (Go to **Network>New** OR Go to **Network>WLAN SSID** and click **edit**).
2. Click the **Security** tab.
3. Under **Fast Roaming**, select the **802.11r** check box.
4. When the **802.11r** checkbox is selected, the **MDID** text box is displayed. Enter the mobility domain identifier in **MDID**.
5. Click **Next** and then click **Finish**.

In the SCALANCE W CLI

To enable MDID on a WLAN SSID:

```
(AP)(config)# wlan ssid-profile <name>

(AP)(SSID Profile <name>)# mdid <Mobility domain ID>
```

11.2.3 Radio Resource Management (802.11k)

The 802.11k standard provides mechanisms for APs and clients to dynamically measure the available radio resources and enables stations to query and manage their radio resources. In an 802.11k-enabled network, APs and clients can share radio and link measurement information, neighbor reports, and beacon reports with each other. This allows the WLAN network infrastructural elements and clients to assess resources and make optimal mobility decisions to ensure QoS and seamless continuity.

SCALANCE W supports the following radio resource management information elements with 802.11k support enabled:

- **Power Constraint IE**—The power constraint element contains the information necessary to allow a client to determine the local maximum transmit power in the current channel.
- **AP Channel Report IE**—The AP channel report element contains a list of channels in a regulatory class where a client is likely to find an AP, including the AP transmitting the AP channel report.
- **Radio Resource Management Enabled Capabilities IE**—The RRM-enabled capabilities element signals support for radio measurements in a device. The clients use this IE to specify their radio measurement capabilities.
- **BSS Load Element**—The BSS load element contains information on the density of clients and traffic levels in the QBSS.
- **TPC Report IE**—The TPC IE contains transmit power and link margin information.
- **Quiet IE**: The Quiet IE defines an interval during which no transmission occurs in the current channel. This interval may be used to assist in making channel measurements without interference from other stations in the BSS.
- **Extended Capabilities IE**—The extended capabilities IE carries information about the capabilities of an IEEE 802.11 station

Beacon Report Requests and Probe Responses

The beacon request frame is sent by an AP to request a client to report the list of beacons detected by the client on all channels.

- The beacon request is sent using the radio measurement request action frame.
- It is sent only to those clients that have the capability to generate beacon reports. The clients indicate their capabilities through the *RRM enabled capabilities IE* sent in the association request frames.
- By default, the beacon request frames are sent at a periodicity of 60 seconds.

Configuring a WLAN SSID for 802.11k Support

You can enable 802.11k support on a WLAN SSID by using the SCALANCE W UI or the CLI.

In the SCALANCE W UI

1. Navigate to the WLAN wizard (Go to **Network > New** OR Go to **Network > WLAN SSID** and click **edit**).
2. Click the **Security** tab.
3. Under **Fast Roaming**, select the **802.11k** check box.
4. Click **Next** and then click **Finish**.

Note

To allow the AP and clients to exchange neighbor reports, ensure that Client match is enabled through **RF > ARM > Client match > Enabled** in the UI or by executing the **client-match** command in the **arm** configuration subcommand mode.

In the CLI

To enable 802.11k profile:

```
(AP)(config)# wlan ssid-profile <name>
```

```
(AP)(SSID Profile <name>)# dot11k
```

To view the beacon report details:

```
(AP)# show ap dot11k-beacon-report <mac>
```

To view the neighbor details:

```
(AP)# show ap dot11k-nbrs
```

Example

```
(AP)(config)# wlan ssid-profile dot11k-profile
```

```
(AP)(SSID Profile "dot11k-profile")# dot11k
```

11.2.4 BSS Transition Management (802.11v)

The 802.11v standard provides Wireless Network Management enhancements to the IEEE 802.11 MAC and PHY. It extends radio measurements to define mechanisms for wireless network management of stations including BSS transition management.

APs support the generation of the BSS transition management request frames to the 802.11k clients when a suitable AP is identified for a client through Client Match.

Configuring a WLAN SSID for 802.11v Support

You can enable 802.11v support on a WLAN SSID by using the SCALANCE W UI or the CLI.

In the SCALANCE W UI

1. Navigate to the WLAN wizard (Go to **Network > New** OR Go to **Network > WLAN SSID** and click **edit**).
2. Click the **Security** tab.
3. Under **Fast Roaming**, select the **802.11v** check box.
4. Click **Next** and then click **Finish**.

In the CLI

To enable 802.11v profile:

```
(AP)(config)# wlan ssid-profile <name>
```

```
(AP)(SSID Profile <name>)# dot11v
```

Example

```
(AP)(config)# wlan ssid-profile dot11v-profile
```

```
(AP)(SSID Profile "dot11v-profile")# dot11v
```

11.3 Configuring Modulation Rates on a WLAN SSID

APs allow you to enable or disable modulation rates for a radio band; HT MCS set; and VHT MCS rates set, when configuring a WLAN SSID profile. For example, the 802.11g band supports the modulation rate including 1, 2, 5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps and 802.11a band supports a modulation rate set including 6, 9, 12, 18, 24, 36, 48, 54 Mbps.

The 802.11 radio profiles support basic modulation and transmission rates. The 802.11g basic modulation rates determine the 802.11b or 802.11g rates for the data that are advertised in beacon frames and probe response and 802.11g transmission rates determine the 802.11b or 802.11g rates at which the AP can transmit data.

For 802.11n clients, you can now configure an HT MCS rate set so that the SSID does not broadcast the disabled MCS rates list.

For 802.11ac clients, only 10 MCS rates supported in the 802.11ac mode and APs use a combination of VHT MCSs and spatial streams to convey the supported MCS rates.

To configure modulation rates:

```
(AP)# config terminal

(AP)(config)# wlan ssid-profile <ssid_profile>

(AP)(SSID Profile "<ssid_profile>")# a-basic-rates 6 9 12 18

(AP)(SSID Profile "<ssid_profile>")# a-tx-rates 36 48 54

(AP)(SSID Profile "<ssid_profile>")# supported-mcs-set 1,3,6,7

(AP)(SSID Profile "<ssid_profile>")# vht-support-mcs-map 7, 9, 8
```

11.4 Multi-User-MIMO

The MU-MIMO feature allows the 802.11ac Wave 2 APs to send multiple frames to multiple clients simultaneously over the same frequency spectrum. With MU-MIMO, APs can support simultaneous directional RF links and up to four simultaneous full-rate Wi-Fi connections (for example, smart phone, tablet, laptop, multimedia player, or other client device).

The MU-MIMO feature is enabled by default on WLAN SSIDs to allow APs to use the MU beam former bit in beacon frames to broadcast to clients. When disabled, the MU beamformer bit is set to unsupported.

Enabling or Disabling MU-MIMO

The MU-MIMO feature is enabled by default on WLAN SSIDs. To disable this feature:

```
(host)(config)# wlan ssid-profile <ssid_profile> (host)(SSID Profile
"<ssid_profile>")# vht-mu-txbf-disable
```

To re-enable MU-MIMO:

```
(host)(config)# wlan ssid-profile <ssid_profile>

(host)(SSID Profile "<ssid_profile>")# no vht-mu-txbf-disable
```

RTS/CTS Flow Control

The RTS/CTS mechanism allows devices to reserve the RF medium and minimize the frame collisions introduced by hidden stations. When RTS is enabled, a higher number of retransmissions occurring on the WLAN triggers the RTS/CTS handshake and the transmitter station sends an RTS frame to the receiver station. The receiver station responds with a CTS frame. The RTS/CTS frames are sent only when the packet size exceeds the RTS threshold. By default, the RTS threshold is set to 2333 octets.

Configuring RTS/CTS Threshold

You can set the RTS/CTS threshold value within the range of 0–2347 octets. By default, the RTS/CTS threshold is set to 2333.

To configure the RTS/CTS threshold:

```
(AP)(config)# wlan ssid-profile <ssid_profile>

(AP)(SSID Profile "<ssid_profile>")# rts-threshold <threshold>
```

To disable RTS/CTS, set the RTS threshold value to 0.

11.5 Management Frame Protection

SCALANCE W supports the IEEE 802.11w standard, also known as Management Frame Protection. The Management Frame Protection increases the security by providing data confidentiality of management frames.

Management Frame Protection uses 802.11i framework that establishes encryption keys between the client and AP.

To enable Management Frame Protection on the AP:

```
(AP)(config)# wlan ssid-profile myAP

(AP)(SSID Profile "myAP")# mfp-capable

(AP)(SSID Profile "myAP")# mfp-required
```

If the *mfp-required* parameter is enabled, the SSID supports only the clients that exhibit the Management Frame Protection functionality.

If the *mfp-required* parameter is enabled, the SSID supports only the clients that exhibit the Management Frame Protection functionality.

Note

- The Management Frame Protection configuration is a per-SSID configuration
- Management Frame Protection can be enabled only on WPA2-PSK and WPA2-enterprise SSIDs. The 802.11r fast roaming option will not take effect when MFP is enabled.

11.6 Disabling Short Preamble for Wireless Client

To improve the network performance and communication between the AP and its clients, you can enable or disable the transmission and reception of short preamble frames. If the short preamble is optional for the wireless devices connecting to an SSID, you can disable short preamble through the AP CLI. Short preamble is enabled by default.

To disable the short preamble:

```
(AP)# config terminal

(AP)(config)# wlan ssid-profile <ssid_profile>

(AP)(SSID Profile "<ssid_profile>")# short-preamble-disable
```

11.7 Editing Status of a WLAN SSID Profile

You can enable or disable an SSID profile in the SCALANCE W UI or the CLI.

In the SCALANCE W UI

To modify the status of a WLAN SSID profile:

1. On the **Network** tab, select the network that you want to edit. The **edit** link is displayed.
2. Click the **edit** link. The **Edit network** window is displayed.
3. Select or clear the **Disable SSID** check box to disable or enable the SSID. The SSID is enabled by default.
4. Click **Next** (or the tab name) to move to the next tab.
5. Click **Finish** to save the modifications.

In the CLI

To disable an SSID:

```
(AP)(config)# wlan ssid-profile <name>
(AP)(SSID Profile <name>)# disable
```

To enable an SSID:

```
(AP)(config)# wlan ssid-profile <name>
(AP)(SSID Profile <name>)# enable
```

11.8 Editing a WLAN SSID Profile

To edit a WLAN SSID profile:

1. On the **Network** tab, select the network that you want to edit. The **edit** link is displayed.
2. Click the **edit** link. The **Edit network** window is displayed.
3. Modify the settings as required. Click **Next** to move to the next tab.
4. Click **Finish** to save the changes.

11.9 Deleting a WLAN SSID Profile

To delete a WLAN SSID profile:

1. On the **Network** tab, click the network that you want to delete. A **x** link is displayed beside the network to be deleted.
2. Click **x**. A delete confirmation window is displayed.
3. Click **Delete Now**.

Wired Profiles 12

12.1 Configuring a Wired Profile

The Ethernet ports allow third-party devices such as VoIP phones or printers (which support only wired connections) to connect to the wireless network. You can also configure an ACL for additional security on the Ethernet downlink.

The wired profile configuration for Employee network involves the following procedures:

1. Configuring Wired Settings (Page 125)
2. Configuring VLAN for a Wired Profile (Page 127)
3. Configuring Security Settings for a Wired Profile (Page 129)
4. Configuring Access Rules for a Wired Profile (Page 131)

For information on creating a wired profile for guest network, see Captive Portal for Guest Access (Page 139).

12.1.1 Configuring Wired Settings

You can configure wired settings for a wired profile by using the SCALANCE W UI or the CLI.

In the SCALANCE W UI

1. Click the **Wired** link under **More** on the SCALANCE W main window. The **Wired** window is displayed.
2. Click **New** under **Wired Networks**. The **New Wired Network** window is displayed.
3. Click the **Wired Settings** tab and configure the following parameters:
   - **Name**—Specify a name for the profile.
   - **Primary Usage**—Select **Employee** or **Guest**.
   - **Speed/Duplex**—Ensure that appropriate values are selected for **Speed/Duplex**. Contact your network administrator if you need to assign speed and duplex parameters.
   - **POE**—Set **POE** to **Enabled** to enable PoE.
   - **Admin Status**—Ensure that an appropriate value is selected. The **Admin Status** indicates if the port is up or down.

4. Click **Show advanced options** and configure the following parameters as required:
   - **Content Filtering**—To ensure that all DNS requests to non-corporate domains on this wired network are sent to OpenDNS, select **Enabled** for **Content Filtering**.
   - **Uplink**—Select **Enabled** to configure uplink on this wired profile. If **Uplink** is set to **Enabled** and this network profile is assigned to a specific port, the port will be enabled as Uplink port. For more information on assigning a wired network profile to a port, see Assigning a Profile to Ethernet Ports (Page 133).
   - **Spanning Tree**—Select the **Spanning Tree** check box to enable STP on the wired profile. STP ensures that there are no loops in any bridged Ethernet network and operates on all downlink ports, regardless of forwarding mode. STP will not operate on the uplink port and is supported only on APs with three or more ports. By default, Spanning Tree is disabled on wired profiles.
   - **Inactivity Timeout**—Specify the time out interval within the range of 60–86,400 seconds for inactive wired clients. The default interval is 1000 seconds.
5. Click **Next**. The **VLAN** tab details are displayed.
6. Configure VLAN for the wired profile. For more information, see Configuring VLAN for a Wired Profile (Page 127).

In the CLI

To configure the settings for a wired profile:

```
(AP)(config)# wired-port-profile <name>

(AP)(wired ap profile <name>)# type {<employee>|<guest>}

(AP)(wired ap profile <name>)# speed {10|100|1000|auto}

(AP)(wired ap profile <name>)# duplex {half|full|auto}

(AP)(wired ap profile <name>)# no shutdown

(AP)(wired ap profile <name>)# poe

(AP)(wired ap profile <name>)# uplink-enable

(AP)(wired ap profile <name>)# content-filtering

(AP)(wired ap profile <name>)# spanning-tree
```

12.1.2 Configuring VLAN for a Wired Profile

Note

If you are creating a new wired profile, complete the Wired Settings procedure before configuring the VLAN settings. For more information, see Configuring Wired Settings (Page 125).

You can configure VLAN using the SCALANCE W UI or the CLI.

In the SCALANCE W UI

To configure a VLAN:

1. In the **VLAN** tab, enter the following information.

   Mode—You can specify any of the following modes:

   – **Access**—Select this mode to allow the port to carry a single VLAN specified as the native VLAN.

   – **Trunk**—Select this mode to allow the port to carry packets for multiple VLANs specified as allowed VLANs.

   Specify any of the following values for **Client IP Assignment**:

   – **Virtual Controller Assigned**: Select this option to allow the virtual controller to assign IP addresses to the wired clients. When the virtual controller assignment is used, the source IP address is translated to the physical IP address of the master AP for all client traffic that goes through this interface. The virtual controller can also assign a guest VLAN to a wired client.

   – **Network Assigned**: Select this option to allow the clients to receive an IP address from the network to which the virtual controller is connected. On selecting this option, the **New** button to create a VLAN is displayed. Create a new VLAN if required.

   If the **Trunk** mode is selected:

   – Specify the VLAN in **Allowed VLAN**, enter a list of comma separated digits or ranges, for example, 1,2,5 or 1–4, or all. The Allowed VLAN refers to the VLANs carried by the port in Access mode.

   – If is set to , specify a value for **Native VLAN**. A VLAN that does not have a VLAN ID tag in the frames is referred to as Native VLAN. You can specify a value within the range of 1–4093.

   If the **Access** mode is selected:

   – If **Client IP Assignment** is set to **Virtual Controller Assigned**, proceed to step 2.

   – If **Client IP Assignment** is set to **Network Assigned**, specify a value for **Access VLAN** to indicate the VLAN carried by the port in the **Access** mode.

2. Client VLAN assignment—You can specify any of the following options.

   – Default—Select this option to set the default VLAN.

   – Custom—Select this option to configure a custom VLAN.

3. Click **Next**. The **Security** tab details are displayed.
4. Configure security settings for the wired profile. For more information, see Configuring Security Settings for a Wired Profile (Page 129).

In the CLI

To configure VLAN settings for a wired profile:

```
(AP)(config)# wired-port-profile <name>

(AP)(wired ap profile <name>)# switch port-mode {trunk|access}

(AP)(wired ap profile <name>)# allowed-vlan <vlan>

(AP)(wired ap profile <name>)# native-vlan {<guest|1…4095>}
```

To configure a new VLAN assignment rule:

```
(AP)(config)# wired-port-profile <name>

(AP)(wired ap profile <name>)# set-vlan <attribute>{equals|not-equals|starts-with|
ends-with|contains| matches-regular-expression} <operator> <VLAN-ID>|value-of}
```

12.1.3 Configuring Security Settings for a Wired Profile

Note

If you are creating a new wired profile, complete the Wired Settings and VLAN procedures before specifying the security settings. For more information, see Configuring Wired Settings (Page 125) and Configuring VLAN Settings for a WLAN SSID Profile (Page 127).

Configuring Security Settings for a Wired Employee Network

You can configure security parameters for the Employee network by using the SCALANCE W UI or the CLI.

In the SCALANCE W UI

To configure security parameters for the Employee network:

1. Configure the following parameters in the **Security** tab.
   - **Port type**—To support trusted ports in an AP, select **Trusted**. When the Port type is trusted, MAC and 802.1X authentication parameters cannot be configured. The Port Type is **Untrusted** by default.

   In a trusted mode, APs will not create any user entry. A predefined ACL is applied to the trusted port in order to control the client traffic that needs to be source NATed.
   - **MAC authentication**—To enable MAC authentication, select **Enabled**. The MAC authentication is disabled by default.
   - **802.1X authentication**—To enable 802.1X authentication, select **Enabled**. The 802.1X authentication is disabled by default.
   - **MAC authentication fail-thru**—To enable authentication fail-thru, select **Enabled**. When this feature is enabled, 802.1X authentication is attempted when MAC authentication fails. The **MAC authentication fail-thru** check box is displayed only when both **MAC authentication** and **802.1X authentication** are **Enabled.**
2. Select any of the following options for **Authentication server 1**:
   - **New**—On selecting this option, an external RADIUS server must be configured to authenticate the users. For information on configuring an external server, see Configuring an External Server for Authentication (Page 188) and Authentication and User Management (Page 173).
   - **Internal server**— If an internal server is selected, add the clients that are required to authenticate with the internal RADIUS server. Click the **Users** link to add users. For information on adding a user, see Managing AP Users (Page 173).

3. **Accounting**—Select any of the following options:
   - **Disabled**—Disables accounting.
   - **Use authentication servers**—When selected, the authentication servers configured for the wired profile are used for accounting purposes.
   - **Use separate servers**—Allows you to configure separate accounting servers.
   - **Accounting interval**—Allows you set an accounting interval within the range of 0–60 minutes for sending interim accounting information to the RADIUS server.
   - **Reauth interval**—Specify the interval at which all associated and authenticated clients must be reauthenticated.
4. **Load balancing**—Set this to **Enabled** if you are using two RADIUS authentication servers, so that the load across the two RADIUS servers is balanced. For more information on the dynamic load balancing mechanism, see Dynamic Load Balancing between Two Authentication Servers (Page 187).
5. Click **Next**. The **Access** tab details are displayed

In the CLI

To configure security settings for an employee network:

```
(AP)(config)# wired-port-profile <name>

(AP)(wired ap profile <name>)# mac-authentication

(AP)(wired ap profile <name>)# l2-auth-failthrough

(AP)(wired ap profile <name>)# auth-server <name>

(AP)(wired ap profile <name>)# server-load-balancing

(AP)(wired ap profile <name>)# radius-accounting

(AP)(wired ap profile <name>)# radius-accounting-mode {user-association|user-
authentication}

(AP)(wired ap profile <name>)# radius-interim-accounting-interval <minutes>

(AP)(wired ap profile <name>)# radius-reauth-interval <Minutes>

(AP)(wired ap profile <name>)# trusted
```

12.1.4 Configuring Access Rules for a Wired Profile

The Ethernet ports allow third-party devices such as VoIP phones or printers (that support only wired connections) to connect to the wireless network. You can also configure an ACL for additional security on the Ethernet downlink.

Note

If you are creating a new wired profile, complete the Wired Settings and configure the VLAN and security parameters before defining access rules. For more information, see Configuring Wired Settings (Page 125), Configuring VLAN for a Wired Profile (Page 127), and Configuring Security Settings for a Wired Profile (Page 129).

You can configure access rules by using the SCALANCE W UI or the CLI.

In the SCALANCE W UI

1. On the **Access** tab, configure the following access rule parameters.
2. Select any of the following types of access control:
   - **Role-based**—Allows the users to obtain access based on the roles assigned to them.
   - **Unrestricted**—Allows the users to obtain unrestricted access on the port.
   - **Network-based**—Allows the users to be authenticated based on access rules specified for a network.
3. If the **Role-based** access control is selected, perform the following steps:
   - Under , select an existing role for which you want to apply the access rules, or click **New** and add the required role. The list of roles defined for all networks is displayed under **Roles**.

     Note

     The default role with the same name as the network is automatically defined for each network. The default roles cannot be modified or deleted.

   - Select the access rule associated with a specific role and modify if required. To add a new access rule, click **New** in the **Access Rules** window. You can configure up to 64 access rules. For more information on configuring access rules, see Configuring ACL Rules for Network Services (Page 220).
   - Configure rules to assign roles for an authenticated client. You can also configure rules to derive VLANs for the wired network profile. For more information on role assignment rules and VLAN derivation rules, see Configuring Derivation Rules (Page 240) and Configuring VLAN Derivation Rules (Page 249).

- Select the **Assign pre-authentication role** check box to add a pre-authentication role that allows some access to the users before client authentication.
- Select the **Enforce Machine Authentication** check box, to configure access rights to clients based on whether the client device supports machine authentication. Select the **Machine auth only** and rules. Machine Authentication is only supported on Windows devices and devices such as iPads

Note

If **Enforce Machine Authentication** is enabled, both the device and the user must be authenticated for the role assignment rule to apply.

4. Click **Finish**.

In the CLI

To configure access rules for a wired profile:

```
(AP)(config)# wired-port-profile <name>

(AP)(wired ap profile <name>)# access-rule-name <name>
```

To configure role assignment rules:

```
(AP)(config)# wired-port-profile <name>

(AP)(wired ap profile <name>)# set-role <attribute>{{equals|not-equal|starts-with|
ends-with|contains|matches-regular-expression}<operator> <role>|value-of}
```

To configure a pre-authentication role:

```
(AP)(config)# wired-port-profile <name>

(AP)(wired ap profile <name>)# set-role-pre-auth <role>
```

To configure machine and user authentication roles:

```
(AP)(config)# wired-port-profile <name>

(AP)(wired ap profile <name>)# set-role-machine-auth <machine_only> <user-only>
```

To configure unrestricted access:

```
(AP)(config)# wired-port-profile <name>

(AP)(wired ap profile <name>)# set-role-unrestricted
```

12.2 Assigning a Profile to Ethernet Ports

You can assign profiles to Ethernet ports using the SCALANCE W UI or the CLI.

In the SCALANCE W UI

To assign profiles to Ethernet ports:

1. Click the **Wired** link under **More** on the SCALANCE W main window. The **Wired** window is displayed.
2. To assign an Ethernet downlink profile to Ethernet 0 port:
   - Ensure that the wired bridging on the port is enabled. For more information, see Configuring Wired Bridging on Ethernet 0 for Mesh Point (Page 420).
   - Select and assign a profile from the **0/0** drop-down list.
   - To assign a wired profile to Ethernet 0/1 port, select the profile from the **0/1** drop-down list.
   - If the AP supports Ethernet 2, Ethernet 3, and Ethernet 4 ports, assign profiles to other Ethernet ports by selecting a profile from the **0/2**, **0/3**, and **0/4** drop-down lists. If the

In the CLI

To assign profiles to Ethernet ports:

```
(AP)(config)# enet0-port-profile <name>

(AP)(config)# enet1-port-profile <name>

(AP)(config)# enet2-port-profile <name>

(AP)(config)# enet3-port-profile <name>

(AP)(config)# enet4-port-profile <name>
```

12.3 Editing a Wired Profile

To edit a wired profile:

1. Click the **Wired** link under **More** on the SCALANCE W main window. The **Wired** window is displayed.
2. In the **Wired** window, select the wired profile to modify.
3. Click **Edit**. The **Edit Wired Network** window is displayed.
4. Modify the required settings.
5. Click **Finish** to save the modifications

12.4 Deleting a Wired Profile

To delete a wired profile:

- Click the **Wired** link under **More** on the SCALANCE W main window. The Wired window is displayed.
- In the **Wired** window, select the wired profile to delete.
- Click **Delete**. The wired profile is deleted.

12.5 LACP

The APs support the IEEE 802.11ac standard for high-performance WLAN. To support maximum traffic, port aggregation is required as it increases throughput and enhances reliability. To support port aggregation, SCALANCE W supports LACP based on the IEEE 802.3ad standard. The 802.3ad standard for Ethernet aggregation uses LACP as a method to manage link configuration and balance traffic among aggregated ports.

LACP provides a standardized means for exchanging information with partner systems to form a dynamic LAG. The LACP feature is automatically enabled during AP boots and it dynamically detects the AP if connected to a partner system with LACP capability, by checking if there is any LACP PDU received on either Ethernet 0 or Ethernet 1 port.

If a switch in the cluster has the LACP capability, you can combine Ethernet 0 or Ethernet 1 interfaces into the LAG to form a single logical interface (port-channel). Port-channels can be used to provide additional bandwidth or link redundancy between two devices. AP supports link aggregation using either standard port-channel (configuration based) or LACP (protocol signaling based). You can deploy 2 access points with LACP configuration to benefit from the higher (greater than 1 Gbps) aggregate throughput capabilities of the two radios.

12.5.1 Enabling Port-Channel on a Switch

1. Create a switching profile by running the following commands:

```
(host) (config) #interface port-channel <0-63>

(host) (port-channel "1") #switching-profile <profile name>
```

2. Create a port-channel and associate the switching profile by running the following commands:

```
(host)(config)# interface-profile lacp-profile <profile-name> group-id <0-63> mode
active

(host)(config)# interface gigabitethernet <slot/module/port> lacp-profile
<profile-name>
```

Verifying LACP Configuration on the AP

There is no configuration required on the AP for enabling LACP support. However, you can view the status of LACP on APs by using the following command:

```
(AP)# show lacp status

AP LACP Status

--------------

Link Status   LACP Rate   Num Ports   Actor Key    Partner Key   Partner MAC
-----------   ---------   ---------   ---------    -----------   -----------
Up            slow        2           17           1             70:81:05:11:3e:80

Slave Interface Status

----------------------

Slave I/f Name Permanent MAC Addr Link Status      Member of LAG   Link Fail Count
-------------- ------------------ -----------      -------------   ---------------
eth0           6c:f3:7f:c6:76:6e  Up               Yes             0
eth1           6c:f3:7f:c6:76:6f  Up               Yes             0

Traffic Sent on Enet Ports

--------------------------

Radio Num            Enet 0 Tx Count                  Enet 1 Tx Count
---------            ---------------                  ---------------
0                    0                                0
1                    0                                0
non-wifi             2                                17
```

12.5.2 Enabling Static LACP Configuration

When APs connect to switches which have the LACP capability, the LACP feature does not work as expected. To enable a static LACP configuration, new commands are introduced.

APs support the dynamic LACP configuration according to a peer switch. When the peer switch enables LACP configuration, the APs form the LACP. Users can enable, disable, and remove the static LACP configuration in the AP. When the AP boots up, it forms the LACP according to the static configuration.

To enable the static LACP mode on APs:

```
(AP)# lacp-mode enable
```

To disable the static LACP mode on APs:

```
(AP)# lacp-mode disable
```

Verifying Static LACP Mode

To verify the static LACP configuration, execute the following command in the AP CLI:

```
(AP)# show ap-env Antenna

Type:Internal

name:TechPubsAP

per_ap_ssid:1234

per_ap_vlan:abc

lacp_mode:enable
```

12.6 Understanding Hierarchical Deployment

An AP with more than one wired port can be connected to the downlink wired port of another AP.

You can also form an AP network by connecting the downlink port of an AP to other APs. Only one AP in the network uses its downlink port to connect to the other APs. This AP (called the root AP) acts as the wired device for the network, provides DHCP service and an L3 connection to the ISP uplink with NAT. The root AP is always the master of the SCALANCE W network.

A typical hierarchical deployment consists of the following:

- A direct wired ISP connection or a wireless uplink.
- One or more DHCP pools for private VLANs.
- One downlink port configured on a private VLAN without authentication for connecting to slave APs. Ensure that the downlink port configured in a private VLAN is not used for any wired client connection. Other downlink ports can be used for connecting to the wired clients.

Captive Portal for Guest Access 13

12.7

13.1 Understanding Captive Portal

SCALANCE W supports the captive portal authentication method, where a web page is presented to the guest users when they try to access the Internet from hotels, conference centers, or Wi-Fi hotspots. The web page also prompts the guest users to authenticate or accept the usage policy and terms. Captive portals are used at many Wi-Fi hotspots and can be used to control wired access as well.

The SCALANCE W captive portal solution consists of the following:

- The captive portal web login page hosted by an internal or external server.
- The RADIUS authentication or user authentication against AP's internal database.
- The SSID broadcast by the AP.
- Using SCALANCE W, the administrators can create a wired or WLAN guest network based on captive portal authentication for guests, visitors, contractors, and any non-employee users who can use the enterprise Wi-Fi network. The administrators can also create guest accounts and customize the captive portal page with organization-specific logo, terms, and usage policy. With captive portal authentication and guest profiles, the devices that connect to the guest SSID are assigned IP addresses and an initial role. When a guest user tries to access a URL through HTTP or HTTPS, the captive portal web page prompting the user to authenticate with a username and password is displayed.

SCALANCE W supports the captive portal authentication method, where a web page is presented to the guest users when they try to access the Internet from hotels, conference centers, or Wi-Fi hotspots. The web page also prompts the guest users to authenticate or accept the usage policy and terms. Captive portals are used at many Wi-Fi hotspots and can be used to control wired access as well.

13.1.1 Types of Captive Portal

SCALANCE W supports the following types of captive portal authentication:

- **Internal captive portal**—For Internal captive portal authentication, an internal server is used for hosting the captive portal service. It supports the following types of authentication:
  - **Internal Authenticated**—When **Internal Authenticated** is enabled, a guest user must authenticate in the captive portal page to access the Internet. The guest users who are required to authenticate must already be added to the user database.
  - **Internal Acknowledged**—When is enabled, a guest user must accept the terms and conditions to access the Internet.
  - **External captive portal**—For external captive portal authentication, an external portal on the cloud or on a server outside the enterprise network is used.

13.1.2 Walled Garden

The administrators can also control the resources that the guest users can access and the amount of bandwidth or airtime they can use at any given time. When an external captive portal is used, the administrators can configure a walled garden, which determines access to the URLs requested by the guest users. For example, a hotel environment where the unauthenticated users are allowed to navigate to a designated login page (for example, a hotel website) and all its contents. The users who do not sign up for the Internet service can view only the “allowed” websites (typically hotel property websites).

The administrators can allow or block access to specific URLs by creating a whitelist and blacklist. When the users attempt to navigate to other websites, which are not in the whitelist of the walled garden profile, the users are redirected to the login page. If the requested URL is on the blacklist, it is blocked. If it appears on neither list, the request is redirected to the external captive portal.

13.2 Configuring a WLAN SSID for Guest Access

You can create an SSID for guest access by using the SCALANCE W UI or the CLI:

In the SCALANCE W UI

1. On the **Network** tab of the SCALANCE W main window, click the **New** link. The **New WLAN** window is displayed.
2. Enter a name that uniquely identifies a wireless network in the **Name (SSID)** text box.
3. Select the **Guest** option for **Primary usage**.
4. Click the **Show advanced options** link. The advanced options for configuration are displayed.
5. Enter the required values for the following WLAN configuration parameters:

Parameter	Description
Broadcast filtering	Select any of the following values: • **All**—When set to **All**, the AP drops all broadcast and multicast frames except DHCP and ARP, IGMP group queries, and IPv6 neighbor discovery protocols. • **ARP**—When set to **ARP**, the AP drops all broadcast and multicast frames except DHCP and ARP, IGMP group queries, and IPv6 neighbor discovery protocols and additionally converts ARP requests to unicast and send frames directly to the associated client. • **Unicast-ARP-Only** — When set to **Unicast-ARP-Only**, the AP allows all broadcast and multicast frames as it is, however the ARP requests are converted to unicast frames and sends them to the associated clients. The broadcast filtering is set to **Unicast-ARP-Only** by default when an SSID profile is created. • **Disabled**— When set to **Disabled**, all broadcast and multicast traffic is forwarded to the wireless interfaces.
Multicast transmission optimization	Select **Enabled** if you want the AP to select the optimal rate for sending broadcast and multicast frames based on the lowest of unicast rates across all associated clients. When this option is enabled, multicast traffic can be sent at up to 24 Mbps. The default rate for sending frames for 2.4 GHz is 1 Mbps and 5 GHz is 6 Mbps. This option is disabled by default.

Parameter	Description
Dynamic multicast optimization	Select **Enabled** to allow AP to convert multicast streams into unicast streams over the wireless link. Enabling DMO enhances the quality and reliability of streaming video, while preserving the bandwidth available to the non-video clients. **NOTE:** When you enable DMO on multicast SSID profiles, ensure that the DMO feature is enabled on all SSIDs configured in the same VLAN.
DMO channel utilization threshold	Specify a value to set a threshold for DMO channel utilization. With DMO, the AP converts multicast streams into unicast streams as long as the channel utilization does not exceed this threshold. The default value is 90% and the maximum threshold value is 100%. When the threshold is reached or exceeds the maximum value, the AP sends multicast traffic over the wireless link.
Transmit Rates	Specify the following parameters: • **2.4 GHz**—If the 2.4 GHz band is configured on the AP, specify the minimum and maximum transmission rate. The default value for minimum transmission rate is 1 Mbps and maximum transmission rate is 54 Mbps. • **5 GHz**—If the 5 GHz band is configured on the AP, specify the minimum and maximum transmission rate. The default value for minimum transmission rate is 6 Mbps and maximum transmission rate is 54 Mbps
Band	Select a value to specify the band at which the network transmits radio signals. You can set the band to **2.4 GHz**, **5 GHz**, or **All**. The **All** option is selected by default.
DTIM interval	The **DTIM interval** indicates the delivery traffic indication message (DTIM) period in beacons, which can be configured for every WLAN SSID profile. The DTIM interval determines how often the AP should deliver the buffered broadcast and multicast frames to associated clients in the powersave mode. The default value is 1, which means the client checks for buffered data on the AP at every beacon. You can also configure a higher DTIM value for power saving.
Min RSSI probe request	Sets a minimum RSSI threshold for probe requests.
Min RSSI auth request	Sets a minimum RSSI threshold for authentication requests.
Very high throughput	Enables VHT function on AP devices that support VHT. For 802.11ac APs, the VHT function is enabled by default. However, you can disable the VHT function if you want the 802.11ac APs to function as 802.11n APs. If VHT is configured or disabled on an SSID, the changes will apply only to the SSID on which it is enabled or disabled.

Parameter	Description
Zone	Specify the zone for the SSID. When the zone is defined in SSID profile and if the same zone is defined on an AP, the SSID is created on that AP. For more information on configuring zone details, see Configuring Zone Settings on an AP (Page **Fehler! Textmarke nicht definiert.**). The following constraints apply to the zone configuration: • An AP can belong to only one zone and only one zone can be configured on an SSID. • If an SSID belongs to a zone, all APs in this zone can broadcast this SSID. If no AP belongs to the zone configured on the SSID, the SSID is not broadcast. • If an SSID does not belong to any zone, all APs can broadcast this SSID.
Time Range	Click **Edit**, select a Time Range Profile from the list and specify if the profile must be enabled or disabled for the SSID, and then click **OK**.
Bandwidth Limits	Under **Bandwidth Limits**: • **Airtime**—Select this check box to specify an aggregate amount of airtime that all clients in this network can use for sending and receiving data. Specify the airtime percentage. • **Each radio**—Select this check box to specify an aggregate amount of throughput that each radio is allowed to provide for the connected clients. • **Downstream** and **Upstream**—Specify the downstream and upstream rates within a range of 1 to 65,535 Kbps for the SSID users. If the assignment is specific for each user, select the **Peruser** check box.

Parameter	Description
Wi-Fi Multimedia (WMM) traffic management	Configure the following options for WMM traffic management. WMM supports voice, video, best effort, and background access categories. To allocate bandwidth for the following types of traffic, specify a percentage value under **Share**. To configure DSCP mapping, specify a value under **DSCP Mapping**. • **Background WMM**—For background traffic such as file downloads or print jobs. • **Best effort WMM**—For best effort traffic such as traffic from legacy devices or traffic from applications or devices that do not support QoS. • **Video WMM**—For video traffic generated from video streaming. • **Voice WMM**— For voice traffic generated from the incoming and outgoing voice communication. For more information on WMM traffic and DSCP mapping, see Wi-Fi Multimedia Traffic Management (Page 343).
	For voice traffic and Spectralink Voice Prioritization, configure the following parameters: • **Traffic Specification (TSPEC)**—To prioritize time-sensitive traffic such as voice traffic initiated by the client, select the **Traffic Specification (TSPEC)** check box. • **TSPEC Bandwidth**—To reserve bandwidth, set the TPSEC bandwidth to the desired value within the range of 200–600,000 Kbps. The default value is 2000 Kbps. • **Spectralink Voice Protocol (SVP)** —Select the check box to prioritize voice traffic for SVP handsets.

Parameter	Description
Content filtering	Select **Enabled** to route all DNS requests for the non-corporate domains to OpenDNS on this network.
Inactivity timeout	Specify an interval for session timeout in seconds, minutes or hours. If a client session is inactive for the specified duration, the session expires and the users are required to log in again. You can specify a value within the range of 60-86,400 seconds or up to 24 hours for a client session. The default value is 1000 seconds.
Deauth Inactive Clients	Select **Enabled** to allow the AP to send a deauthentication frame to the inactive client and clear client entry.
SSID	Select the **Hide** check box if you do not want the SSID (network name) to be visible to users. Select the **Disable** check box if you want to disable the SSID. On selecting this, the SSID will be disabled, but will not be removed from the network. By default, all SSIDs are enabled.
Out of service (OOS)	Enable or disable the SSID based on the following out-of-service states of the AP: • VPN down • Uplink down • Internet down • Primary uplink down The network will be out of service when selected event occurs and the SSID is enabled or disabled as per the configuration settings applied. For example, if you select the VPN down option from the drop-down list and set the status to enabled, the SSID is enabled when the VPN connection is down and is disabled when the VPN connection is restored.
OOS time (global)	Configure a hold time interval in seconds within a range of 30 to 300 seconds, after which the out-of-service operation is triggered. For example, if the VPN is down and the configured hold time is 45 seconds, the effect of this out-of-service state impacts the SSID availability after 45 seconds.
Max clients threshold	Specify the maximum number of clients that can be configured for each BSSID on a WLAN. You can specify a value within the range of 0 to 255. The default value is 64.
SSID Encoding	To encode the SSID, select UTF8. By default, the SSIDs are not encoded.
Deny inter user bridging	When enabled, the bridging traffic between two clients connected to the same SSID on the same VLAN is disabled. The clients can connect to the Internet, but cannot communicate with each other, and the bridging traffic between the clients is sent to the upstream device to make the forwarding decision.
ESSID	Enter the ESSID. If the value defined for ESSID value is not the same as profile name, the SSIDs can be searched based on the ESSID value and not by its profile name.

6. Click **Next** to configure VLAN settings. The VLAN tab contents are displayed.
7. Select any for the following options for **Client IP assignment**:
   – **Virtual Controller assigned**— On selecting this option, the wired client obtains the IP address from the virtual controller. When this option is used, the source IP address is

translated to the physical IP address of the master AP for all client traffic that goes through this interface. The virtual controller can also assign a guest VLAN to the client,.

– **Network assigned**— On selecting this option, the IP address is obtained from the network.

8. Based on the type client IP assignment mode selected, you can configure the VLAN assignment for clients as described in the following table:

Client IP Assignment	Client VLAN Assignment
Virtual Controller assigned	If the **Virtual Controller assigned** is selected for client IP assignment, the virtual controller creates a private subnet and VLAN on the AP for the wireless clients. The NAT for all client traffic that goes out of this interface is carried out at the source. This setup eliminates the need for complex VLAN and IP address management for a multi-site wireless network. On selecting this option, the following client VLAN assignment options are displayed: • **Default**: When selected, the default VLAN as determined by the virtual controller is assigned for clients. • **Custom**: When selected, you can specify a custom VLAN assignment option. You can select an existing DHCP scope for client IP and VLAN assignment or you can create a new DHCP scope by selecting **New**. For more information on DHCP scopes, see Configuring DHCP Scopes. (Page 253)

Client IP Assignment	Client VLAN Assignment
Network assigned	If the **Network assigned** is selected, you can specify any of the following options for the **Client VLAN assignment**. • **Default**—On selecting this option, the client obtains the IP address in the same subnet as the APs. By default, the client VLAN is assigned to the native VLAN on the wired network. • **Static**—On selecting this option, you need to specify a single VLAN, a comma separated list of VLANS, or a range of VLANs for all clients on this network. Select this option for configuring VLAN pooling. • **Dynamic**—On selecting this option, you can assign the VLANs dynamically from a DHCP server. To create VLAN assignment rules, click **New** to assign the user to a VLAN. In the **New VLAN Assignment Rule** window, enter the following information: – **Attribute**—Select an attribute returned by the RADIUS server during authentication. – **Operator**—Select an operator for matching the string. – **String**—Enter the string to match – **VLAN**—Enter the VLAN to be assigned.

9. Click **Next** to configure internal or external captive portal authentication, roles, and access rules for the guest users.

Note

If the client IP assignment mode is set to **Network assigned** in a guest SSID profile, the guest clients can log out of the captive portal network by accessing the https://securelogin.scalance.com/auth/logout.html URL.

In the CLI

To configure WLAN settings for an SSID profile:

```
(AP)(config)# wlan ssid-profile <name>

(AP)(SSID Profile <name>)# essid <ESSID-name>

(AP)(SSID Profile <name>)# type <Guest>

(AP)(SSID Profile <name>)# broadcast-filter <type>

(AP)(SSID Profile <name>)# dtim-period <number-of-beacons>

(AP)(SSID Profile <name>)# multicast-rate-optimization

(AP)(SSID Profile <name>)# dynamic-multicast-optimization

(AP)(SSID Profile <name>)# dmo-channel-utilization-threshold

(AP)(SSID Profile <name>)# a-max-tx-rate <rate>

(AP)(SSID Profile <name>)# a-min-tx-rate <rate>

(AP)(SSID Profile <name>)# g-max-tx-rate <rate>

(AP)(SSID Profile <name>)# g-min-tx-rate <rate>

(AP)(SSID Profile <name>)# zone <zone>
```

```
(AP)(SSID Profile <name>)# bandwidth-limit <limit>

(AP)(SSID Profile <name>)# per-user-bandwidth-limit <limit>

(AP)(SSID Profile <name>)# air-time-limit <limit>

(AP)(SSID Profile <name>)# wmm-background-share <percentage-of-traffic_share>

(AP)(SSID Profile <name>)# wmm-best-effort-share<percentage-of-traffic-share>

(AP)(SSID Profile <name>)# wmm-video-share <percentage-of-traffic_share>

(AP)(SSID Profile <name>)# wmm-voice-share <percentage-of-traffic_share>

(AP)(SSID Profile <name>)# rf-band {<2.4>|<5.0>|<all>}

(AP)(SSID Profile <name>)# content-filtering (AP)(SSID Profile <name>)# hide-ssid

(AP)(SSID Profile <name>)# inactivity-timeout <interval>

(AP)(SSID Profile <name>)# local-probe-req-thresh <threshold>

(AP)(SSID Profile <name>)# max-clients-threshold <number-of-clients>
```

To manually assign VLANs for WLAN SSID users:

```
(AP)(config)# wlan ssid-profile <name>

(AP)(SSID Profile <name>)# vlan <vlan-ID>
```

To create a new VLAN assignment rule:

```
(AP)(config)# wlan ssid-profile <name>

(AP)(SSID Profile <name>)# set-vlan <attribute>{equals|not-equals|starts-with|ends-
with|contains|matches-regular-expression} <operator> <VLAN-ID>|value-of}
```

13.3 Configuring Wired Profile for Guest Access

You can configure wired settings for a wired profile by using the SCALANCE W UI or the CLI.

In the SCALANCE W UI

1. Click the **Wired** link under **More** on the SCALANCE W main window. The **Wired** window is displayed.
2. Click **New** under **Wired Networks**. The **New Wired Network** window is displayed.
3. Click the **Wired Settings** tab and enter the following information:
   - **Name**—Specify a name for the profile.
   - **Primary Usage**—Select **Employee** or **Guest**.
   - **Speed/Duplex**—Ensure that appropriate values are selected for **Speed/Duplex**. Contact your network administrator if you need to assign speed and duplex parameters.
   - **POE**—Set **POE** to **Enabled** to enable PoE
   - **Status**—Ensure that an appropriate value is selected. The **Admin Status** indicates if the port is up or down.
   - **Content Filtering**—To ensure that all DNS requests to non-corporate domains on this wired network are sent to OpenDNS, select **Enabled** for **Content Filtering**.
   - **Uplink**—Select **Enabled** to configure uplink on this wired profile. If **Uplink** is set to **Enabled** and this network profile is assigned to a specific port, the port will be enabled as Uplink port. For more information on assigning a wired network profile to a port, see Assigning a Profile to Ethernet Ports (Page 133).
   - **Spanning Tree**—Select the **Spanning Tree** check box to enable STP on the wired profile. STP ensures that there are no loops in any bridged Ethernet network and operates on all downlink ports, regardless of forwarding mode. STP will not operate on the uplink port and is supported only on APs with three or more ports. By default Spanning Tree is disabled on wired profiles.
4. Click **Next**. The VLAN tab details are displayed.

5. Enter the following information.

   Mode—You can specify any of the following modes:

   – **Access**—Select this mode to allow the port to carry a single VLAN specified as the native VLAN.

   – **Trunk**—Select this mode to allow the port to carry packets for multiple VLANs specified as allowed VLANs.

   Specify any of the following values for **Client IP Assignment**:

   – **Virtual Controller Assigned**: Select this option to allow the virtual controller to assign IP addresses to the wired clients. When the virtual controller assignment is used, the source IP address is translated to the physical IP address of the master AP for all client traffic that goes through this interface. The virtual controller can also assign a guest VLAN to a wired client.

   – **Network Assigned**: Select this option to allow the clients to receive an IP address from the network to which the virtual controller is connected. On selecting this option, the **New** button to create a VLAN is displayed. Create a new VLAN if required.

   If the **Trunk** mode is selected:

   – Specify the **Allowed VLAN**, enter a list of comma separated digits or ranges: for example, 1,2,5 or 1– 4, or all. The Allowed VLAN refers to the VLANs carried by the port in Access mode.

   – If the **Client IP Assignment** is set to **Network Assigned**, specify a value for **Native VLAN**. A VLAN that does not have a VLAN ID tag in the frames is referred to as Native VLAN. You can specify a value within the range of 1–4093.

   If the **Access** mode is selected:

   – If the **Client IP Assignment** is set to **Virtual Controller Assigned**, proceed to step 2.

   – If the **Client IP Assignment** is set to **Network Assigned**, specify a value for **Access VLAN** to indicate the VLAN carried by the port in the **Access** mode

6. Click **Next** to configure internal or external captive portal authentication, roles, and access rules for the guest users.

In the CLI

To configure the settings for the wired profile:

```
(AP)(config)# wired-port-profile <name>

(AP)(wired ap profile <name>)# type <guest>

(AP)(wired ap profile <name>)# speed {10|100|1000|auto}

(AP)(wired ap profile <name>)# duplex {half|full|auto}

(AP)(wired ap profile <name>)# no shutdown

(AP)(wired ap profile <name>)# poe

(AP)(wired ap profile <name>)# uplink-enable

(AP)(wired ap profile <name>)# content-filtering

(AP)(wired ap profile <name>)# spanning-tree
```

To configure VLAN settings for a wired profile:

```
(AP)(config)# wired-port-profile <name>

(AP)(wired ap profile <name>)# switchport-mode {trunk|access}

(AP)(wired ap profile <name>)# allowed-vlan <vlan>

(AP)(wired ap profile <name>)# native-vlan {<guest|1…4095>}
```

To configure a new VLAN assignment rule:

```
(AP)(config)# wired-port-profile <name>

(AP)(wired ap profile <name>)# set-vlan <attribute>{equals|not-equals|starts-
with|ends-with|contains|matches-regular-expression} <operator> <VLAN-ID>|value-of}
```

13.4 Configuring Internal Captive Portal for Guest Network

For internal captive portal authentication, an internal server is used for hosting the captive portal service. You can configure internal captive portal authentication when adding or editing a guest network created for wireless or wired profile through the SCALANCE W UI or the CLI.

In the SCALANCE W UI

1. Navigate to the WLAN wizard or Wired window.
   – To configure internal captive portal authentication for a WLAN SSID, on the **Network** tab, click **New** to create a new network profile or **edit** to modify an existing profile.
   – To configure internal captive portal authentication for a wired profile, click **More > Wired**. In the **Wired** window, click **New** under **Wired Networks** to create a new network profile, or click **Edit** to select and modify an existing profile.
2. Click the **Security** tab and assign values for the Internal Captive Portal Configuration Parameters:

Parameter	Description
Splash page type	Select any of the following from the drop-down list. • **Internal - Authenticated**—When **Internal Authenticated** is enabled, the guest users are required to authenticate in the captive portal page to access the Internet. The guest users who are required to authenticate must already be added to the user database. • **Internal - Acknowledged**—When **Internal Acknowledged** is enabled, the guest users are required to accept the terms and conditions to access the Internet.Select any of the following from the drop-down list.
MAC authentication	Select **Enabled** from the **Mac Authentication** drop-down list to enable MAC authentication.
Delimiter character	Specify a character (for example, colon or dash) as a delimiter for the MAC address string. When configured, the AP will use the delimiter in the MAC authentication request. For example, if you specify colon as the delimiter, MAC addresses in the xx:xx:xx:xx:xx:xx format are used. If the delimiter is not specified, the MAC address in the xxxxxxxxxxxx format is used. **NOTE**: This option is available only when MAC authentication is enabled.

Parameter	Description
WISPr (Applicable for WLAN SSIDs only.)	Select **Enabled** if you want to enable WISPr authentication. For more information on WISPr authentication, see Configuring WISPr Authentication (Page 212). **NOTE:** The WISPr authentication is applicable only for Internal-Authenticated splash pages and is not applicable for wired profiles.
Auth server 1 Auth server 2	Select any one of the following: • A server from the list of servers, if the server is already configured. • **Internal Server** to authenticate user credentials at run time. • Select for configuring a new external RADIUS or LDAP server for authentication.
Load balancing	Select **Enabled** to enable load balancing if two authentication servers are used.
Reauth interval	Select a value to allow the APs to periodically reauthenticate all associated and authenticated client
Blacklisting (Applicable for WLAN SSIDs only.)	If you are configuring a wireless network profile, select **Enabled** to enable blacklisting of the clients with a specific number of authentication failures.
Accounting mode (Applicable for WLAN SSIDs only)	Select an accounting mode from the **Accounting mode** drop-down list for posting accounting information at the specified accounting interval. When the accounting mode is set to **Authentication**, the accounting starts only after client authentication is successful and stops when the client logs out of the network. If the accounting mode is set to **Association**, the accounting starts when the client associates to the network successfully and stops when the client is disconnected.
Accounting interval	Configure an accounting interval in minutes within the range of 0–60, to allow APs to periodically post accounting information to the RADIUS server.
Encryption (Applicable for WLAN SSIDs only.)	Select **Enabled** to configure encryption parameters. Select an encryption and configure a passphrase.

Parameter	Description
Splash Page Design	Under **Splash Page Visuals**, use the editor to specify display text and colors for the initial page that will be displayed to the users when they connect to the network. The initial page asks for user credentials or email, depending on the splash page type (Internal - Authenticated or Internal - Acknowledged). To customize the splash page design, perform the following steps: • To change the color of the splash page, click the **Splash page** rectangle and select the required color from the **Background Color** palette. • To change the welcome text, click the first square box in the splash page, type the required text in the **Welcome** text box, and click **OK**. Ensure that the welcome text does not exceed 127 characters. • To change the policy text, click the second square box in the splash page, type the required text in the **Policy** text box, and click **OK**. Ensure that the policy text does not exceed 255 characters. • To upload a custom logo, click **Upload your own custom logo Image**, browse the image file, and click **upload image**. Ensure that the image file size does not exceed 16 KB. • To redirect users to another URL, specify a URL in **Redirect URL**. • Click **Preview** to preview the captive portal page. **NOTE:** You can customize the captive portal page using double-byte characters. Traditional Chinese, Simplified Chinese, and Korean are a few languages that use double-byte characters. Click the banner, term, or policy in the **Splash Page Visuals** to modify the text in the red box. These fields accept double-byte characters or a combination of English and double-byte characters.

3. Click **Next** to configure access rules.

```
(AP)(SSID Profile <name>)# end
```

In the CLI

To configure internal captive portal authentication:

```
(AP)(config)# wlan ssid-profile <name>

(AP)(SSID Profile <name>)# essid <ESSID-name>

(AP)(SSID Profile <name>)# type <Guest>

(AP)(SSID Profile <name>)# captive-portal <internal-authenticated> exclude-
uplink{3G|4G|Wifi|Ethernet}

(AP)(SSID Profile <name>)# mac-authentication

(AP)(SSID Profile <name>)# auth-server <server1>

(AP)(SSID Profile <name>)# radius-reauth-interval <Minutes>
```

To configure internal captive portal for a wired profile:

```
(AP)(config)# wired-port-profile <name>

(AP)(wired ap profile <name>)# type <guest>

(AP)(wired ap profile <name>)# captive-portal {<internal-authenticated>|<internal-
acknowledged>} exclude-uplink{3G|4G|Wifi|Ethernet}

(AP)(wired ap profile <name>)# mac-authentication

(AP)(wired ap profile <name>)# auth-server <server1>
```

To customize internal captive portal splash page:

```
(AP)(config)# wlan captive-portal

(AP)(Captive Portal)# authenticated

(AP)(Captive Portal)# background-color <color-indicator>

(AP)(Captive Portal)# banner-color <color-indicator>

(AP)(Captive Portal)# banner-text <text>

(AP)(Captive Portal)# decoded-texts <text>

(AP)(Captive Portal)# redirect-url <url>

(AP)(Captive Portal)# terms-of-use <text>

(AP)(Captive Portal)# use-policy <text>
```

To upload a customized logo from a TFTP server to the AP:

```
(AP)# copy config tftp <ip-address> <filename> portal logo
```

13.5 Configuring External Captive Portal for Guest Network

13.5.1 External Captive Portal Profiles

You can now configure external captive portal profiles and associate these profiles to a user role or SSID. You can create a set of captive portal profiles in the **External Captive Portal** window (accessed from the **Security** tab) and associate these profiles with an SSID or a wired profile. You can also create a new captive portal profile on the **Security** tab of the WLAN wizard or a Wired Network window. In the current release, you can configure up to 16 external captive portal profiles.

When the captive portal profile is associated to an SSID, it is used before user authentication. If the profile is associated to a role, it is used only after the user authentication. When a captive portal profile is applied to an SSID or wired profile, the users connecting to the SSID or wired network are assigned a role with the captive portal rule. The guest user role allows only DNS and DHCP traffic between the client and the network, and directs all HTTP or HTTPS requests to the captive portal unless explicitly permitted to allow all types of traffic.

13.5.2 Creating a Captive Portal Profile

You can create a captive portal profile using the SCALANCE W UI or the CLI.

In the SCALANCE W UI

1. **Go to** Security > External Captive Portal.
2. Click **New**. The **New** popup window is displayed.
3. Specify values for the following Captive Portal Profile Configuration Parameters:

Parameter	**Description**
Name	Enter a name for the profile.
Type	Select any one of the following types of authentication: l **Radius Authentication**—Select this option to enable user authentication against a RADIUS server. l **Authentication Text**—Select this option to specify an authentication text. The specified text will be returned by the external server after a successful user authentication.

Parameter	Description
IP or hostname	Enter the IP address or the host name of the external splash page server.
URL	Enter the URL for the external captive portal server.
Port	Enter the port number.
Use https (Available only if RADIUS Authentication is selected)	Select **Enabled** to enforce clients to use HTTPS to communicate with the captive portal server.
Captive Portal failure	Allows you to configure Internet access for the guest clients when the external captive portal server is not available. Select **Deny Internet** to prevent clients from using the network, or **Allow Internet** to allow the guest clients to access Internet when the external captive portal server is not available.
Automatic URL Whitelisting	Select **Enabled** to enable the automatic whitelisting of URLs. On selecting the check box for the external captive portal authentication, the URLs that are allowed for the unauthenticated users to access are automatically whitelisted. The automatic URL whitelisting is disabled by default.
Auth Text (Available only if Authentication Text is selected)	If the External Authentication splash page is selected, specify the authentication text to be returned by the external server after successful authentication.
Server Offload	Select **Enabled** to enable server offload. The server offload feature ensures that the non-browser client applications are not unnecessarily redirected to the external portal server and thereby reducing the load on the external captive portal server. The **Server Offload** option is **Disabled** by default.
Prevent frame overlay	When the **Prevent frame overlay** option is enabled, a frame can display a page only if it is in the same domain as the main page. This option is **Enabled** by default and can be used to prevent the overlay of frames.
Switch IP	Sends the IP address of the Virtual controller in the redirection URL when external captive portal servers are used. This option is disabled by default.
Redirect URL	Specify a redirect URL if you want to redirect the users to another URL.

In the CLI

To configure an external captive portal profile:

```
(AP)(config)# wlan external-captive-portal [profile_name]

(AP)(External Captive Portal)# server <server>

(AP)(External Captive Portal)# port <port>

(AP)(External Captive Portal)# url <url>

(AP)(External Captive Portal)# https

(AP)(External Captive Portal)# redirect-url <url>

(AP)(External Captive Portal)# server-fail-through (AP)(External Captive Portal)# no
auto-whitelist-disable (AP)(External Captive Portal)# server-offload

(AP)(External Captive Portal)# switch-ip

(AP)(External Captive Portal)# prevent-frame-overlay

(AP)(External Captive Portal)# end

(AP)# commit apply
```

13.5.3 Configuring an SSID or Wired Profile to Use External Captive Portal Authentication

You can configure external captive portal authentication when adding or editing a guest network profile using the SCALANCE W UI or the CLI.

In the SCALANCE W UI

1. Navigate to the WLAN wizard or Wired window.
   - To configure external captive portal authentication for a WLAN SSID, on the **Network** tab, click **New** to create a new network profile or **edit** to modify an existing profile.
   - To configure external captive portal authentication for a wired profile, Go to **More > Wired**. In the **Wired** window, click **New** under **Wired Networks** to create a new network, or click **Edit** to select an existing profile.
2. On the **Security** tab, select **External** from the **Splash page type** drop-down list.
3. From the **Captive Portal Profile** drop-down list, select a profile. You can select and modify a default profile, or an already existing profile, or click **New** and create a new profile.

4. Configure the following external Captive Portal configuration parameters based on the type of splash page you selected.

Parameter	Description
Captive-portal proxy server	If required, configure a captive portal proxy server or a global proxy server to match your browser configuration by specifying the IP address and port number in the **Captive-portal proxy server** text box.
WISPr	Select **Enabled** if you want to enable WISPr authentication. For more information on WISPr authentication, see Configuring WISPr Authentication (Page 212). **NOTE:** The WISPr authentication is applicable only for the **External** and **Internal- Authenticated** splash pages and is not applicable for wired profiles.
MAC authentication	Select **Enabled** if you want to enable MAC authentication. For information on MAC authentication, see Configuring MAC Authentication for a Network Profile (Page 206).
Delimiter character	Specify a character (for example, colon or dash) as a delimiter for the MAC address string. When configured, the AP will use the delimiter in the MAC authentication request. For example, if you specify colon as the delimiter, MAC addresses in the xx:xx:xx:xx:xx:xx format are used. If the delimiter is not specified, the MAC address in the xxxxxxxxxxxx format is used. **NOTE:** This option is available only when MAC authentication is enabled.
Uppercase support	Set to **Enabled** to allow the AP to use uppercase letters in MAC address string for MAC authentication. **NOTE:** This option is available only if MAC authentication is enabled.
Authentication server	To configure an authentication server, select any of the following options: • If the server is already configured, select the server from the list. • To create new external RADIUS server, select **New**. For more information, see Configuring an External Server for Authentication (Page 188).
Reauth interval	Specify a value for the reauthentication interval at which the APs periodically reauthenticate all associated and authenticated clients.
Accounting mode	Select an accounting mode from the **Accounting mode** drop-down list for posting accounting information at the specified **Accounting interval**. When the accounting mode is set to **Authentication**, the accounting starts only after client authentication is successful and stops when the client logs out of the network. If the accounting mode is set to **Association**, the accounting starts when the client associates to the network successfully and stops when the client is disconnected.
Accounting interval	Configure an accounting interval in minutes within the range of 0–60, to allow APs to periodically post accounting information to the RADIUS server.
Blacklisting	If you are configuring a wireless network profile, select **Enabled** to enable blacklisting of the clients with a specific number of authentication failures.

Parameter	Description
Max authentication failures	If you are configuring a wireless network profile and **Blacklisting** is enabled, specify the maximum number of authentication failures after which users who fail to authenticate must be dynamically blacklisted.
Walled garden	Click the link to open the **Walled Garden** window. The walled garden configuration determines access to the websites. For more information, see Configuring Walled Garden Access (Page 169).
Disable if uplink type is	Select the type of the uplink to exclude.
Encryption	Select Enabled to configure encryption settings and specify the encryption parameters.

5. Click **Next** to continue and then click **Finish** to apply the changes.

In the CLI

To configure security settings for guest users of the WLAN SSID profile:

```
(AP)(config)# wlan ssid-profile <name>

(AP)(SSID Profile <name>)# essid <ESSID-name>

(AP)(SSID Profile <name>)# type <Guest>

(AP)(SSID Profile <name>)# captive-portal{<type>[exclude-uplink <types>]|external
[exclude-uplink <types>| profile <name>[exclude-uplink <types>]]}

(AP)(SSID Profile <name>)# captive-portal-proxy-server <IP> <port>

(AP)(SSID Profile <name>)# blacklist

(AP)(SSID Profile <name>)# mac-authentication

(AP)(SSID Profile <name>)# max-authentication-failures <number>

(AP)(SSID Profile <name>)# auth-server <server-name>

(SCALANCE W Access Point (SSID Profile <name>)# radius-accounting

(SCALANCE W Access Point (SSID Profile <name>)# radius-interim-accounting-interval

(SCALANCE W Access Point (SSID Profile <name>)# radius-accounting-mode {user-
association|user- authentication}

(AP)(SSID Profile <name>)# wpa-passphrase <WPA_key>

(AP)(SSID Profile <name>)# wep-key <WEP-key> <WEP-index>

(AP)(SSID Profile <name>)# end

(AP)# commit apply
```

To configure security settings for guest users of the wired profile:

```
(AP)(config)# wired-port-profile <name>

(AP)(wired ap profile <name>)# type <Guest>

(AP)(wired ap profile <name>)# captive-portal{<type>[exclude-uplink <types>]|external
[exclude-uplink <types>| profile <name>[exclude-uplink <types>]]}

(AP)(wired ap profile <name>)# mac-authentication

(AP)(wired ap profile <name>)# end

(AP)# commit apply
```

13.5.4 External Captive Portal Redirect Parameters

If the external captive portal redirection is enabled on a network profile, AP sends an HTTP response with the redirect URL to display the splash page and enforce captive portal authentication by clients. The HTTP response from the AP includes the following parameters:

Table 13- 1 External Captive Portal Redirect Parameters

Parameter	Example Value	Description
cmd	login	Type of operation
mac	34:02:86:c6:d2:3e	Client MAC address
essid	guest-ecp-109	ESSID
ip	192.0.2.0	Client IP address
apname	9c:1c:12:cb:a2:90	AP host name
apmac	9c:1c:12:cb:a2:90	AP MAC address
vcname	scalance-C8:1D:DA"	Virtual controller name
url	http://www.google.com/	original URL

13.5.5 Configuring External Captive Portal Authentication Using ClearPass Guest

You can configure SCALANCE W to point to ClearPass Guest as an external captive portal server. With this configuration, the user authentication is performed by matching a string in the server response and that in the RADIUS server (either ClearPass Guest or a different RADIUS server).

Creating a Web Login Page in ClearPass Guest

The ClearPass Guest Visitor Management Appliance provides a simple and personalized UI through which operational staff can quickly and securely manage visitor network access. With ClearPass Guest, the users can have a controlled access to a dedicated visitor management user database. Through a customizable web portal, the administrators can easily create an account, reset a password, or set an expiry time for visitors. Visitors can be registered at reception and provisioned with an individual guest account that defines the visitor profile and the duration of their visit. By defining a web login page on the ClearPass Guest Visitor Management Appliance, you can to provide a customized graphical login page for visitors accessing the network.

Configuring RADIUS Server in SCALANCE W UI

To configure SCALANCE W to point to ClearPass Guest as an external captive portal server:

1. Select the WLAN SSID for which you want to enable external captive portal authentication with ClearPass Policy Manager. You can also configure the RADIUS server when configuring a new SSID profile.
2. On the **Security** tab, select **External** from the **Splash page type** drop-down list.
3. Select **New** from the **Captive portal profile** drop-down list and update the following:
   – Enter the IP address of the ClearPass Guest server in the **IP or hostname** text box. Obtain the ClearPass Guest IP address from your system administrator.
   – Enter **/page_name.php** in the **URL** text box. This URL must correspond to the **Page Name** configured in the ClearPass Guest RADIUS Web Login page. For example, if the Page Name is **Siemens**, the URL should be **/siemens.php** in the SCALANCE W UI.
   – Enter the **Port** number (generally should be **80**). The ClearPass Guest server uses this port for HTTP services.
   – Click **OK**.
4. To create an external RADIUS server, select **New** from the **Authentication server 1** drop-down list. For information on authentication server configuration parameters, see Configuring an External Server for Authentication (Page 188).
5. Click **Next** and then click **Finish**.
6. Click the updated SSID in the **Network** tab.
7. Open any browser and type any URL. SCALANCE W redirects the URL to ClearPass Guest login page.
8. Log in to the network with the username and password specified while configuring the RADIUS server.

Configuring RADIUS Attribute for ClearPass Policy Manager Server Load Balancing

The administrators can configure a RADIUS server IP address as one of the parameters on ClearPass Policy Manager server for external captive portal user authentication. Configuring a RADIUS server attribute for guest user authentication allows the administrators to balance the load on the ClearPass Policy Manager servers.

When the RADIUS server IP address is configured under **Extra Fields** in the ClearPass Guest login page, the RADIUS server IP parameter is submitted to the server as part of the HTTP or HTTPS POST data when the guest users initiate an HTTP or HTTPS request. The AP intercepts this information to perform the actual RADIUS authentication with the server IP defined in the POST message.

13.6 Configuring Facebook Login

SCALANCE W supports the Facebook Wi-Fi feature that allows the captive portal clients using a Facebook account to authenticate on an AP. You can configure a guest network to use a customized Facebook page as an external captive portal URL and allow the AP to redirect clients to a Facebook page when it receives an HTTP request. The users can select the appropriate option to authenticate and access the Internet. By configuring the Facebook login feature, businesses can pair their network with the Facebook Wi-Fi service, so that the users logging into Wi-Fi hotspots are presented with a business page, before gaining access to the network.

The Facebook Wi-Fi integration with the AP includes the following procedures::

- Setting up a Facebook Page (Page 163)
- Configuring an SSID (Page 163)
- Configuring the Facebook Portal Page (Page 164)
- Accessing the Portal Page (Page 165)

13.6.1 Setting up a Facebook Page

To enable integration with the AP, ensure that you have a Facebook page created as a local business with a valid location.

- For more information on creating a Facebook page, see the online help available at https://www.facebook.com/help.
- For more information on setting up and using Facebook Wi-Fi service, see https://www.facebook.com/help/126760650808045.

13.6.2 Configuring an SSID

You can a configure guest network profile and enable Facebook login through the SCALANCE W UI or the CLI.

In the SCALANCE W UI

To enable Facebook login:

1. Navigate to **Network > New** to create a new network profile.
2. Enter a name for the SSID.
3. Select **Guest** under **Primary usage**.
4. Configure other required parameters in the **WLAN Settings** and **VLAN** tabs.
5. On the **Security** tab, select **Facebook** from the **Splash page type** drop-down list.
6. Click **Next**. The **Access** tab contents are displayed.
7. Click **OK**. The SSID with the Facebook option is created. After the SSID is created, the AP automatically registers with Facebook. If the AP registration is successful, the **Facebook configuration** link is displayed in the **Security** tab of the WLAN wizard.

In the CLI

To configure an account for captive portal authentication:

```
(AP)(config)# wlan ssid-profile <name>
```

```
(AP)(SSID Profile <name>)# captive-portal {<type>[exclude-uplink <types>]|external
[exclude-uplink <types>|profile <name>[exclude-uplink <types>]]}
```

Example

The following example configures a Facebook account for captive portal authentication:

```
(AP)(config)# wlan ssid-profile guestNetwork
```

```
(AP)(SSID Profile "guestNetwork")# captive-portal facebook
```

13.6.3 Configuring the Facebook Portal Page

To bind the virtual controller with the Facebook portal:

1. Open the SSID with the Facebook option enabled, navigate to the **Security** tab and click the **Facebook configuration** link. The Facebook page is displayed

Note

The **Facebook configuration** link is displayed only if the AP is successfully registered with Facebook.

2. Log in with your Facebook credentials. The **Facebook Wi-Fi Configuration** page is displayed.
3. Select the Facebook page.
4. Under **Bypass Mode**, select any of the following options:
   - **Skip Check-in link**—When selected, the users are not presented with your business Facebook page, but are allowed to access the Internet by clicking the **Skip Check-in** link.
   - **Require Wi-Fi code**—When selected, the users are assigned a Wi-Fi code to gain access to the Facebook page.

5. Customize the session length and terms of service if required.
6. Click **Save Settings**.

13.6.4 Accessing the Portal Page

To access the portal page:

1. Connect to the SSID with the Facebook option enabled.
2. Launch a web browser. The browser opens the Facebook Wi-Fi page. If the Wi-Fi-code based login is enabled, the users are prompted to enter the Wi-Fi code. If the **Skip Check-in** link is displayed, click the link to skip checking in to the Facebook business page and proceed to access the Internet.
3. If you want to check in the business page, click **Check In** and provide your credentials. After checking in, click **Continue Browsing** to access the web page that was originally requested.

13.7 Configuring Guest Logon Role and Access Rules for Guest Users

For captive portal profile, you can create any the following types of roles:

- A pre-authenticated role—This role is assigned before the captive portal authentication. The user can only access certain destinations with this role.
- A guest role—This role is assigned after user authentication.
- A captive-portal role—This role can be assigned to any network such as Employee, Voice, or Guest. When the user is assigned with this role, a splash page is displayed after opening a browser and the users may need to authenticate.

You can configure up to 128 access rules for guest user roles through the SCALANCE W UI or the CLI.

In the SCALANCE W UI

To configure roles and access rules for the guest network:

1. On the **Access Rules** tab, set the slider to any of the following types of access control:
   - **Unrestricted**—Select this to set unrestricted access to the network.
   - **Network-based**—Set the slider to **Network-based** to set common rules for all users in a network. The **Allow any to all destinations** access rule is enabled by default. This rule allows traffic to all destinations. To define an access rule:

     Click **New**.

     Select appropriate options in the **New Rule** window.

     Click **OK**.
   - **Role-based**—Select **Role-based** to enable access based on user roles.

     For role-based access control:

     Create a user role if required. For more information, see Configuring User Roles (Page 237).

     Create access rules for a specific user role. For more information, see Configuring ACL Rules for Network Services (Page 220). You can also configure an access rule to enforce captive portal authentication for an SSID with the 802.1X authentication method. For more information, see Configuring Captive Portal Roles for an SSID (Page 167).

     Create a role assignment rule. For more information, see Configuring Derivation Rules (Page 240). SCALANCE W supports role derivation based on the DHCP option for captive portal authentication. When the captive portal authentication is successful, a new user role is assigned to the guest users based on DHCP option configured for the SSID profile instead of the pre-authenticated role.
2. Click **Finish.**

In the CLI

To configure access control rules for a WLAN SSID:

```
(AP)(config)# wlan access-rule <name>
```

```
(AP)(Access Rule <name>)# rule <dest> <mask> <match> {<protocol> <start-port> <end-port> {permit|deny|src-nat|dst-nat{<IP-address> <port>|<port>}}| app <app> {permit|deny}| appcategory <appgrp>|webcategory <webgrp> {permit|deny}|webreputation <webrep> [<option1....option9>]
```

To configure access control rules based on the SSID:

```
(AP)(config)# wlan ssid-profile <name> (AP)(SSID Profile <name>)# set-role-by-ssid
```

To configure role assignment rules:

```
(AP)(config)# wlan ssid-profile <name>
```

```
(AP)(SSID Profile <name>)# set-role <attribute>{{equals|not-equals|starts-with|ends-with|contains|matches-regular-expression}<operator><role>|value-of}
```

To configure a pre-authentication role:

```
(AP)(config)# wlan ssid-profile <name>
```

```
(AP)(SSID Profile <name>)# set-role-pre-auth <role>
```

To configure machine and user authentication roles:

```
(AP)(config)# wlan ssid-profile <name>
```

```
(AP)(SSID Profile <name>)# set-role-machine-auth <machine_only> <user_only>
```

To configure unrestricted access:

```
(AP)(config)# wlan ssid-profile <name>
```

```
(AP)(SSID Profile <name>)# set-role-unrestricted
```

Example

The following example configures access rules for the wireless network:

```
(AP)(config)# wlan access-rule WirelessRule
```

13.8 Configuring Captive Portal Roles for an SSID

You can configure an access rule to enforce captive portal authentication for SSIDs that use 802.1X authentication to authenticate clients. You can configure rules to provide access to external or internal captive portal, so that some of the clients using this SSID can derive the captive portal role.

The following conditions apply to the 802.1X and captive portal authentication configuration:

- If a user role does not have captive portal settings configured, the captive portal settings configured for an SSID are applied to the client's profile.
- If the SSID does not have captive portal settings configured, the captive portal settings configured for a user role are applied to the client's profile.
- If captive portal settings are configured for both SSID and user role, the captive portal settings configured for a user role are applied to the client's profile

You can create a captive portal role for both **Internal** and **External** splash page types. To enforce the captive portal role, use the SCALANCE W UI or the CLI.

In the SCALANCE W UI

To create a captive portal role:

1. Select an SSID profile from the **Network** tab. The **Edit <WLAN-Profile>** window is displayed.
2. On the **Access** tab, move the slider to **Role-based** access control by using the scroll bar.
3. Select a role or create a new one if required.
4. Click **New** to add a new rule. The **New Rule** window is displayed.

5. In the **New Rule** window, specify the following parameters. The following figures show the parameters for captive portal role configuration:

Parameter	**Description**
Rule type	Select **Captive Portal** from the Rule Type drop-down list.
Splash Page Type	Select any of the following attributes: • Select **Internal** to configure a rule for internal captive portal authentication. • Select **External** to configure a rule for external captive portal authentication.
Internal	If **Internal** is selected as splash page type, perform the following steps: • Under **Splash Page Visuals**, use the editor to specify display text and colors for the initial page that would be displayed to users connecting to the network. The initial page asks for user credentials or email, depending on the splash page type configured. • To change the color of the splash page, click the **Splash page** rectangle and select the required color from the **Background Color** palette. • To change the welcome text, click the first square box in the splash page, type the required text in the **Welcome** text box, and then click **OK**. Ensure that the welcome text does not exceed 127 characters. • To change the policy text, click the second square box in the splash page, type the required text in the **Policy** text box, and click **OK**. Ensure that the policy text does not exceed 255 characters. • Specify the URL to which you want to redirect the guest users. • To upload a custom logo, click **Upload your own custom logo Image**, browse the image file, and click **upload image**. • To preview the captive portal page, click **Preview**.

Parameter	Description
External	If **External** is selected, perform the following steps: • Select a profile from the **Captive portal profile** drop-down list. • If you want to edit the profile, click **Edit** and update the following parameters: – **Type**—Select either **Radius Authentication** (to enable user authentication against a RADIUS server) or **Authentication Text** (to specify the authentication text to be returned by the external server after a successful user authentication). – **IP or hostname**— Enter the IP address or the host name of the external splash page server. – **URL**— Enter the URL for the external splash page server. – **Port**—Enter the port number. – **Redirect URL**—Specify a redirect URL if you want to redirect the users to another URL. – **Captive Portal failure**—The **Captive Portal failure** drop- down list allows you to configure Internet access for the guest clients when the external captive portal server is not available. Select **Deny Internet** to prevent clients from using the network, or **Allow Internet** to allow the guest clients to access Internet when the external captive portal server is not available. – **Automatic URL Whitelisting**—Select **Enabled** or **Disabled** to enable or disable automatic whitelisting of URLs. On selecting the check box for the external captive portal authentication, the URLs allowed for the unauthenticated users to access are automatically whitelisted. The automatic URL whitelisting is disabled by default. – **Auth Text**—Indicates the authentication text returned by the external server after a successful user authentication.

6. Click **OK**. The enforce captive portal rule is created and listed as an access rule.
7. Create a role assignment rule based on the user role to which the captive portal access rule is assigned.
8. Click **Finish.**

The client can connect to this SSID after authenticating with username and password. After a successful user login, the captive portal role is assigned to the client.

In the CLI

To create a captive portal role:

```
(AP)(config)# wlan access-rule <Name>

(AP)(Access Rule <Name>)# captive-portal {external [profile <name>]|internal}
```

13.9 Configuring Walled Garden Access

On the Internet, a walled garden typically controls access to web content and services. The walled garden access is required when an external captive portal is used. For example, a hotel environment where the unauthenticated users are allowed to navigate to a designated login page (for example, a hotel website) and all its contents.

The users who do not sign up for the Internet service can view the allowed websites (typically hotel property websites). The website names must be DNS-based and support the option to define wildcards. When a user attempts to navigate to other websites that are not in the whitelist of the walled garden profile, the user is redirected to the login page. AP supports walled garden only for the HTTP requests. For example, if you add yahoo.com in walled garden whitelist and the client sends an HTTPS request (https://yahoo.com), the requested page is not displayed and the users are redirected to the captive portal login page.

In addition, a blacklisted walled garden profile can also be configured to explicitly block the unauthenticated users from accessing some websites.

You can create a walled garden access in SCALANCE W UI or the CLI.

In the SCALANCE W UI

1. Click the **Security** link at the top of the SCALANCE W main window. The **Security** window is displayed.
2. Click **Walled Garden**. The **Walled Garden** tab contents are displayed.
3. To allow the users to access a specific domain, click **New** and enter the domain name or URL in the **Whitelist** section of the window. This allows access to a domain while the user remains unauthenticated. Specify a POSIX regular expression (regex(7)). For example:
   – yahoo.com matches various domains such as news.yahoo.com, travel.yahoo.com and finance.yahoo.com
   – www.apple.com/library/test is a subset of www.apple.com site corresponding to path /library/test/*
   – favicon.ico allows access to /favicon.ico from all domains.
4. To deny users access to a domain, click New and enter the domain name or URL in the Blacklist section of the window. This prevents the unauthenticated users from viewing specific websites. When a URL specified in the blacklist is accessed by an unauthenticated user, AP sends an HTTP 403 response to the client with an error message. If the requested URL does not appear on the blacklist or whitelist, the request is redirected to the external captive portal.
5. To modify the list, select the domain name or URL and click **Edit** . To remove an entry from the list, select the URL from the list and click **Delete**.
6. Click **OK** to apply the changes.

In the CLI

To create a walled garden access:

```
(AP)(config)# wlan walled-garden

(AP)(Walled Garden)# white-list <domain>

(AP)(Walled Garden)# black-list <domain>
```

13.9.1 Disabling Captive Portal Authentication

To disable captive portal authentication:

1. Select a wireless or wired profile. Depending on the network profile selected, the **Edit <WLAN-Profile>** or **Edit Wired Network** window is displayed.

Note

You can also customize splash page design on the **Security** tab of **New WLAN** (WLAN wizard) and **New Wired Network** (wired profile window) when configuring a new profile

2. Navigate to the **Security** tab.
3. Select **None** from the **Splash page type** drop-down list. Although the splash page is disabled, you can enable MAC authentication, configure authentication servers, set accounting parameters, blacklist clients based on MAC authentication failures, and configure encryption keys for authorized access.
4. If required, configure the security parameters
5. Click **Next** and then click **Finish** to apply the changes

Authentication and User Management 14

14.1 Managing AP Users

The AP users can be classified as follows:

- Administrator—An admin user who creates SSIDs, wired profiles, and DHCP server configuration parameters; and manages the local user database. The admin users can access the virtual controller Management UI.
- Guest administrator—A guest interface management user who manages guest users added in the local user database.
- Administrator with read-only access—The read-only admin user does not have access to the SCALANCE W CLI. The SCALANCE W UI will be displayed in the read-only mode for these users.
- Employee users—Employees who use the enterprise network for official tasks.
- Guest users—Visiting users who temporarily use the enterprise network to access the Internet.

The user access privileges are determined by AP management settings in the AirWave Management client, and the type of the user. The following table outlines the access privileges defined for the admin user, guest management interface admin, and read-only users

Table 14- 1 User Privileges

User Category	AMP in Management Mode	AP in Monitor Mode or without AMP
administrator	Access to local user database only	Complete access to the AP
read-only administrator	No write privileges	No write privileges
guest administrator	Access to local user database only	Access to local user database only

14.1.1 Configuring AP Users

The SCALANCE W user database consists of a list of guest and employee users. The addition of a user involves specifying the login credentials for a user. The login credentials for these users are provided outside the SCALANCE W system.

A guest user can be a visitor who is temporarily using the enterprise network to access the Internet. However, if you do not want to allow access to the internal network and the Intranet, you can segregate the guest traffic from the enterprise traffic by creating a guest WLAN and specifying the required authentication, encryption, and access rules.

An employee user is the employee who is using the enterprise network for official tasks. You can create Employee WLANs, specify the required authentication, encryption and access rules, and allow the employees to use the enterprise network.

Note

The user database is also used when an AP is configured as an internal RADIUS server

---

Note

The local user database of APs can support up to 512 user entries.

In the SCALANCE W UI

To configure users:

1. Click the **Security** link located directly above the Search bar in the SCALANCE W main window.
2. Click **Users for Internal Server**, to view the contents of the **Users for Internal Server** tab.
3. Enter the user name in the **Username** text box.
4. Enter the password in the **Password** text box and reconfirm.
5. Select the type of network from the **Type** drop-down list.
6. Click **Add** and click **OK.** The users are listed in the **Users** list.

To edit user settings:

1. Select the user you want to modify from the **Users** list in the table.
2. Click **Edit** to modify user settings.
3. Click **OK**.

To delete a user:

1. Select the user you want to delete from the **Users** list in the table.
2. Click **Delete**.
3. Click **OK**.

To delete all or multiple users at a time:

1. Select multiple users you want to delete from the **Users** list in the table.
2. Click **Delete All**.
3. Click **OK**.

Note

Deleting a user only removes the user record from the user database, and will not disconnect the online user associated with the user name.

In the CLI

To configure an employee user:

```
(AP)(config)# user <username> <password> radius
```

To configure a guest user:

```
(AP)(config)# user <username> <password> portal
```

14.1.2 Configuring Authentication Parameters for Management Users

You can configure RADIUS or TACACS authentication servers to authenticate and authorize the management users of an AP. The authentication servers determine if the user has access to administrative interface. The privilege level for different types of management users is defined on the RADIUS or TACACS server instead of the AP. The APs map the management users to the corresponding privilege level and provide access to the users based on the attributes returned by the RADIUS or TACACS server.

You can configure authentication parameters for local admin, read-only, and guest management administrator account settings through the SCALANCE W UI or the CLI.

In the SCALANCE W UI

1. Navigate to **System > Admin**. The **Admin** tab details are displayed.

Type of User	Authentication Options	Steps to Follow
Local administrator	Internal	Select **Internal** if you want to specify a single set of user credentials. If using an internal authentication server: 1. Specify the **Username** and **Password**. 2. Retype the password to confirm.
	Authentication server	Select the RADIUS or TACACS authentication servers. You can also create a new server by selecting **New** from the **Authentication server** drop-down list. • **Authentication server w/ fallback to internal**— Select **Authentication server w/ fallback to internal** option if you want to use both internal and external servers. When enabled, the authentication switches to **Internal** if there is no response from the RADIUS server (RADIUS server timeout). To use this option, select the authentication servers and configure the user credentials for internal-server- based authentication. • **Load balancing**—If two servers are configured, users can use them in the primary or backup mode, or load balancing mode. To enable load balancing, select **Enabled** from the **Load balancing** drop-down list. For more information on load balancing, see Dynamic Load Balancing between Two Authentication Servers (Page 187) . • **TACACS accounting**—If a TACACS server is selected, enable **TACACS accounting** to report management commands if required.

Type of User	Authentication Options	Steps to Follow
Administrator with Read-Only Access	Internal	Select **Internal** to specify a single set of user credentials. If using an internal authentication server: 1. Specify the **Username** and **Password**. 2. Retype the password to confirm.
	Authentication server	If a RADIUS or TACACS server is configured, select **Authentication server** for authentication.
Guest	Internal	Select **Internal** to specify a single set of user credentials. If using an internal authentication server: 1. Specify the **Username** and **Password**. 2. Retype the password to confirm.
	Authentication server	If a RADIUS or TACACS server is configured, select **Authentication server** for authentication.

2. Click **OK**.

In the CLI

To configure a local admin user:

```
(AP)(config)# mgmt-user <username> [password]
```

To configure guest management administrator credentials:

```
(AP)(config)# mgmt-user <username> [password] guest-mgmt
```

To configure a user with read-only privilege:

```
(AP)(config)# mgmt-user <username> [password] read-only
```

To configure management authentication settings:

```
(AP)(config)# mgmt-auth-server <server1>

(AP)(config)# mgmt-auth-server <server2>

(AP)(config)# mgmt-auth-server-load-balancing

(AP)(config)# mgmt-auth-server-local-backup
```

To enable TACACS accounting:

```
(AP)(config)# mgmt-accounting command all
```

14.1.3 Adding Guest Users through the Guest Management Interface

To add guest users through the Guest Management interface:

1. Log in to the SCALANCE W UI with the guest management interface administrator credentials. The guest management interface is displayed.
2. To add a user, click **New**. The **New Guest User** popup window is displayed.
3. Specify a **Username** and **Password**.
4. Retype the password to confirm.
5. Click **OK**.

14.2 Supported Authentication Methods

Authentication is a process of identifying a user through a valid username and password or based on the user's MAC addresses. The following authentication methods are supported in SCALANCE W:

- 802.1X Authentication
- MAC Authentication
- MAC Authentication with 802.1X Authentication
- Captive Portal Authentication
- MAC Authentication with Captive Portal Authentication
- 802.1X Authentication with Captive Portal Role
- WISPr Authentication

802.1X Authentication

802.1X is an IEEE standard that provides an authentication framework for WLANs. The 802.1X standard uses the EAP to exchange messages during the authentication process. The authentication protocols that operate inside the 802.1X framework include EAP-TLS, PEAP, and EAP-TTLS. These protocols allow the network to authenticate the client while also allowing the client to authenticate the network. For more information on EAP authentication framework supported by the APs, see Supported EAP Authentication Frameworks (Page 181).

The 802.1X authentication method allows an AP to authenticate the identity of a user before providing network access to the user. The RADIUS protocol provides centralized authentication, authorization, and accounting management. For authentication purpose, the wireless client can associate to a NAS or RADIUS client such as a wireless AP. The wireless client can pass data traffic only after a successful 802.1X authentication. SCALANCE W supports the IMSI authentication process for device encryption. The EAP-AKA protocol is used with 802.1X to authenticate client access to a client network. The EAP-AKA makes use of IMSI as a permanent identity in the authentication exchange. It is a unique encryption method that is used to track device movement and protect user privacy.

For more information on configuring an AP to use 802.1X authentication, see Configuring 802.1X Authentication for a Network Profile (Page 202).

MAC Authentication

MAC authentication is used for authenticating devices based on their physical MAC addresses. MAC authentication requires that the MAC address of a machine matches a manually defined list of addresses. This authentication method is not recommended for scalable networks and the networks that require stringent security settings. For more information on configuring an AP to use MAC authentication, see Configuring MAC Authentication for a Network Profile (Page 206).

MAC Authentication with 802.1X Authentication

This authentication method has the following features:

- MAC authentication precedes 802.1X authentication—The administrators can enable MAC authentication for 802.1X authentication. MAC authentication shares all the authentication server configurations with 802.1X authentication. If a wireless or wired client connects to the network, MAC authentication is performed first. If MAC authentication fails, 802.1X authentication does not trigger. If MAC authentication is successful, 802.1X authentication is attempted. If 802.1X authentication is successful, the client is assigned an 802.1X authentication role. If 802.1X authentication fails, the client is assigned a **deny-all** role or **mac-auth-only** role.
- MAC authentication only role—Allows you to create a **mac-auth-only** role to allow role-based access rules when MAC authentication is enabled for 802.1X authentication. The **mac-auth-only** role is assigned to a client when the MAC authentication is successful and 802.1X authentication fails. If 802.1X authentication is successful, the **mac-auth-only** role is overwritten by the final role. The **mac-auth-only** role is primarily used for wired clients.
- L2 authentication fall-through—Allows you to enable the **l2-authentication-fallthrough** mode. When this option is enabled, the 802.1X authentication is allowed even if the MAC authentication fails. If this option is disabled, 802.1X authentication is not allowed. The **l2-authentication-fallthrough** mode is disabled by default.

For more information on configuring an AP to use MAC as well as 802.1X authentication, see Configuring MAC Authentication with 802.1X Authentication (Page 209).

Captive Portal Authentication

Captive portal authentication is used for authenticating guest users. For more information on captive portal authentication, see Captive Portal for Guest Access. (Page 139)

MAC Authentication with Captive Portal Authentication

You can enforce MAC authentication for captive portal clients. For more information on configuring an AP to use MAC authentication with captive portal authentication, see Configuring MAC Authentication with Captive Portal Authentication (Page 211).

802.1X Authentication with Captive Portal Role

This authentication mechanism allows you to configure different captive portal settings for clients on the same SSID. For example, you can configure an 802.1X SSID and create a role for captive portal access, so that some of the clients using the SSID derive the captive portal role. You can configure rules to indicate access to external or internal captive portal, or none. For more information on configuring captive portal roles for an SSID with 802.1X authentication, see Configuring Captive Portal Roles for an SSID (Page 167).

WISPr Authentication

WISPr authentication allows the smart clients to authenticate on the network when they roam between WISP even if the wireless hotspot uses an ISP with whom the client may not have an account.

If a hotspot is configured to use WISPr authentication in a specific ISP and a client attempts to access the Internet at that hotspot, the WISPr AAA server configured for the ISP authenticates the client directly and allows the client to access the network. If the client only has an account with a *partner* ISP, the WISPr AAA server forwards the client’s credentials to the partner ISP’s WISPr AAA server for authentication. When the client is authenticated on the partner ISP, it is also authenticated on the hotspot’s own ISP as per their service agreements. The AP assigns the default WISPr user role to the client when the client's ISP sends an authentication message to the AP. For more information on WISPr authentication, see Configuring WISPr Authentication (Page 212).

14.3 Supported EAP Authentication Frameworks

The following EAP authentication frameworks are supported in the SCALANCE W network:

- EAP-TLS—The EAP-TLS method supports the termination of EAP-TLS security using the internal RADIUS server . The EAP-TLS requires both server and CA certificates installed on the AP. The client certificate is verified on the virtual controller (the client certificate must be signed by a known CA) before the username is verified on the authentication server.
- EAP-TTLS —The EAP-TTLS method uses server-side certificates to set up authentication between clients and servers. However, the actual authentication is performed using passwords.
- EAP-PEAP—EAP-PEAP is an 802.1X authentication method that uses server-side public key certificates to authenticate clients with server. The PEAP authentication creates an encrypted SSL/TLS tunnel between the client and the authentication server. Exchange of information is encrypted and stored in the tunnel ensuring the user credentials are kept secure.
- LEAP—LEAP uses dynamic WEP keys for authentication between the client and authentication server.

Note

It is not recommended to use of LEAP authentication, because it does not provide any resistance to network attacks.

Authentication Termination on AP

APs support EAP termination for enterprise WLAN SSIDs. The EAP termination can reduce the number of exchange packets between the AP and the authentication servers. SCALANCE W allows EAP termination for PEAP-GTC and PEAP-MS-CHAV2. PEAP-GTC termination allows authorization against a LDAP server and external RADIUS server while PEAP-MS-CHAV2 allows authorization against an external RADIUS server.

This allows the users to run PEAP-GTC termination with their username and password to a local Microsoft Active Directory server with LDAP authentication.

- EAP-GTC—This EAP method permits the transfer of unencrypted usernames and passwords from the client to the server. The main uses for EAP-GTC are procuring one-time token cards such as Secure ID and using LDAP or RADIUS as the user authentication server. You can also enable caching of user credentials on the AP to an external authentication server for user data backup.
- EAP-MSCHAPv2—This EAP method is widely supported by Microsoft clients. A RADIUS server must be used as the back-end authentication server.

14.4 Configuring Authentication Servers

14.4.1 Supported Authentication Servers

Based on the security requirements, you can configure internal or external authentication servers. This section describes the types of servers that can be configured for client authentication:

- Internal RADIUS Server
- External RADIUS Server
- Dynamic Load Balancing between Two Authentication Servers

You can configure TACACS+ server for authenticating management users. For more information on management users and TACACS+ server-based authentication, see Configuring Authentication Parameters for Management Users (Page 175).

Internal RADIUS Server

Each AP has an instance of free RADIUS server operating locally. When you enable the internal RADIUS server option for the network, the client on the AP sends a RADIUS packet to the local IP address. The internal RADIUS server listens and replies to the RADIUS packet. SCALANCE W serves as a RADIUS server for 802.1X authentication. However, the internal RADIUS server can also be configured as a backup RADIUS server for an external RADIUS server.

External RADIUS Server

If the external RADIUS server, the IP address of the virtual controller is configured as the NAS IP address. SCALANCE W RADIUS is implemented on the virtual controller and this eliminates the need to configure multiple NAS clients for every AP on the RADIUS server for client authentication. SCALANCE W RADIUS dynamically forwards all the authentication requests from a NAS to a remote RADIUS server. The RADIUS server responds to the authentication request with an **Access-Accept** or **Access-Reject** message, and the clients are allowed or denied access to the network depending on the response from the RADIUS server. When you enable an external RADIUS server for the network, the client on the AP sends a RADIUS packet to the local IP address. The external RADIUS server then responds to the RADIUS packet.

SCALANCE W supports the following external authentication servers:

- RADIUS
- LDAP
- ClearPass Policy Manager Server for AirGroup CoA

To use an LDAP server for user authentication, configure the LDAP server on the virtual controller, and configure user IDs and passwords. To use a RADIUS server for user authentication, configure the RADIUS server on the virtual controller.

RADIUS Server Authentication with VSA

An external RADIUS server authenticates network users and returns to the AP the VSA that contains the name of the network role for the user. The authenticated user is placed into the management role specified by the VSA.

SCALANCE W supports the following VSAs for user role and VLAN derivation rules:

- AP-Group
- AP-Name
- ARAP-Features
- ARAP-Security
- ARAP-Security-Data
- ARAP-Zone-Access
- Acct-Authentic
- Acct-Delay-Time
- Acct-Input-Gigawords
- Acct-Input-Octets
- Acct-Input-Packets
- Acct-Interim-Interval
- Acct-Link-Count
- Acct-Multi-Session-Id
- Acct-Output-Gigawords
- Acct-Output-Octets Acct-Output-Packets Acct-Session-Id
- Acct-Session-Time
- Acct-Status-Type
- Acct-Terminate-Cause
- Acct-Tunnel-Packets-Lost Add-Port-To-IP-Address Aruba-AP-Group
- Aruba-AP-IP-Address
- Aruba-AS-Credential-Hash
- Aruba-AS-User-Name
- Aruba-Admin-Path
- Aruba-Admin-Role
- Aruba-AirGroup-Device-Type
- Aruba-AirGroup-Shared-Group
- Aruba-AirGroup-Shared-Role Aruba-AirGroup-Shared-User Aruba-AirGroup-User-Name Aruba-AirGroup-Version
- Aruba-Auth-SurvMethod Aruba-Auth-Survivability Aruba-CPPM-Role
- Aruba-Calea-Server-Ip
- Aruba-Device-Type
- Aruba-Essid-Name
- Aruba-Framed-IPv6-Address

- Aruba-Location-Id
- Aruba-Mdps-Device-Iccid Aruba-Mdps-Device-Imei Aruba-Mdps-Device-Name
- Aruba-Mdps-Device-Product
- Aruba-Mdps-Device-Profile Aruba-Mdps-Device-Serial Aruba-Mdps-Device-Udid
- Aruba-Mdps-Device-Version
- Aruba-Mdps-Max-Devices
- Aruba-Mdps-Provisioning-Settings
- Aruba-Named-User-Vlan
- Aruba-Network-SSO-TokeAruba-No-DHCP-Fingerprint Aruba-Port-Bounce-Host
- Aruba-Port-Id
- Aruba-Priv-Admin-User Aruba-Template-User Aruba-User-Group
- Aruba-User-Role
- Aruba-User-Vlan
- Aruba-WorkSpace-App-Name
- Authentication-Sub-Type
- Authentication-Type
- CHAP-Challenge
- Callback-Id
- Callback-Number
- Chargeable-User-Identity
- Cisco AV-Pair
- Class
- Connect-Info
- Connect-Rate
- Crypt-Password DB-Entry-State Digest-Response Domain-Name
- EAP-Message
- Error-Cause
- Event-Timestamp
- Exec-Program
- Exec-Program-Wait
- Expiration
- Fall-Through
- Filter-Id
- Framed-AppleTalk-Link
- Framed-AppleTalk-Network

- Framed-AppleTalk-Zone
- Framed-Compression
- Framed-IP-Address
- Framed-IP-Netmask Framed-IPX-Network Framed-IPv6-Pool
- Framed-IPv6-Prefix Framed-IPv6-Route Framed-Interface-Id Framed-MTU
- Framed-Protocol
- Framed-Route
- Framed-Routing
- Full-Name
- Group
- Group-Name
- Hint
- Huntgroup-Name
- Idle-Timeout
- Location-Capable
- Location-Data
- Location-Information
- Login-IP-Host
- Login-IPv6-Host Login-LAT-Node Login-LAT-Port
- Login-LAT-Service
- Login-Service Login-TCP-Port Menu
- Message-Auth
- NAS-IPv6-Address
- NAS-Port-Type Operator-Name Password
- Password-Retry
- Port-Limit
- Prefix
- Prompt
- Rad-Authenticator
- Rad-Code
- Rad-Id
- Rad-Length
- Reply-Message
- Requested-Location-Info
- Revoke-Text Server-Group Server-Name Service-Type

- Session-Timeout
- Simultaneous-Use
- State
- Strip-User-Name
- Suffix
- Termination-Action
- Termination-Menu
- Tunnel-Assignment-Id Tunnel-Client-Auth-Id Tunnel-Client-Endpoint Tunnel-Connection-Id Tunnel-Medium-Type Tunnel-Preference
- Tunnel-Private-Group-Id
- Tunnel-Server-Auth-Id Tunnel-Server-Endpoint Tunnel-Type
- User-Category
- User-Name
- User-Vlan
- Vendor-Specific
- fw_mode
- dhcp-option
- dot1x-authentication-type
- mac-address
- mac-address-and-dhcp-options

14.4.2 TACACS Servers

You can now configure a TACACS server as the authentication server to authenticate and authorize all types of management users, and account user sessions. When configured, the TACACS server allows a remote access server to communicate with an authentication server to determine if the user has access to the network. The AP users can create several TACACS server profiles and associate these profiles to the user accounts to enable authentication of the management users.

TACACS supports the following types of authentication:

- ASCII
- PAP
- CHAP
- ARAP
- MS-CHAP

Note

The TACACS server cannot be attributed to any SSID or wired profile in general as the authentication server and is configured only for the AP management users.

Dynamic Load Balancing between Two Authentication Servers

You can configure two authentication servers to serve as a primary and backup RADIUS server and enable load balancing between these servers. Load balancing of authentication servers ensures that the authentication load is split across multiple authentication servers and enables the APs to perform load balancing of authentication requests destined to authentication servers such as RADIUS or LDAP.

The load balancing in AP is performed based on outstanding authentication sessions. If there are no outstanding sessions and if the rate of authentication is low, only primary server will be used. The secondary is used only if there are outstanding authentication sessions on the primary server. With this, the load balance can be performed across RADIUS servers of asymmetric capacity without the need to obtain inputs about the server capabilities from the administrators.

14.4.3 Configuring an External Server for Authentication

You can configure RADIUS, TACACS, LDAP, and ClearPass Policy Manager servers through the SCALANCE W UI or the CLI.

In the SCALANCE W UI

To configure an external authentication server:

1. Navigate to **Security > Authentication Servers**. The **Security** window is displayed.
2. To create a new server, click **New**. A window for specifying details for the new server is displayed.

3. Configure parameters based on the type of sever.
   - **RADIUS**—To configure a RADIUS server, specify the attributes described in the following table:

Parameter	**Description**
Name	Enter a name for the server.
Server address	Enter the host name or the IP address of the external RADIUS server. **NOTE:** The hose name value will be accepted only if the **RadSec** parameter is enabled.
RadSec	Set **RadSec** to **Enabled** to enable secure communication between the RADIUS server and AP clients by creating a TLS tunnel between the AP and the server. If **RadSec** is enabled, the following configuration options are displayed: • **RadSec port**—Communication port number for RadSec TLS connection. By default, the port number is set to 2083. • RFC 3576 • RFC 5997 • NAS IP address • NAS identifier For more information on RadSec configuration, see Enabling RADIUS Communication over TLS (Page 194).
Auth port	Enter the authorization port number of the external RADIUS server within the range of 1–65,535. The default port number is 1812.
Accounting port	Enter the accounting port number within the range of 1–65,535. This port is used for sending accounting records to the RADIUS server. The default port number is 1813.
Shared key	Enter a shared key for communicating with the external RADIUS server.
Retype key	Re-enter the shared key.
Timeout	Specify a timeout value in seconds. The value determines the timeout for one RADIUS request. The AP retries to send the request several times (as configured in the **Retry count**) before the user gets disconnected. For example, if the **Timeout** is 5 seconds, **Retry counter** is 3, user is disconnected after 20 seconds. The default value is 5 seconds.
Retry count	Specify a number between 1 and 5. Indicates the maximum number of authentication requests that are sent to the server group, and the default value is 3 requests.
RFC 3576	Select **Enabled** to allow the APs to process RFC 3576-compliant CoA and disconnect messages from the RADIUS server. Disconnect messages cause a user session to be terminated immediately, whereas the CoA messages modify session authorization attributes such as data filters.

Parameter	Description
RFC 5997	This helps to detect the server status of the RADIUS server. Every time there is an authentication or accounting request timeout, the AP will send a status request enquiry to get the actual status of the RADIUS server before confirming the status of the server to be DOWN. • **Authentication**—Select this check-box to ensure the AP sends a status-server request to determine the actual state of the authentication server before marking the server as unavailable. • **Accounting**—Select this check-box to ensure the AP sends a status-server request to determine the actual state of the accounting server before marking the server as unavailable. **NOTE**: You can choose to select either the Authentication or Accounting check-boxes or select both check-boxes to support RFC5997.
NAS IP address	Allows you to configure an arbitrary IP address to be used as RADIUS attribute 4, NAS IP Address, without changing source IP Address in the IP header of the RADIUS packet. **NOTE:** If you do not enter the IP address, the virtual controller IP address is used by default when **Dynamic RADIUS Proxy** is enabled.
NAS Identifier	Allows you to configure strings for RADIUS attribute 32, NAS Identifier, to be sent with RADIUS requests to the RADIUS server.
Dead Time	Specify a dead time for authentication server in minutes. When two or more authentication servers are configured on the AP and a server is unavailable, the dead time configuration determines the duration for which the authentication server would be available if the server is marked as unavailable.
Dynamic RADIUS proxy parameters	Specify the following dynamic RADIUS proxy parameters: • DRP IP—IP address to be used as source IP for RADIUS packets. • DRP Mask—Subnet mask of the DRP IP address. • DRP VLAN—VLAN in which the RADIUS packets are sent. • DRP Gateway—Gateway IP address of the DRP VLAN. For more information on dynamic RADIUS proxy parameters and configuration procedure, see Configuring Dynamic RADIUS Proxy Parameters (Page 196).
Service type	Sets the service type value to frame for the following authentication methods: • **802.1X**—Changes the service type to frame for 802.1X authentication. • **Captive Portal**—Changes the service type to frame for Captive Portal authentication. • **MAC**—Changes the service type to frame for MAC authentication

To assign the RADIUS authentication server to a network profile, select the newly added server when configuring security settings for a wireless or wired network profile.

Note

You can also add an external RADIUS server by selecting the **New** option when configuring a WLAN or wired profile. For more information, see Configuring Security Settings for a WLAN SSID Profile (Page 104) and Configuring Security Settings for a Wired Profile (Page 129).

– **LDAP**—To configure an LDAP server, select the **LDAP** option and configure the attributes described in the following table.

Parameter	Description
Name	Enter a name for the server.
IP address	Enter the IP address of the LDAP server.
Auth port	Enter the authorization port number of the LDAP server. The default port number is 389. **NOTE:** Secure LDAP over SSL is currently not supported on APs. Changing the authentication port to 636 will not enable secure LDAP over SSL.
Admin-DN	Enter a DN for the admin user with read/search privileges across all the entries in the LDAP database (the user need not have write privileges, but the user must be able to search the database, and read attributes of other users in the database).
Admin password	Enter a password for administrator.
Base-DN	Enter a DN for the node that contains the entire user database.
Filter	Specify the filter to apply when searching for a user in the LDAP database. The default filter string is **(objectclass=*)**.
Key Attribute	Specify the attribute to use as a key while searching for the LDAP server. For Active Directory, the value is **sAMAccountName**
Timeout	Enter a value between 1 and 30 seconds. The default value is 5.
Retry count	Enter a value between 1 and 5. The default value is 3.
Dead Time	Specify a dead time for the authentication server in minutes within the range of 1–1440 minutes. The default dead time interval is 5 minutes. When two or more authentication servers are configured on the AP and a server is unavailable, the dead time configuration determines the duration for which the authentication server would be available if the server is marked as unavailable.

– **TACACS**—To configure TACACS server, select the option and configure the following parameters:

Parameter	Description
Name	Enter a name for the server.
IP address	Enter the IP address of the TACACS server.
Auth Port	Enter a TCPIP port used by the server. The default port number is 49.
Shared Key	Enter a secret key of your choice to authenticate communication between the TACACS+ client and the server.
Retype Key	Re-enter the shared key.

Parameter	Description
Timeout	Enter a number between 1 and 30 seconds to indicate the timeout period for TACACS+ requests. The default value is 20 seconds.
Retry Count	Enter a number between 1 and 5 to indicate the maximum number of authentication attempts. The default value is 3.
Dead time	Specify a dead time in minutes within the range of 1–1440 minutes. The default dead time interval is 5 minutes.
Session authorization	Enables or disables session authorization. When enabled, the optional authorization session is turned on for the admin users. By default, session authorization is disabled.

Note

You can also add TACACS server by selecting the **New** option when configuring authentication parameters for management users. For more information, see Configuring Authentication Parameters for Management Users (Page 175).

– **CPPM Server** for AirGroup CoA—To configure a ClearPass Policy Manager server used for AirGroup CoA, select the **CoA only** check box. The RADIUS server is automatically selected.

Parameter	Description
Name	Enter a name of the server.
Server address	Enter the host name or IP address of the server.
Air Group CoA port	Enter a port number for sending AirGroup CoA on a port different from the standard CoA port. The default value is 5999.
Shared key	Enter a shared key for communicating with the external RADIUS server.
Retype key	Re-enter the shared key.

4. Click **OK.**

Note

The ClearPass Policy Manager server acts as a RADIUS server and asynchronously provides the AirGroup parameters for the client device including shared user, role, and location.

In the CLI

To configure a RADIUS server with DRP parameters:

```
(AP)(config)# wlan auth-server <profile-name>

(AP)(Auth Server <profile-name>)# ip <host>

(AP)(Auth Server <profile-name>)# key <key>

(AP)(Auth Server <profile-name>)# port <port>

(AP)(Auth Server <profile-name>)# acctport <port>

(AP)(Auth Server <profile-name>)# nas-id <NAS-ID>
```

```
(AP)(Auth Server <profile-name>)# timeout <seconds>

(AP)(Auth Server <profile-name>)# retry-count <number>

(AP)(Auth Server <profile-name>)# rfc3576

(AP)(Auth Server <profile-name>)# rfc5997 {auth-only|acct-only}

(AP)(Auth Server <profile-name>)# deadtime <minutes>

(AP)(Auth Server <profile-name>)# drp-ip <IP-address> <mask> vlan <vlan>
gateway<gateway-IP-address)
```

To enable RadSec:

```
(AP)(config)# wlan auth-server <profile-name>

(AP)(Auth Server "name")# ip <host>

(AP)(Auth Server "name")# radsec [port <port>]

(AP)(Auth Server "name")# rfc3576

(AP)(Auth Server "name")# rfc5997 {auth-only|acct-only}

(AP)(Auth Server "name")# nas-id <id>

(AP)(Auth Server "name")# nas-ip <ip>
```

To configure an LDAP server:

```
(AP)(config)# wlan ldap-server <profile-name>

(AP)(LDAP Server <profile-name>)# ip <IP-address>

(AP)(LDAP Server <profile-name>)# port <port>

(AP)(LDAP Server <profile-name>)# admin-dn <name>

(AP)(LDAP Server <profile-name>)# admin-password <password>

(AP)(LDAP Server <profile-name>)# base-dn <name>

(AP)(LDAP Server <profile-name>)# filter <filter>

(AP)(LDAP Server <profile-name>)# key-attribute <key>

(AP)(LDAP Server <profile-name>)# timeout <seconds>

(AP)(LDAP Server <profile-name>)# retry-count <number>

(AP)(LDAP Server <profile-name>)# deadtime <minutes>
```

To configure a TACACS+ server:

```
(AP)(config)# wlan tacacs-server <profile-name>

(AP)(TACACS Server <profile-name>)# ip <IP-address>

(AP)(TACACS Server <profile-name>)# port <port>

(AP)(TACACS Server <profile-name>)# key <key>

(AP)(TACACS Server <profile-name>)# timeout <seconds>

(AP)(TACACS Server <profile-name>)# retry-count <number>

(AP)(TACACS Server <profile-name>)# deadtime <minutes>
```

To configure a ClearPass Policy Manager server used for AirGroup CoA:

```
(AP)(config)# wlan auth-server <profile-name>

(AP)(Auth Server <profile-name>)# ip <host>

(AP)(Auth Server <profile-name>)# key <key>

(AP)(Auth Server <profile-name>)# cppm-rfc3576-port <port>

(AP)(Auth Server <profile-name>)# cppm-rfc3576-only
```

14.4.4 Enabling RADIUS Communication over TLS (RadSec)

You can configure an AP to use TLS tunnel and to enable secure communication between the RADIUS server and AP. Enabling RADIUS communication over TLS increases the level of security for authentication that is carried out across the cloud network. When configured, this feature ensures that the RadSec protocol is used for safely transmitting the authentication and accounting data between the AP and the RadSec server.

The following conditions apply to RadSec configuration:

- When the TLS tunnel is established, RADIUS packets will go through the tunnel.
- By default, the TCP port 2083 is assigned for RadSec. Separate ports are not used for authentication, accounting, and dynamic authorization changes.
- SCALANCE W supports dynamic CoA (RFC 3576) over RadSec and the RADIUS server uses an existing TLS connection opened by the AP to send the request.
- By default, the AP uses its device certificate to establish a TLS connection with RadSec server. You can also upload your custom certificates on to AP. For more information on uploading certificates, see Uploading Certificates (Page 216).

Configuring RadSec Server

You can configure RadSec Server using the SCALANCE W UI or the CL:

In the SCALANCE W UI

1. Navigate to **Security > Authentication Servers**. The **Security** window is displayed.
2. To create a new server, click **New**. A popup window for specifying details for the new server is displayed.
3. Under **RADIUS Server**, configure the following parameters:
   – Enter the name of the server.
   – Enter the host name or the IP address of the server.
   – Select **Enabled** to enable RadSec.
   – Ensure that the port defined for RadSec is correct. By default, the port number is set to 2083.
   – To allow the APs to process RFC 3576-compliant CoA and disconnect messages from the RADIUS server, set **RFC 3576** to **Enabled**. Disconnect messages cause a user

session to be terminated immediately, whereas the CoA messages modify session authorization attributes such as data filters.

   - If **RFC 3576** is enabled, specify an AirGroup CoA port if required.
   - Enter the NAS IP address.
   - Specify the NAS identifier to configure strings for RADIUS attribute 32 and to send it with RADIUS requests to the RADIUS server.

4. Click **OK**.

In the CLI

```
(AP)(config)# wlan auth-server <profile-name>

(AP)# ip <host>

(AP)(Auth Server "name")# radsec [port <port>]

(AP)(Auth Server "name")# rfc3576

(AP)(Auth Server "name")# nas-id <id>

(AP)(Auth Server "name")# nas-ip <ip>
```

Associate the Server Profile with a Network Profile

You can associate the server profile with a network profile using the SCALANCE W UI or the CLI.

In the SCALANCE W UI

1. Access the WLAN wizard or the Wired Settings window.
   - To open the WLAN wizard, select an existing SSID on the **Network** tab, and click **edit**.
   - To open the wired settings window, click **More** > **Wired**. In the **Wired** window, select a profile and click **Edit**.

     You can also associate the authentication servers when creating a new WLAN or wired profile.

   Note

   You can also associate the authentication servers when creating a new WLAN or wired profile.

2. Click the **Security** tab and select a splash page profile.
3. Select an authentication type.
4. From the **Authentication Server 1** drop-down list, select the server name on which RadSec is enabled.
5. Click **Next** and then click **Finish**

In the CLI

To associate an authentication server to a WLAN SSID:

```
(AP)(config)# wlan ssid-profile <name>

(AP)(SSID Profile <name>)# auth-server <server-name>
```

To associate an authentication server to a wired profile:

```
(AP)(config)# wired-port-profile <name>

(AP)(wired ap profile <name>)# auth-server <name>
```

14.4.5 Configuring Dynamic RADIUS Proxy Parameters

The RADIUS server can be deployed at different locations and VLANs. In most cases, a centralized RADIUS or local server is used to authenticate users. However, some user networks can use a local RADIUS server for employee authentication and a centralized RADIUS-based captive portal server for guest authentication. To ensure that the RADIUS traffic is routed to the required RADIUS server, the dynamic RADIUS proxy feature must be enabled.

Note

The dynamic RADIUS proxy parameters configuration is not required if RadSec is enabled in the RADIUS server profile.

If the AP clients need to authenticate to the RADIUS servers through a different IP address and VLAN, ensure that the following steps are completed:

1. Enable dynamic RADIUS proxy.
2. Configure dynamic RADIUS proxy IP, VLAN, netmask, and gateway for each authentication server.
3. Associate the authentication servers to SSID or a wired profile to which the clients connect.

After completing the configuration steps mentioned above, you can authenticate the SSID users against the configured dynamic RADIUS proxy parameters.

Enabling Dynamic RADIUS Proxy

You can enable RADIUS server support using the SCALANCE W UI or the CLI.

In the SCALANCE W UI

To enable RADIUS server support:

1. In the SCALANCE W main window, click the **System** link. The **System** window is displayed.
2. On the **General** tab of the **System** window, select the **RADIUS** check box for **Dynamic Proxy**.
3. Click **OK**.

Note

When dynamic RADIUS proxy is enabled, the virtual controller network uses the IP Address of the virtual controller for communication with external RADIUS servers. Ensure that the virtual controller IP Address is set as a NAS IP when configuring RADIUS server attributes with dynamic RADIUS proxy enabled. For more information on configuring RADIUS server attributes, see Configuring an External Server for Authentication (Page 188).

Note

In case of VPN deployments, the tunnel IP received when establishing a VPN connection is used as the NAS IP. In such cases, the virtual controller IP need not be configured for the external RADIUS servers.

In the CLI

To enable the dynamic RADIUS proxy feature:

```
(AP)(config)# dynamic-radius-proxy
```

Configuring Dynamic RADIUS Proxy Parameters

You can configure DRP parameters for the authentication server by using the SCALANCE W UI or the CLI.

In the SCALANCE W UI

To configure dynamic RADIUS proxy in the SCALANCE W UI:

1. Go to **Security** > **Authentication Servers**.
2. To create a new server, click **New** and configure the required RADIUS server parameters as described in Table RADIUS (Page 188).
3. Ensure that the following dynamic RADIUS proxy parameters are configured:
   - **DRP IP**—IP address to be used as source IP for RADIUS packets.
   - **DRP Mask**—Subnet mask of the DRP IP address.
   - **DRP VLAN**—VLAN in which the RADIUS packets are sent.
   - **DRP Gateway**—Gateway IP address of the DRP VLAN.
4. Click **OK**.

In the CLI

To configure dynamic RADIUS proxy parameters:

```
(AP)(config)# wlan auth-server <profile-name>

(AP)(Auth Server <profile-name>)# ip <IP-address>

(AP)(Auth Server <profile-name>)# key <key>

(AP)(Auth Server <profile-name>)# port <port>

(AP)(Auth Server <profile-name>)# acctport <port>
```

```
(AP)(Auth Server <profile-name>)# nas-id <NAS-ID>

(AP)(Auth Server <profile-name>)# nas-ip <NAS-IP-address>

(AP)(Auth Server <profile-name>)# timeout <seconds>

(AP)(Auth Server <profile-name>)# retry-count <number>

(AP)(Auth Server <profile-name>)# deadtime <minutes>

(AP)(Auth Server <profile-name>)# drp-ip <IP-address> <mask> vlan <vlan>
gateway<gateway-IP-address>
```

14.4.6 Associate Server Profiles to a Network Profile

To associate the authentication server profiles with a network profile:

1. Access the WLAN wizard or the Wired Settings window.
   - To open the WLAN wizard, select an existing SSID on the **Network** tab, and click **edit**.
   - To open the wired settings window, click **More** > **Wired**. In the **Wired** window, select a profile and click **edit**.

     You can also associate the authentication servers when creating a new WLAN or wired profile.
2. Click the **Security** tab.
3. If you are configuring the authentication server for a WLAN SSID, on the **Security** tab, move the slider to Enterprise security level.
4. Ensure that an authentication type is enabled.
5. From the **Authentication Server 1** drop-down list, select the server name on which dynamic RADIUS proxy parameters are enabled. You can also create a new server with RADIUS and RADIUS proxy parameters by selecting **New**.
6. Click **Next** and then click **Finish**.
7. To assign the RADIUS authentication server to a network profile, select the newly added server when configuring security settings for a wireless or wired network profile.

Note

You can also add an external RADIUS server by selecting New for Authentication Server when configuring a WLAN or wired profile. For more information, see Configuring Security Settings for a WLAN SSID Profile (Page 104) and Configuring Security Settings for a Wired Profile (Page 129).

In the CLI

To associate an authentication server to a WLAN SSID:

```
(AP)(config)# wlan ssid-profile <name>

(AP)(SSID Profile <name>)# auth-server <server-name>
```

To associate an authentication server to a wired profile:

```
(AP)(config)# wired-port-profile <name>

(AP)(wired ap profile <name>)# auth-server <name>
```

14.5 Understanding Encryption Types

Encryption is the process of converting data into a cryptic format or code when it is transmitted on a network. Encryption prevents unauthorized use of the data.

SCALANCE W supports the following types of encryption:

- **WEP**—WEP is an authentication method where all users share the same key. WEP is not as secure as other encryption types such as TKIP.
- **TKIP**—TKIP uses the same encryption algorithm as WEP. However, TKIP is more secure and has an additional message integrity check.
- **AES**—The AES encryption algorithm is a widely supported encryption type for all wireless networks that contain any confidential data. AES in Wi-Fi leverages 802.1X or PSKs to generate per-station keys for all devices. AES provides a high level of security like IPsec clients.

Note

WEP and TKIP are limited to WLAN connection speed of 54 Mbps. The 802.11n connection supports only AES encryption. Siemens recommends AES encryption. Ensure that all devices that do not support AES are upgraded or replaced with the devices that support AES encryption.

WPA and WPA-2

WPA is created based on the draft of 802.11i, which allowed users to create more secure WLANs. WPA-2 encompasses the full implementation of the 802.11i standard. WPA-2 is a superset that encompasses the full WPA feature set.

The following table summarizes the differences between the two certifications::

Table 14- 2 WPA and WPA-2 Features

Certification	Authentication	Encryption
WPA	• PSK • IEEE 802.1X with Extensible Authentication Protocol (EAP)	TKIP with message integrity check
WPA-2	• PSK • IEEE 802.1X with EAP	AES—Counter Mode with Cipher Block Chaining Message Authentication Code

WPA and WPA-2 can be further classified as follows:

- **Personal**—Personal is also called PSK. In this type, a unique key is shared with each client in the network. Users have to use this key to securely log in to the network. The key remains the same until it is changed by authorized personnel. You can also configure key change intervals

- **Enterprise**—Enterprise is more secure than WPA Personal. In this type, every client automatically receives a unique encryption key after securely logging in to the network. This key is automatically updated at regular intervals. WPA uses TKIP and WPA-2 uses the AES algorithm.

Recommended Authentication and Encryption Combinations

The following table summarizes the recommendations for authentication and encryption combinations for the Wi-Fi networks.

Table 14- 3 Recommended Authentication and Encryption Combinations

Network Type	Authentication	Encryption
Employee	802.1X	AES
Guest Network	Captive portal	None
Voice Network or Handheld devices	802.1X or PSK as supported by the device	AES if possible, TKIP or WEP if necessary (combine with security settings assigned for a user role).

14.6 Configuring Authentication Survivability

The authentication survivability feature supports a survivable authentication framework against any remote link failures when working with external authentication servers. When enabled, this feature allows the APs to authenticate the previously connected clients against the cached credentials if the connection to the authentication server is temporarily lost.

SCALANCE W supports the following EAP standards for authentication survivability:

- **EAP-PEAP**: The PEAP, also known as Protected EAP, is a protocol that encapsulates EAP within a potentially encrypted and authenticated TLS tunnel. The EAP-PEAP supports MS-CHAPv2 and GTC methods.
- **EAP-TLS**: EAP-TLS is an IETF open standard that uses the TLS protocol.

When the authentication survivability feature is enabled, the following authentication process is used:

1. The client associates to an AP and authenticates to the external authentication server. The external authentication server can be either ClearPass Policy Manager for EAP-PEAP or RADIUS server for EAP-TLS.
2. Upon successful authentication, the associated AP caches the authentication credentials of the connected clients for the configured duration. The cache expiry duration for authentication survivability can be set within the range of 1–99 hours, with 24 hours being the default cache timeout duration.
3. If the client roams or tries to reconnect to the AP and the remote link fails due to the unavailability of the authentication server, the AP uses the cached credentials in the

internal authentication server to authenticate the user. However, if the client tries to reconnect after the cache expiry, the authentication fails.

4. When the authentication server is available and if the client tries to reconnect, the AP detects the availability of server and allows the client to authenticate to the server. Upon successful authentication, the AP cache details are refreshed

Enabling Authentication Survivability

You can enable authentication survivability for a wireless network profile through the SCALANCE W UI or the CLI.

In the SCALANCE W UI

To configure authentication survivability for a wireless network:

1. On the **Network** tab, click **New** to create a new network profile or select an existing profile for which you want to enable authentication survivability and click **edit**.
2. In the **Edit <profile-name>** or the **New WLAN** window, ensure that all required WLAN and VLAN attributes are defined, and then click **Next**.
3. On the **Security** tab, under **Enterprise** security settings, select an existing authentication server or create a new server by clicking **New**.
4. To enable authentication survivability, select **Enabled** from the **Authentication survivability** drop-down list. On enabling this, the AP authenticates the previously connected clients using EAP-PEAP and EAP-TLS authentication when connection to the external authentication server is temporarily lost.
5. Specify the cache timeout duration, after which the cached details of the previously authenticated clients expire. You can specify a value within the range of 1–99 hours and the default cache timeout duration is 24 hours.
6. Click **Next** and then click **Finish** to apply the changes.

Important Points to Remember

- Any client connected through ClearPass Policy Manager and authenticated through AP remains authenticated with the AP even if the client is removed from the ClearPass Policy Manager server during the ClearPass Policy Manager downtime.
- Do not make any changes to the authentication survivability cache timeout duration when the authentication server is down.
- For EAP-PEAP authentication, ensure that the ClearPass Policy Manager 6.0.2 or later version is used for authentication. For EAP-TLS authentication, any external or third-party server can be used.
- For EAP-TLS authentication, ensure that the server and CA certificates from the authentication servers are uploaded on the AP. For more information, see Uploading Certificates (Page 216).
- Authentication cache will be lost if the AP on which the user credentials are cached, is rebooted.

In the CLI

To configure authentication survivability for a wireless network:

```
(AP)(config)# wlan ssid-profile <name>
```

```
(AP)(SSID Profile <name>)# type {<Employee>|<Voice>|<Guest>}

(AP)(SSID Profile <name>)# auth-server <server-name1> (

AP)(SSID Profile <name>)# auth-survivability

(AP)(SSID Profile <name>)# exit

(AP)(config)# auth-survivability cache-time-out <hours>
```

To view the cache expiry duration:

```
(AP)# show auth-survivability time-out
```

To view the information cached by the AP:

```
(AP)# show auth-survivability cached-info
```

To view logs for debugging:

```
(AP)# show auth-survivability debug-log
```

14.7 Configuring 802.1X Authentication for a Network Profile

This section consists of the following procedures:

- Configuring 802.1X Authentication for Wireless Network Profiles
- Configuring 802.1X Authentication for Wired Profiles

The SCALANCE W network supports internal RADIUS server and external RADIUS server for 802.1X authentication.

The steps involved in 802.1X authentication are as follows:

1. The NAS requests authentication credentials from a wireless client.
2. The wireless client sends authentication credentials to the NAS.
3. The NAS sends these credentials to a RADIUS server.
4. The RADIUS server checks the user identity and authenticates the client if the user details are available in its database. The RADIUS server sends an **Access-Accept** message to the NAS. If the RADIUS server cannot identify the user, it stops the authentication process and sends an **Access-Reject** message to the NAS. The NAS forwards this message to the client and the client must re-authenticate with appropriate credentials.
5. After the client is authenticated, the RADIUS server forwards the encryption key to the NAS. The encryption key is used for encrypting or decrypting traffic sent to and from the client.

In the 802.1X termination-disabled mode, if the identity in the **EAP-ID-Resp** message is longer than or equal to 248 octets and the identity contains **@FQDN** at the end, then the **EAP-ID-Resp** message is not dropped. The RADIUS User-Name attribute contains the truncated-string (up to 127 octets) from the original identify before the last **@FQDN** followed by the last **@FQDN**.

Note

The NAS acts as a gateway to guard access to a protected resource. A client connecting to the wireless network first connects to the NAS.

Configuring 802.1X Authentication for Wireless Network Profiles

You can configure 802.1X authentication for a wireless network profile in the SCALANCE W UI or the CLI.

In the SCALANCE W UI

To enable 802.1X authentication for a wireless network:

1. On the **Network** tab, click **New** to create a new network profile or select an existing profile for which you want to enable 802.1X authentication and click **edit**.
2. In the **Edit <profile-name>** or the **New WLAN** window, ensure that all required WLAN and VLAN attributes are defined, and then click **Next**.
3. On the **Security** tab, specify the following parameters for the **Enterprise** security level:

   Select any of the following options from the **Key management** drop-down list.

   – WPA-2 Enterprise

   – WPA Enterprise

   – Both (WPA-2 & WPA)

   – Dynamic WEP with 802.1X
4. If you do not want to use a session key from the RADIUS server to derive pairwise unicast keys, set **Session Key for LEAP** to **Enabled**.
5. To terminate the EAP portion of 802.1X authentication on the IP instead of the RADIUS server, set **Termination** to **Enabled**.

   By default, for 802.1X authentication, the client conducts an EAP exchange with the RADIUS server, and the AP acts as a relay for this exchange. When **Termination** is enabled, the AP by itself acts as an authentication server and terminates the outer layers of the EAP protocol, only relaying the innermost layer to the external RADIUS server.
6. Specify the type of authentication server to use and configure other required parameters. You can also configure two different authentication servers to function as primary and backup servers when **Termination** is enabled. For more information on RADIUS authentication configuration parameters, see Configuring an External Server for Authentication (Page 188).
7. Click **Next** to define access rules, and then click **Finish** to apply the changes.

In the CLI

To configure 802.1X authentication for a wireless network:

```
(AP)(config)# wlan ssid-profile <name>

(AP)(SSID Profile <name>)# type {<Employee>|<Voice>}

(AP)(SSID Profile <name>)# opmode {wpa2-aes|wpa-tkip|wpa-tkip,wpa2-aes|dynamic-wep}

(AP)(SSID Profile <name>)# leap-use-session-key

(AP)(SSID Profile <name>)# termination

(AP)(SSID Profile <name>)# auth-server <server1>

(AP)(SSID Profile <name>)# auth-server <server2>

(AP)(SSID Profile <name>)# radius-reauth-interval <minutes>

(AP)(SSID Profile <name>)# auth-survivability

(AP)(SSID Profile <name>)# exit

(AP)(config)# auth-survivability cache-time-out <hours>
```

Configuring 802.1X Authentication for Wired Profiles

You can configure 802.1X authentication for a wired profile in the SCALANCE W UI or the CLI.

In the SCALANCE W UI

To enable 802.1X authentication for a wired profile:

1. Click the **Wired** link under **More** in the main window. The **Wired** window is displayed.
2. Click **New** under **Wired Networks** to create a new network or select an existing profile for which you want to enable 802.1X authentication and then click **Edit**.
3. In the **New Wired Network** or the **Edit Wired Network** window, ensure that all the required Wired and VLAN attributes are defined, and then click **Next**.
4. On the **Security** tab, select **Enabled** from the **802.1X authentication** drop-down list.
5. Specify the type of authentication server to use and configure other required parameters. For more information on configuration parameters, see Configuring Security Settings for a Wired Profile (Page 129).
6. Click **Next** to define access rules, and then click **Finish** to apply the changes.
7. Assign the profile to an Ethernet port. For more information, see Assigning a Profile to Ethernet Ports (Page 133).

In the CLI

To enable 802.1X authentication for a wired profile:

```
(AP)(config)# wired-port-profile <name>

(AP)(wired ap profile <name>)# type {<employee>|<guest>}

(AP)(wired ap profile <name>)# dot1x

(AP)(wired ap profile <name>)# auth-server <server1>

(AP)(wired ap profile <name>)# auth-server <server2>
```

```
(AP)(wired ap profile <name>)# server-load-balancing

(AP)(wired ap profile <name>)# radius-reauth-interval <Minutes>
```

14.8 Enabling 802.1X Supplicant Support

The 802.1X authentication protocol prevents the unauthorized clients from gaining access to the network through publicly accessible ports. If the ports to which the APs are connected, are configured to use the 802.1X authentication method, ensure that you configure the APs to function as an 802.1X client or supplicant. If your network requires all wired devices to authenticate using PEAP or TLS protocol, you need to configure the AP uplink ports for 802.1X authentication, so that the switch grants access to the AP only after completing the authentication as a valid client.

To enable the 802.1X supplicant support on an AP, ensure that the 802.1X authentication parameters are configured on all APs in the cluster and are stored securely in the AP flash.

Note

The 802.1X supplicant support feature is not supported with mesh and Wi-Fi uplink.

Configuring an AP for 802.1X Supplicant Support

To enable 802.1X supplicant support, configure 802.1X authentication parameters on every AP using the SCALANCE W UI or the CLI

In the SCALANCE W UI

1. To use PEAP protocol-based 802.1X authentication method, complete the following steps:
   – In the **Access Points** tab, click the AP on which you want to set the variables for 802.1X authentication, and then click the **edit** link
   – In the **Edit Access Point** window, click the **Uplink** tab.
   – Under PEAP user, enter the username, password, and retype the password for confirmation. The AP username and password are stored in AP flash. When the AP boots, the */tmp/ap1xuser* and */tmp/ap1xpassword* files are created based on these two variables.

   Note

   The default inner authentication protocol for PEAP is MS-CHAPV2.

2. To upload server certificates for validating the authentication server credentials, complete the following steps:
   – Click **Upload New Certificate**.
   – Specify the URL from where you want to upload the certificates and select the type of certificate.
3. Click **OK.**

4. To configure 802.1X authentication on uplink ports of an AP, complete the following steps:
   – Go to **System** > **Show advanced options** > **Uplink**
   – Click AP1X.
   – Select PEAP or TLS as the authentication type.
   – If you want to validate the server credentials using server certificate, select the **Validate Server** check box. Ensure that the server certificates for validating server credentials are uploaded to AP database.
   – Click **OK**
5. Reboot the AP.

In the CLI

To set username and password variable used by the PEAP protocol-based 802.1X authentication:

```
(AP)# ap1x-peap-user <ap1xuser> <password>
```

To set the PEAP 802.1X authentication type:

```
(AP)(config)# ap1x peap [validate-server]
```

To set TLS 802.1X authentication type:

```
(AP)(config)# ap1x tls <tpm|user> [validate-server]
```

To upload user or CA certificates for PEAP or TLS authentication:

```
(AP)# copy tftp <addr> <file> ap1x {ca|cert <password>} format pem
```

To download user or server certificates from a TFTP, FTP, or web server: `(AP)# download ap1x <url> format pem [psk <psk>]`

```
(AP)# download ap1xca <url> format pem
```

To view the certificate details:

```
(AP)# show ap1xcert
```

To verify the configuration, use any of the following commands:

```
(AP)# show ap1x config

(AP)# show ap1x debug-logs

(AP)# show ap1x status
```

14.9 Configuring MAC Authentication for a Network Profile

MAC authentication can be used alone or it can be combined with other forms of authentication such as WEP authentication. However, it is recommended that you do not use the MAC-based authentication.

This section describes the following procedures:

- Configuring MAC Authentication for Wireless Network Profiles
- Configuring MAC Authentication for Wired Profiles

Configuring MAC Authentication for Wireless Network Profiles

You can configure MAC authentication with 802.1X authentication for a wireless network profile using the SCALANCE W UI or the CLI.

In the SCALANCE W UI

To enable MAC Authentication for a wireless network:

1. On the **Network** tab, click **New** to create a new network profile or select an existing profile for which you want to enable MAC and 802.1X authentications and click **edit.**
2. In the **Edit <profile-name>** or the **New WLAN** window, ensure that all required WLAN and VLAN attributes are defined, and then click **Next**.
3. On the **Security** tab, select **Enabled** from the **MAC authentication** drop-down list for the **Personal** or the **Open** security level.
4. Specify the type of authentication server to use
5. If an internal authentication server is used, perform the following steps to allow MAC-address-based authentication:
   - Click the **Users** link beside the **Internal server** parameter. The **Users** window is displayed.
   - Specify the client MAC address as the username and password.
   - Specify the type of the user (employee or guest).
   - Click **Add**.
   - Repeat the steps to add more users.
   - Click **OK**.
6. To allow the AP to use a delimiter in the MAC authentication request, specify a character (for example, colon or dash) as a delimiter for the MAC address string. For example, if you specify colon as the delimiter, MAC addresses in the xx:xx:xx:xx:xx:xx format are used. If the delimiter is not specified, the MAC address in the xxxxxxxxxxxx format is used
7. To allow the AP to use uppercase letters in the MAC address string, set Uppercase support to **Enabled**.
8. Configure other parameters as required.
9. Click **Next** to define access rules, and then click **Finish** to apply the changes.

In the CLI

To configure MAC-address based authentication with external server:

```
(AP)(config)# wlan ssid-profile <name>

(AP)(SSID Profile <name>)# type {<Employee>|<Voice>|<Guest>}

(AP)(SSID Profile <name>)# mac-authentication
```

```
(AP)(SSID Profile <name>)# mac-authentication-delimiter <delim>

(AP)(SSID Profile <name>)# mac-authentication-upper-case

(AP)(SSID Profile <name>)# external-server

(AP)(SSID Profile <name>)# auth-server <server-name1>

(AP)(SSID Profile <name>)# auth-server <server-name2>

(AP)(SSID Profile <name>)# server-load-balancing

(AP)(SSID Profile <name>)# radius-reauth-interval <minutes>
```

To add users for MAC authentication based on internal authentication server:

```
(AP)(config)# user <username> [<password>] [portal|radius]
```

Configuring MAC Authentications for Wired Profiles

You can configure MAC authentication for a wired profile in the SCALANCE W UI or the CLI.

In the SCALANCE W UI

To enable MAC authentication for a wired profile:

1. Click the **Wired** link under **More** in the main window. The **Wired** window is displayed.
2. Click **New** under **Wired Networks** to create a new network or select an existing profile for which you want to enable MAC authentication and then click **Edit**.
3. In the **New Wired Network** or the **Edit Wired Network** window, ensure that all the required Wired and VLAN attributes are defined, and then click **Next**.
4. On the **Security** tab, select **Enabled** from the **MAC authentication** drop-down list.
5. Specify the type of authentication server to use
6. If an internal authentication server is used, perform the following steps to allow MAC-address-based authentication:
   - Click the **Users** link beside **Internal server**. The **Users** window is displayed.
   - Specify the client MAC address as the username and password.
   - Specify the type of the user (employee or guest).
   - Click **Add**.
   - Repeat the steps to add more users.
   - Click **OK**.
7. Configure other parameters as required.
8. Click **Next** to define access rules, and then click **Finish** to apply the changes.

In the CLI

To configure MAC-address-based authentication with external server:

```
(AP)(config)# wired-port-profile <name>

(AP)(wired ap profile <name>)# type {<employee>|<guest>}

(AP)(wired ap profile <name>)# mac-authentication
```

```
(AP)(wired ap profile <name>)# auth-server <server-1>

(AP)(wired ap profile <name>)# auth-server <server-2>

(AP)(wired ap profile <name>)# server-load-balancing

(AP)(wired ap profile <name>)# radius-reauth-interval <Minutes>
```

To add users for MAC authentication based on internal authentication server:

```
(AP)(config)# user <username> [<password>] [portal|radius]
```

14.10 Configuring MAC and 802.1X Authentications for Wired Profiles

This section describes the following procedures:

- Configuring MAC and 802.1X Authentications for Wireless Network Profiles
- Configuring MAC and 802.1X Authentications for Wired Profiles

Configuring MAC and 802.1X Authentications for Wireless Network Profiles

You can configure MAC authentication with 802.1X authentication for a wireless network profile using the SCALANCE W UI or the CLI.

In the SCALANCE W UI

1. On the **Network** tab, click **New** to create a new network profile or select an existing profile for which you want to enable MAC and 802.1X authentications and click **edit.**
2. In the **Edit <profile-name>** or the **New WLAN** window, ensure that all required WLAN and VLAN attributes are defined, and then click **Next**.
3. On the **Security** tab, ensure that the required parameters for MAC authentication and 802.1X authentication are configured.
4. Select the **Perform MAC authentication before 802.1X** check box to use 802.1X authentication only when the MAC authentication is successful.
5. Select the **MAC authentication fail-thru** check box to use 802.1X authentication even when the MAC authentication fails.
6. Click **Next** and then click **Finish** to apply the changes.

In the CLI

To configure MAC-address based authentication with external server:

```
(AP)(config)# wlan ssid-profile <name>

(AP)(SSID Profile <name>)# type {<Employee>|<Voice>|<Guest>}

(AP)(SSID Profile <name>)# mac-authentication(AP)(SSID Profile <name>)# l2-auth-
failthrough

(AP)(SSID Profile <name>)# auth-server <server-name1>

(AP)(SSID Profile <name>)# radius-reauth-interval <minutes>

(AP)(SSID Profile <name>)# auth-survivability
```

```
(AP)(SSID Profile <name>)# exit

(AP)(config)# auth-survivability cache-time-out <hours>
```

Configuring MAC and 802.1X Authentications for Wired Profiles

You can configure MAC and 802.1X authentications for a wired profile in the SCALANCE W UI or the CLI.

In the SCALANCE W UI

To enable MAC and 802.1X authentications for a wired profile:

1. Click the **Wired** link under **More** in the main window. The **Wired** window is displayed.
2. Click **New** under **Wired Networks** to create a new network or select an existing profile for which you want to enable MAC authentication and then click **Edit**.
3. In the **New Wired Network** or the **Edit Wired Network** window, ensure that all the required Wired and VLAN attributes are defined, and then click **Next**.
4. On the **Security** tab, perform the following steps:
   - Select **Enabled** from the **MAC authentication** drop-down list.
   - Select **Enabled** from the **802.1X authentication** drop-down list.
   - Select **Enabled** from the **MAC authentication fail-thru** drop-down list.
5. Specify the type of authentication server to use and configure other required parameters. For more information on configuration parameters, see Configuring Security Settings for a Wired Profile (Page 129).
6. Click **Next** to define access rules, and then click **Finish** to apply the changes.

In the CLI

To enable MAC and 802.1X authentications for a wired profile:

```
(AP)(config)# wired-port-profile <name>

(AP)(wired ap profile "<name>")# type {<employee>|<guest>}

(AP)(wired ap profile "<name>")# mac-authentication

(AP)(wired ap profile "<name>")# dot1x

(AP)(wired ap profile "<name>")# l2-auth-failthrough

(AP)(wired ap profile "<name>")# auth-server <name>

(AP)(wired ap profile "<name>")# server-load-balancing

(AP)(wired ap profile "<name>")# radius-reauth-interval <Minutes>
```

14.11 Configuring MAC Authentication with Captive Portal Authentication

The following configuration conditions apply to MAC + captive portal authentication method:

- If the captive portal splash page type is **Internal-Authenticated** or **External-RADIUS Server**, MAC authentication reuses the server configurations.
- If the captive portal splash page type is **Internal-Acknowledged** or **External-Authentication Text** and MAC authentication is enabled, a server configuration page is displayed.

You can configure the MAC authentication with captive portal authentication for a network profile using the SCALANCE W UI or the CLI.

In the SCALANCE W UI

1. Select an existing wireless or wired profile for which you want to enable MAC with captive portal authentication. Depending on the network profile selected, the **Edit <WLAN-Profile>** or the **Edit Wired Network** window is displayed

   Note

   To enable MAC authentication with captive portal authentication on a new WLAN SSID or wired profile, click the Security tab on the **New WLAN** window and the **New Wired Network** window.

2. On the **Security** tab, specify the following parameters:
   - Select **Enabled** from the **MAC authentication** drop-down list to enable MAC authentication for captive portal users. If the MAC authentication fails, the captive portal authentication role is assigned to the client.
   - To enforce MAC authentication, click the **Access** tab and select **Enforce MAC auth only role** check box.
3. Click **Next** and then click **Finish** to apply the changes.

In the CLI

To configure MAC authentication with captive portal authentication for a wireless profile:

```
(AP)(config)# wlan ssid-profile <name>

(AP)(SSID Profile <name>)# type <guest>

(AP)(SSID Profile <name>)# mac-authentication

(AP)(SSID Profile <name>)# captive-portal {<type> [exclude-uplink <types>]|external
[Profile <name>] [exclude-uplink <types>]}

(AP)(SSID Profile <name>)# set-role-mac-auth <mac-only>
```

To configure MAC authentication with captive portal authentication for a wired profile:

```
(AP)(config)# wired-port-profile <name>

(AP)(wired ap profile <name>)# type <guest>

(AP)(wired ap profile <name>)# mac-authentication

(AP)(wired ap profile <name>)# captive-portal <type>

(AP)(wired ap profile <name>)# captive-portal {<type> [exclude-
uplink<types>]|external [Profile <name>] [exclude-uplink <types>]}
```

```
(AP)(wired ap profile <name>)# set-role-mac-auth <mac-only>
```

14.12 Configuring WISPr Authentication

SCALANCE W supports the following smart clients:

- iPass
- Boingo

These smart clients enable client authentication and roaming between hotspots by embedding iPass Generic Interface Specification *redirect*, *authentication*, and *logoff* messages within HTML messages that are sent to the AP.

Note

WISPr authentication is supported only for the **Internal - Authenticated** and **External - RADIUS Server** captive portal authentication. Select the **Internal – Authenticated** or the **External - RADIUS Server** option from the **Splash page type** drop-down list to configure WISPr authentication for a WLAN profile.

You can configure WISPr authentication using the SCALANCE W UI or the CLI.

In the SCALANCE W UI

1. Click the **System** link located directly above the Search bar in the SCALANCE W main window. The **System** window is displayed.
2. Click **Show advanced options**.
3. Click **WISPr** tab. The **WISPr** tab contents are displayed.
4. Enter the ISO Country Code for the WISPr Location ID in the **ISO country code** text box.
5. Enter the E.164 Area Code for the WISPr Location ID in the **E.164 area code** text box.
6. Enter the operator name of the hotspot in the **Operator name** text box.
7. Enter the E.164 Country Code for the WISPr Location ID in the **E.164 country code** text box.
8. Enter the **SSID/Zone** section for the WISPr Location ID in the **SSID/Zone** text box.
9. Enter the name of the Hotspot location in the **Location name** text box. If no name is defined, the name of the AP to which the user is associated is used.
10. Click **OK** to apply the changes.

The WISPr RADIUS attributes and configuration parameters are specific to the RADIUS server used by your ISP for the WISPr authentication. Contact your ISP to determine these values. You can find a list of ISO and ITU country and area codes at the ISO and ITU websites (www.iso.org and http://www.itu.int).

Note

A Boingo smart client uses a NAS identifier in the <CarrierID>_<VenueID> format for location identification. To support Boingo clients, ensure that you configure the NAS identifier parameter in the RADIUS server profile for the WISPr server

---

In the CLI

```
(AP)(config)# wlan wispr-profile

(AP)(WISPr)# wispr-location-id-ac

(AP)(WISPr)# wispr-location-id-cc

(AP)(WISPr)# wispr-location-id-isocc

(AP)(WISPr)# wispr-location-id-network

(AP)(WISPr)# wispr-location-name-location

(AP)(WISPr)# wispr-location-name-operator-name
```

14.13 Blacklisting Clients

The client blacklisting denies connection to the blacklisted clients. When a client is blacklisted, it is not allowed to associate with an AP in the network. If a client is connected to the network when it is blacklisted, a deauthentication message is sent to force client disconnection.

This section describes the following procedures:

- Blacklisting Clients Manually
- Blacklisting Users Dynamically

Blacklisting Clients Manually

Manual blacklisting adds the MAC address of a client to the blacklist. These clients are added into a permanent blacklist. These blacklisted clients are not allowed to connect to the network unless they are removed from the blacklist.

You can add a client to the blacklist manually using the SCALANCE W UI or the CLI.

In the SCALANCE W UI

1. Click the **Security** link located directly above the Search bar in the SCALANCE W main window.
2. Click the **Blacklisting** tab.
3. Under the **Manual Blacklisting**, click **New**.

4. Enter the MAC address of the client to be blacklisted in the **MAC address to add** text box.

Note

For the blacklisting to take effect on the MAC address, you must enable blacklisting in the SSID profile. For more information, see Blacklisting (Page 104).

5. Click **OK**. The **Blacklisted Since** tab displays the time at which the current blacklisting has started for the client.
6. To delete a client from the manual blacklist, select the MAC Address of the client under the **Manual Blacklisting**, and then click **Delete**

In the CLI

To blacklist a client:

```
(AP)(config)# blacklist-client <MAC-Address>
```

To enable blacklisting in the SSID profile:

```
(AP)(config)# wlan ssid-profile <name>

(AP)(SSID Profile <name>)# blacklisting
```

To view the blacklisted clients:

```
(AP)# show blacklist-client Blacklisted Clients

-------------------

MAC                   Reason          Timestamp    Remaining time(sec)      AP name
---                   ------          ---------    -------------------      -------
00:1c:b3:09:85:15     user-defined    17:21:29     Permanent                -
```

Blacklisting Users Dynamically

The clients can be blacklisted dynamically when they exceed the authentication failure threshold or when a blacklisting rule is triggered as part of the authentication process.

Authentication Failure Blacklisting

When a client takes time to authenticate and exceeds the configured failure threshold, it is automatically blacklisted by an AP.

Session Firewall-Based Blacklisting

In session firewall-based blacklisting, an ACL rule is used to enable the option for dynamic blacklisting. When the ACL rule is triggered, it sends out blacklist information and the client is blacklisted.

Configuring Blacklist Duration

You can set the blacklist duration using the SCALANCE W UI or the CLI.

In the SCALANCE W UI

To set a blacklist duration:

1. Click the **Security** link located directly above the Search bar in the SCALANCE W main window.
2. Click the **Blacklisting** tab.
3. Under **Dynamic Blacklisting**:
4. For **Auth failure blacklist time**, the duration in seconds after which the clients that exceed the authentication failure threshold must be blacklisted
5. For **PEF rule blacklisted time**, enter the duration in seconds after which the clients can be blacklisted due to an ACL rule trigger.

Note

You can configure a maximum number of authentication failures by the clients, after which a client must be blacklisted. For more information on configuring maximum authentication failure attempts, see Configuring Security Settings for a WLAN SSID Profile (Page 104).

Note

To enable session-firewall-based blacklisting, click New and navigate to **WLAN Settings** > **VLAN** > **Security** > **Access** window, and enable the **Blacklist** option of the corresponding ACL rule.

In the CLI

To dynamically blacklist clients:

```
(AP)(config)# auth-failure-blacklist-time <seconds>

(AP)(config)# blacklist-time <seconds>
```

To enable blacklisting in the SSID profile:

```
(AP)(config)# wlan ssid-profile <name>

(AP)(SSID Profile <name>)# blacklisting
```

To view the blacklisted clients:

```
(AP)# show blacklist-client config

Blacklist Time 60

Auth Failure Blacklist Time 60

Manually Blacklisted Clients

----------------------------

MAC Time

--- ----

Dynamically Blacklisted Clients

-------------------------------

MAC Reason Timestamp Remaining time(sec) AP IP
```

```
--- ------ --------- ------------------- -----

Dyn Blacklist Count 0
```

14.14 Uploading Certificate

A certificate is a digital file that certifies the identity of the organization or products of the organization. It is also used to establish your credentials for any web transactions. It contains the organization name, a serial number, expiration date, a copy of the certificate-holder's public key, and the digital signature of the certificate- issuing authority so that a recipient can ensure that the certificate is real.

SCALANCE W supports the following certificate files:

- Authentication server (PEM format)
- Captive portal server (PEM format)—Customized certificate for internal captive portal server
- CA certificate (PEM or DER format)
- RadSec certificate (PEM or DER format)
- SCALANCE W UI certificate (PEM format)

This section describes the following procedures:

- Loading Certificates Through SCALANCE W UI
- Loading Certificates Through SCALANCE W CLI
- Removing Certificates
- Loading Certificates Through AirWave

Loading Certificates through SCALANCE W UI

To load a certificate in the SCALANCE W UI:

1. Click the **Maintenance** link located directly above the Search bar in the SCALANCE W main window.
2. Click the **Certificates** tab. The **Certificates** tab contents are displayed.
3. To upload a certificate, click **Upload New Certificate**. The **New Certificate** window is displayed.
4. Browse and select the file to upload.

5. Select any of the following types of certificates from the **Certificate type** drop-down list:
   – CA—CA certificate to validate the identity of the client.
   – Auth Server—The authentication server certificate to verify the identity of the server to the client.
   – Captive portal server—Captive portal server certificate to verify the identity of internal captive portal server to the client.
   – RadSec—The RadSec server certificate to verify the identity of the server to the client.
   – RadSec CA—The RadSec CA certificate for mutual authentication between the AP clients and the TLS server.
6. Select the certificate format from the **Certificate format** drop-down list.
7. If you have selected **Auth Server**, **Captive portal server**, **SCALANCE W UI**, or **RadSec** as the type of certificate, enter a passphrase in **Passphrase** and retype the passphrase. If the certificate does not include a passphrase, there is no passphrase required.
8. Click **Browse** and select the appropriate certificate file, and click **Upload Certificate**. The **Certificate Successfully Installed** message is displayed.

Note

The AP database can have only one authentication server certificate and one captive portal server certificate at any point in time.

Note

When a Captive Portal server certificate is uploaded using the SCALANCE W UI, the default management certificate on the UI is also replaced by the Captive portal server certificate.

Loading Certificates through SCALANCE W CLI

To upload a CA, server, SCALANCE W UI, or captive portal certificate:

```
(AP)# copy tftp <ip-address> <filename> {cpserver cert <password> format {p12|pem}|
radsec {ca|cert <password>} format pem|system {1xca format {der|pem}| 1xcert
<password> format pem} uiserver cert <password> format pem}
```

To download RadSec certificates:

```
(AP)# download-cert radsec ftp://192.0.2.7 format pem [psk <psk>]
```

```
(AP)# download-cert radsecca ftp://192.0.2.7 format pem
```

Removing Certificates

To clear a certificate:

```
(AP)# clear-cert {ca|cp|radsec|radsecca|server}
```

Loading Certificates Through AirWave

You can manage certificates using AirWave. The AMP directly provisions the certificates and performs basic certificate verification (such as certificate type, format, version, serial number, and so on) before accepting the certificate and uploading to an AP network. The AMP packages the text of the certificate into an HTTPS message and sends it to the virtual controller. After the virtual controller receives this message, it draws the certificate content from the message, converts it to the right format, and saves it on the RADIUS server.

To load a certificate in AirWave:

1. Navigate to **Device Setup > Certificate** and then click **Add** to add a new certificate. The **Certificate** window is displayed.
2. Enter the certificate **Name**, and click **Choose File** to browse and upload the certificate.
3. Select the appropriate **Format** that matches the certificate filename.
   – Select **Server Cert** for certificate **Type**, and provide the passphrase if you want to upload a server certificate.
   – elect either **Intermediate CA** or **Trusted CA** certificate **Type**, if you want to upload a CA certificate,
4. After you upload the certificate, navigate to **Groups,** click the SCALANCE W **Group** and then select **Basic**. The Group name is displayed only if you have entered the **Organization** name in the SCALANCE W UI. For more information, see Configuring Organization String (Page 389) for further information.

   The **Virtual Controller Certificate** section displays the certificates (CA cert and Server).
5. Click **Save** to apply the changes only to AirWave. Click **Save and Apply** to apply the changes to the AP.
6. To clear the certificate options, click **Revert**.

Roles and Policies 15

15.1 Firewall Policies

SCALANCE W firewall provides identity-based controls to enforce application-layer security, prioritization, traffic forwarding, and network performance policies for wired and wireless networks. Using SCALANCE W firewall, you can enforce network access policies that define access to the network, areas of the network that users may access, and the performance thresholds of various applications.

SCALANCE W supports a role-based stateful firewall. SCALANCE W firewall recognizes flows in a network and keeps track of the state of sessions. SCALANCE W firewall manages packets according to the first rule that matches the packet. The firewall logs on the APs are generated as syslog messages.

15.1.1 ACL Rules

You can use ACL rules to either permit or deny data packets passing through the AP. You can also limit packets or bandwidth available to a set of user roles by defining access rules. By adding custom rules, you can block or allow access based on the service or application, source or destination IP addresses.

You can create access rules to allow or block data packets that match the criteria defined in an access rule. You can create rules for either inbound traffic or outbound traffic. Inbound rules explicitly allow or block the inbound network traffic that matches the criteria in the rule. Outbound rules explicitly allow or block the network traffic that matches the criteria in the rule. For example, you can configure a rule to explicitly block outbound traffic to an IP address through the firewall.

The AP clients are associated with user roles, that determine the client’s network privileges and the frequency at which clients re-authenticate.

SCALANCE W supports the following types of ACLs:

- ACLs that permit or deny traffic based on the source IP address of the packet.
- ACLs that permit or deny traffic based on the source or destination IP address, and the source or destination port number.
- ACLs that permit or deny traffic based on network services, application, application categories, web categories, and security ratings.

Note

You can configure up to 128 access control entries in an ACL for a user role.

Note

The maximum configurable universal role is 2048.

15.1.2 Configuring ACL Rules for Network Services

This section describes the procedure for configuring ACLs to control access to network services

- For information on configuring access rules based on application and application categories, see Configuring ACL Rules for Application and Application Categories (Page 337).
- For information on configuring access rules based on web categories and web reputation, see Configuring Web Policy Enforcement Service (Page 341).

In the SCALANCE W UI

To configure ACL rules for a user role:

1. Navigate to **Security > Roles**. The **Roles** tab contents are displayed.

   Alternatively, you can configure access rules for a wired or wireless client through the WLAN wizard or the Wired Profile window.

   – To configure access rules through the Wired Profile window:

     Navigate to **More > Wired**.

     Click **Edit** and then **Edit Wired Network**.

     Click **Access**.

   – To configure access rules through WLAN wizard:

     Navigate to **Network > WLAN SSID**.

     Click **Edit** and then **Edit WLAN**.

     Click **Access**.

2. Select the role for which you want to configure access rules.
3. In the **Access rules** section, click **New** to add a new rule. The **New Rule** window is displayed.
4. Ensure that the rule type is set to **Access Control**.

Note

The maximum roles configurable on an AP is 32.

Note

The maximum ACL entries supported is 2048

Note

The maximum ACL entries for each role is 256

5. To configure a rule to control access to network services, select **Network** under service category and specify the following parameters:

Service Category	Description
Network	Select a service from the list of available services. You can allow or deny access to any or all of the services based on your requirement: • **any**—Access is allowed or denied to all services. • **custom**—Available options are TCP, UDP, and Other. If you select the TCP or UDP options, enter appropriate port numbers. If you select the Other option, enter the appropriate ID. **NOTE:** If TCP and UDP use the same port, ensure that you configure separate access rules to permit or deny access.
Action	Select any of following actions: • Select **Allow** to allow access to users based on the access rule. • Select **Deny** to deny access to users based on the access rule. • Select **Destination-NAT** to allow making changes to the destination IP address. • Select **Source-NAT** to allow making changes to the source IP address. **Default**: All client traffic is directed to the default VLAN. **Tunnel**: The traffic from the Network Assigned clients is directed to the VPN tunnel. **VLAN**: Specify the non-default VLAN ID to which the guest traffic needs to be redirected to.
Destination	Select a destination option for the access rules for network services, applications, and application categories. You can allow or deny access to any the following destinations based on your requirements. • **to all destinations**— Access is allowed or denied to all destinations. • **to a particular server**—Access is allowed or denied to a particular server. After selecting this option, specify the IP address of the destination server. • **except to a particular server**—Access is allowed or denied to servers other than the specified server. After selecting this option, specify the IP address of the destination server. • **to a network**—Access is allowed or denied to a network. After selecting this option, specify the IP address and netmask for the destination network. • **except to a network**—Access is allowed or denied to networks other than the specified network. After selecting this option, specify the IP address and netmask of the destination network. • **to domain name**—Access is allowed or denied to the specified domains. After selecting this option, specify the domain name in the **Domain Name** text box.
Log	Select the **Log** check box if you want a log entry to be created when this rule is triggered. SCALANCE W supports firewall-based logging. Firewall logs on the APs are generated as security logs.

Service Category	Description
Blacklist	Select the **Blacklist** check box to blacklist the client when this rule is triggered. The blacklisting lasts for the duration specified as **Auth failure blacklist time** on the Blacklisting tab of the **Security** window. For more information, see Blacklisting Clients (Page 213).
Classify media	Select the **Classify media** check box to prioritize video and voice traffic. When enabled, a packet inspection is performed on all non-NAT traffic and the traffic is marked as follows: • Video: Priority 5 (Critical) • Voice: Priority 6 (Internetwork Control)
Disable scanning	Select **Disable scanning** check box to disable ARM scanning when this rule is triggered. The selection of **Disable scanning** applies only if ARM scanning is enabled. For more information, see Configuring Radio Settings (Page 330).
DSCP tag	Select the **DSCP tag** check box to specify a DSCP value to prioritize traffic when this rule is triggered. Specify a value within the range of 0–63. To assign a higher priority, specify a higher value.
802.1p priority	Select the **802.1p priority** check box to specify an 802.1p priority. Specify a value between 0 and 7. To assign a higher priority, specify a higher value. **NOTE:** This parameter is applicable only for VLAN tagged frames.

6. Click **OK** and then click **Finish**.

In the CLI

To configure access rules:

```
(AP)(config)# wlan access-rule <access-rule-name>

(AP)(Access Rule <Name>)#rule <dest> <mask> <match/invert> {<protocol> <start-port>

<end-port> {permit|deny|src-nat [vlan <vlan_id>|tunnel]|dst-nat{<IP-address>
<port>|<port>}} [<option1....option9>]
```

Example

```
(AP)(config)# wlan access-rule employee

(AP)(Access Rule "employee")# rule 10.17.88.59 255.255.255.255 match 6 4343 4343 log
classify-media

(AP)(Access Rule "employee")# rule 192.0.2.8 255.255.255.255 invert 6 110 110 permit

(AP)(Access Rule "employee")# rule 192.0.2.2 255.255.255.0 192.0.2.7 255.255.255.0
match tcp 21 21 deny

(AP)(Access Rule "employee")# rule 192.0.2.2 255.255.255.0 192.0.2.7 255.255.255.0
match udp 21 21 deny

(AP)(Access Rule "employee")# rule 192.0.2.2 255.255.255.0 match 6 631 631 permit

(AP)(Access Rule "employee")# rule 192.0.2.8 255.255.255.255 invert 6 21 21 deny

(AP)(Access Rule "employee")# rule 192.0.2.1 255.255.255.0 invert 17 67 69 deny
```

15.1.3 Configuring NAT Rules

NAT is the process of modifying network address information when packets pass through a routing device. The routing device acts as an agent between the public (the Internet) and the private (local network), which allows translation of private network IP addresses to a public address space.

SCALANCE W supports the NAT mechanism to allow a routing device to use the translation tables for mapping the private addresses into a single IP address. When packets are sent from this address, they appear to originate from the routing device. Similarly, if packets are sent to the private IP address, the destination address is translated as per the information stored in the translation tables of the routing device.

Configuring a Source-NAT Access Rule

The source-NAT action in access rules allows the user to override the routing profile entries. For example, when a routing profile is configured to use 0.0.0.0/0, the client traffic in L3 mode access on an SSID destined to the corporate network is sent to the tunnel. When an access rule is configured with **Source-NAT** action, the users can specify the service, protocol, or destination to which the source-NAT is applied.

You can also configure source-based routing to allow client traffic on one SSID to reach the Internet through the corporate network, while the other SSID can be used as an alternate uplink. You can create an access rule to perform source-NAT by using the SCALANCE W UI or the CLI

In the SCALANCE W UI

To configure a source-NAT access rule:

1. Navigate to the WLAN wizard or the Wired settings window:
   - To configure access rules for a WLAN SSID, in the **Network** tab, click **New** to create a new network profile or click **edit** to modify an existing profile.
   - To configure access rules for a wired profile, **More > Wired**. In the **Wired** window, click **New** under **Wired Networks** to create a new network or click **Edit** to select an existing profile.
2. Click the **Access** tab.
3. To configure access rules for the network, move the slider to the **Network-based** access control type. To configure access rules for user roles, move the slider to the **Role-based** access control type.
4. To create a new rule for the network, click **New**.
5. To create an access rule for a user role, select the user role and then click **New**. The **New Rule** window is displayed.

6. In the **New Rule** window, perform the following steps:
   - Select **Access control** from the **Rule type** drop-down list.
   - Select **Source-NAT** from the **Action** drop-down list, to allow for making changes to the source IP address.
   - Select a service from the list of available services.

     Default: All client traffic by default will be directed to the native vlan.

     Tunnel: All network-based traffic will be directed to the VPN tunnel.

     VLAN: All client based traffic will be directed to the specified uplink VLAN using the IP address of the interface that AP has on that VLAN. If the interface is not found, this option has no effect.
   - Select the required option from the **Destination** drop-down list.
   - If required, enable other parameters such as **Log**, **Blacklist**, **Classify media**, **Disable scanning**, **DSCP tag**, and **802.1p priority**.
   - Click **OK**.
7. Click **Finish**.

In the CLI

To configure source-NAT access rule:

```
(AP)(config)# wlan access-rule <access_rule>

(AP)(Access Rule "<access_rule>")# rule <dest> <mask> <match> <protocol> <sport>
<eport> src-nat [vlan <vlan_id>|tunnel]
```

Configuring Policy-Based Corporate Access

To allow different forwarding policies for different SSIDs, you can configure policy-based corporate access. The configuration overrides the routing profile configuration and allows any destination or service to be configured to have direct access to the Internet (bypassing VPN tunnel) based on the ACL rule definition. When policy- based corporate access is enabled, the virtual controller performs source-NAT by using its uplink IP address.

To configure policy-based corporate access:

1. Ensure that an L3 subnet with netmask, gateway, VLAN, and IP address is configured. For more information on configuring L3 subnet, see Configuring L3-Mobility (Page 422).
2. Ensure that the source IP address is associated with the IP address configured for the L3 subnet.
3. Create an access rule for the SSID profile with Source-NAT action as described in Configuring a Source-NAT Access Rule. The source-NAT pool is configured and corporate access entry is created

Configuring a Destination-NAT Access Rule

SCALANCE W supports configuration of the destination NAT rule, which can be used to redirect traffic to the specified IP address and destination port. The destination NAT configuration is supported only in the bridge mode without VPN.

You can configure a destination NAT access rule by using the SCALANCE W UI or the CLI.

In the SCALANCE W UI

To configure a destination-NAT access rule:

1. Navigate to the WLAN wizard or the Wired settings window:
   - To configure access rules for a WLAN SSID, in the **Network** tab, click **New** to create a new network profile or click **edit** to modify an existing profile.
   - To configure access rules for a wired profile, **More > Wired**. In the **Wired** window, click **New** under **Wired Networks** to create a new network or click **Edit** to select an existing profile.
2. Click the **Access** tab and perform any of the following steps:
   - To configure access rules for the network, move the slider to the **Network-based** access control type.
   - To configure access rules for user roles, move the slider to the **Role-based** access control type.
3. To create a new rule for the network, click **New**. To create an access rule for a user role, select the user role and then click **New**. The **New Rule** window is displayed.

1. In the **New Rule** window, perform the following steps:
   - Select **Access control** from the **Rule type** drop-down list.
   - Select **destination-NAT** from the **Action** drop-down list, to allow for making changes to the source IP address.
   - Specify the IP address and port details.
   - Select a service from the list of available services.
   - Select the required option from the **Destination** drop-down list.
   - If required, enable other parameters such as **Log**, **Blacklist**, **Classify media**, **Disable scanning**, **DSCP tag**, and **802.1p priority**.
   - Click **OK**.
2. Click **Finish**.

In the CLI

To configure destination-NAT access rule:

```
(AP)(config)# wlan access-rule <access_rule>
```

```
(AP)(Access Rule "<access_rule>")# rule <dest> <mask> <match> <protocol> <sport>
<eport> dst-nat ip <IP-address> [<port>]
```

15.1.4 Configuring ALG Protocols

You can enable or disable protocols for ALG using the SCALANCE W UI or the CLI.

In the SCALANCE W UI

To enable or disable ALG protocols:

1. Click the **Security** link located directly above the Search bar on the SCALANCE W main window.
2. Click the **Firewall Settings** tab.
3. Select **Enabled** from the corresponding drop-down lists to enable SIP, VOCERA, Alcatel NOE, and Cisco Skinny protocols.
4. Click **OK**

Note

When the protocols for ALG are set to **Disabled**, the changes are not applied until the existing user sessions expire. Reboot the AP and the client, or wait for a few minutes to view the changes.

In the CLI

To configure protocols for ALG:

```
(AP)(config)# alg

(AP)(ALG)# sccp-disable

(AP)(ALG)# no sip-disable

(AP)(ALG)# no ua-disable

(AP)(ALG)# no vocera-disable
```

To view the ALG configuration:

```
(AP)# show alg
```

15.1.5 Configuring Firewall Settings for Protection from ARP Attacks

You can configure firewall settings to protect the network against attacks using the SCALANCE W UI or the CLI

In the SCALANCE W UI

To configure firewall settings:

1. Click the **Security** link located directly above the search bar on the SCALANCE W main window.
2. Click the **Firewall Settings** tab. The contents of the **Firewall Settings** tab are displayed.
3. To configure protection against security attacks, select the following check boxes:
4. Select **Enable** from the **Drop bad ARP** drop-down list to enable the AP to drop the fake ARP packets.
5. Select **Enable** from the **Fix malformed DHCP** drop-down list to enable the AP to fix the malformed DHCP packets.

6. Select **Enable** from the **ARP poison check** drop-down list to enable the AP to trigger alerts about ARP poisoning that may have been caused by rogue APs. ARP poisoning detection triggers alerts when a known client on the AP spoofs the base MAC address of the AP.
7. Click **OK.**

In the CLI

To configure firewall settings to prevent attacks:

```
(AP)(config)# attack

(AP)(ATTACK)# drop-bad-arp-enable

(AP)(ATTACK)# fix-dhcp-enable

(AP)(ATTACK)# poison-check-enable
```

To view the configuration status:

```
Current Attack

--------------

Attack Status

------ ------

drop-bad-arp Enabled fix-dhcp Enabled poison-check Enabled
```

To view the attack statistics

```
(AP)# show attack stats

attack counters
--------------------------------------
Counter


                                                                       Value
-------                                                                ------- 0
arp packet counter
drop bad arp packet counter                                            0
dhcp response packet counter                                           0
fixed bad dhcp packet counter                                          0
send arp attack alert counter                                          0
send dhcp attack alert counter                                         0
arp poison check counter                                               0
garp send check counter                                                0
```

15.1.6 Auto Topology Rules

Auto Topology is a feature that automatically adds ACL rules into the firewall. This ensures that any kind of control-plane messages required for the automatic cluster formation are never blocked. By default, this feature is enabled. However, this feature can be disabled when customers prefer full control on the security policy rather than accepting automatic ACL rules. This feature governs all the ACLs and impacts all the traffic that is hit by the ACLs.

Configuring Firewall Settings to Disable Auto Topology Rules

You can disable the rules by configuring firewall settings in the AP.

In order to deny auto topology communication outside the AP subnet, the inbound firewall settings must be enabled.

When the inbound firewall settings are enabled:

- ACEs must be configured to block auto topology messages, as there is no default rule at the top of predefined ACLs.
- ACEs must be configured to override the guest VLAN auto-expanded ACEs. In other words, the user defined ACEs take higher precedence over guest VLAN ACEs.

For more information on inbound firewall settings, see Managing Inbound Traffic (Page 228).

Note

The priority of a particular ACE is determined based on the order in which it is programmed. Ensure that you do not accidentally override the guest VLAN ACEs.

You can change the status of auto topology rules by using the SCALANCE W UI or the CLI:

In the SCALANCE W UI

1. Click the **Security** located directly above the Search bar in the SCALANCE W main window.
2. Go to the **Firewall Settings** tab.
3. In **Firewall** section, select **Disabled** from the **Auto topology rules** drop-down list.
4. Click **OK**.

In the CLI

```
(AP)(config)# firewall
```

```
(AP)(firewall)# disable-auto-topology-rules
```

To view the configuration status:

```
(AP) # show firewall
```

15.1.7 Managing Inbound Traffic

SCALANCE W now supports an enhanced inbound firewall by allowing the configuration of firewall rules and management subnets, and restricting corporate access through an uplink switch.

To allow flexibility in firewall configuration, SCALANCE W supports the following features:

- Inbound firewall rules
- Configurable management subnets
- Restricted corporate access

Configuring Inbound Firewall Rules

You can now configure firewall rules for the inbound traffic coming through the uplink ports of an AP. The rules defined for the inbound traffic are applied if the destination is not a user connected to the AP. If the destination already has a user role assigned, the user role overrides the actions or options specified in the inbound firewall configuration. However, if a deny rule is defined for the inbound traffic, it is applied irrespective of the destination and user role. Unlike the ACL rules in a WLAN SSID or a wired profile, the inbound firewall rules can be configured based on the source subnet.

Note

For all subnets, a deny rule is created by default as the last rule. If at least one rule is configured, the deny all rule is applied to the upstream traffic by default.

Note

Management access to the AP is allowed irrespective of the inbound firewall rule. For more information on configuring restricted management access, see Configuring Management Subnets.

Note

The inbound firewall is not applied to traffic coming through the GRE tunnel.

You can configure inbound firewall rules through the SCALANCE W UI or the CLI.

In the SCALANCE W UI

1. Navigate to **Security > Inbound Firewall**. The **Inbound Firewall** tab contents are displayed.
2. Under **Inbound Firewall Rules**, click **New**. The **New Rule** window is displayed.

3. Configure the following parameters:

Parameter	Description
Action	Select any of following actions: • Select **Allow** to allow to access users based on the access rule. • Select **Deny** to deny access to users based on the access rule. • Select **Destination-NAT** to allow making changes to the destination IP address. • Select **Source-NAT** to allow making changes to the source IP address. The destination-NAT and source-NAT actions apply only to the network services rules.
Service	Select a service from the list of available services. You can allow or deny access to any or all of the services based on your requirement: • **any**—Access is allowed or denied to all services. • **custom**—Available options are TCP, UDP, and Other. If you select the TCP or UDP options, enter appropriate port numbers. If the **Other** option is selected, ensure that an appropriate ID is entered.
Source	Select any of the following options: • **from all sources**—Traffic from all sources is either allowed, denied, or the IP address is translated at the source or the destination as defined in the rule. • **from a host**—Traffic from a particular host is either allowed, denied, or the IP address is translated at the source or the destination as defined in the rule. After selecting this option, specify the IP address of the host. • **from a network**—Traffic from a particular network is either allowed, denied, or the IP address is translated at the source or the destination as defined in the rule. After selecting this option, specify the IP address and netmask of the source network.

Parameter	Description
Destination	Select a destination option for the access rules for network services, applications, and application categories. You can allow or deny access to any the following destinations based on your requirements. • **to all destinations**—Traffic for all destinations is allowed, denied, or the IP address is translated at the source or the destination as defined in the rule. • **to a particular server**—Traffic to a specific server is allowed, denied, or the IP address is translated at the source or the destination as defined in the rule. After selecting this option, specify the IP address of the destination server. • **except to a particular server**—Access is allowed or denied to servers other than the specified server. After selecting this option, specify the IP address of the destination server. • **to a network**—Traffic to the specified network is allowed, denied, or the IP address is translated at the source or the destination as defined in the rule. After selecting this option, specify the IP address and netmask for the destination network. • **except to a network**—Access is allowed or denied to networks other than the specified network. After selecting this option, specify the IP address and netmask of the destination network. • **to domain name**—Traffic to the specified domain is allowed, denied, or the IP address is translated at the source or the destination as defined in the rule. After selecting this option, specify the domain name in the **Domain Name** text box.
Log	Select the **Log** check box if you want a log entry to be created when this rule is triggered. SCALANCE W supports firewall-based logging function. Firewall logs on the APs are generated as security logs.
Blacklist	Select the **Blacklist** check box to blacklist the client when this rule is triggered. The blacklisting lasts for the duration specified in the **Auth failure blacklist time** on the **Blacklisting** tab of the **Security** window. For more information, see Blacklisting Clients (Page 213).
Classify media	Select the **Classify media** check box to prioritize video and voice traffic. When enabled, a packet inspection is performed on all non-NAT traffic and the traffic is marked as follows: • Video: Priority 5 (Critical) • Voice: Priority 6 (Internetwork Control)
Disable scanning	Select **Disable scanning** check box to disable ARM scanning when this rule is triggered. The selection of **Disable scanning** applies only if ARM scanning is enabled. For more information, see Configuring Radio Settings (Page 330).
DSCP tag	Select the **DSCP tag** check box to specify a DSCP value to prioritize traffic when this rule is triggered. Specify a value within the range of 0–63. To assign a higher priority, specify a higher value.
802.1p priority	Select the **802.1p priority** check box to specify an 802.1p priority. Specify a value between 0 and 7. To assign a higher priority, specify a higher value.

4. Click **OK** and then click **Finish**.

In the CLI

To configure inbound firewall rules:

```
(AP)(config)# inbound-firewall

(AP)(inbound-firewall)# rule <subnet> <smask> <dest> <mask> <protocol> <sport>
<eport>

{permit|deny|src-nat|dst-nat <IP-address> <port>} [<option1....option9>]
```

Example

```
(AP)(config)# inbound-firewall

(AP)(inbound-firewall)# rule 192.0.2.1 255.255.255.255 any any match 6 631 631 permit
```

Configuring Management Subnets

You can configure subnets to ensure that the AP management is carried out only from these subnets. When the management subnets are configured, access through Telnet, SSH, and UI is restricted to these subnets only.

You can configure management subnets by using the SCALANCE W UI or the CLI.

In the SCALANCE W UI

To configure management subnets:

1. Navigate to **Security > Inbound Firewall** tab
2. To add a new management subnet:
   - In the **Add new management subnet** section, enter the subnet address in **Subnet**.
   - Enter the subnet mask in **Mask.**
   - Click **Add**.
3. To add multiple subnets, repeat step 2.
4. Click **OK**.

In the CLI

To configure a management subnet:

```
(AP)(config) # restricted-mgmt-access <subnet-IP-address> <subnet-mask>
```

Configuring Restricted Access to Corporate Network

You can configure restricted corporate access to block unauthorized users from accessing the corporate network. When restricted corporate access is enabled, corporate access is blocked from the uplink port of master AP, including clients connected to a slave AP. You can configure restricted corporate access by using the SCALANCE W UI or the CLI.

In the SCALANCE W UI

To configure restricted corporate access:

1. Navigate to **Security > Inbound Firewall** tab.
2. Select **Enabled** from the **Restrict Corporate Access** drop-down list.
3. Click **OK.**

In the CLI

To configure restricted management access:

```
(AP)(config) # restrict-corp-access
```

15.2 Content Filtering

The content filtering feature allows you to route DNS requests to the OpenDNS platform and create content filtering policies.

With content filter, you can achieve the following:

- Allow all DNS requests to the non-corporate domains on a wireless or wired network to be sent to the OpenDNS server. When the OpenDNS credentials are configured, the AP uses these credentials to access OpenDNS and provide enterprise-level content filtering. For more information, see Configuring OpenDNS Credentials (Page 367).
- Block certain categories of websites based on your organization policy. For example, if you block the **web- based-email** category, clients who are assigned this policy will not be able to visit email-based websites such as mail.yahoo.com.
- Prevent known malware hosts from accessing your wireless network.
- Improve employee productivity by limiting access to certain websites.
- Reduce bandwidth consumption significantly.

Note

Regardless of whether content filtering is disabled or enabled, the DNS requests to http://direct.siemens.com are always resolved internally on SCALANCE W.

The content filtering configuration applies to all APs in the network and the service is enabled or disabled globally across the wireless or wired network profiles.

Enabling Content Filtering

Enabling Content Filtering for a Wireless Profile

To enable content filtering for a wireless SSID, perform the following steps:

In the SCALANCE W UI

1. Select a wireless profile in the **Network** tab and then click the **edit** link. The window for editing the WLAN SSID profile is displayed.
2. Click **Show advanced options**.
3. Select **Enabled** from the **Content Filtering** drop-down list, and click **Next** to continue.

You can also enable content filtering while adding a new wireless profile. For more information, see Configuring WLAN Settings for an SSID Profile (Page 96)

In the CLI

To enable content filtering on a WLAN SSID:

```
(AP)(config)# wlan ssid-profile <name>

(AP)(SSID Profile <name>)# content-filtering
```

Enabling Content Filtering for a Wired Profile

To enable content filtering for a wired profile, perform the following steps:

In the SCALANCE W UI

1. Click the **Wired** link under **More** in the SCALANCE W main window. The **Wired** window is displayed.
2. In the **Wired** window, select the wired profile to modify.
3. Click **Edit**. The **Edit Wired Network** window is displayed.
4. In the **Wired Settings** tab, select **Enabled** from the **Content Filtering** drop-down list, and click **Next** to continue.

In the CLI

To enable content filtering for a wired profile in the CLI:

```
(AP)(config)# wired-port-profile test

(AP)(wired ap profile <name>)# content-filtering
```

Configuring Enterprise Domains

The enterprise domain names list displays the DNS domain names that are valid on the enterprise network. This list is used to determine how client DNS requests must be routed. When **Content Filtering** is enabled, the DNS request of the clients is verified and the domain names that do not match the names in the list are sent to the OpenDNS server.

You can configure an enterprise domain through the SCALANCE W UI or the CLI.

In the SCALANCE W UI

To manually add a domain:

1. Click the **VPN** link under **More** in the SCALANCE W main window. The **Tunnelling** window is displayed.
2. In the **Tunnelling** window, select **Enterprise Domains**.
3. Click **New** and enter a New Domain Name.
4. Click **OK** to apply the changes.

To delete a domain, select the domain and click **Delete**. This will remove the domain name from the list.

In the CLI

To configure an enterprise domain:

```
(AP)(config)# internal-domains

(AP)(domain)# domain-name <name>
```

Configuring URL Filtering Policies

You can configure URL filtering policies to block certain categories of websites based on your organization specifications by defining ACL rules either through the SCALANCE W UI or the CLI.

In the SCALANCE W UI

To control access based on web categories and security settings:

1. Navigate to **Security > Roles**.
2. Select any WLAN SSID or wired profile role, and click **New** in the Access Rules section. The New Rule window appears.
3. Select **Access Control** from the **Rule Type** drop-down list.
4. To set an access policy based on the web category:
   - Under **Service** section, select **Web category** and expand the **Web categories** drop-down list.
   - Select the categories to which you want to deny or allow access. You can also search for a web category and select the required option.
   - From the **Action** drop-down list, select **Allow** or **Deny** as required.
   - Click **OK**.
5. To filter access based on the security ratings of the website:
   - Select **Web reputation** under **Service** section.
   - Move the slider to the required security rating level.
   - From the **Action** drop-down list, select **Allow** or **Deny** as required.
6. To set a bandwidth limit based on web category or web reputation score, select **Application Throttling** check box and specify the downstream and upstream rates in Kbps. For example, you can set a higher bandwidth for trusted sites and a low bandwidth rate for high-risk sites.
7. Click **OK** to save the rules.
8. Click **OK** in the **Roles** tab to save the changes to the role for which you defined ACL rules.

In the CLI

To control access based on web categories and security ratings:

```
(AP)(config)# wlan access-rule <access_rule>
```

```
(AP)(Access Rule "<access-rule>")# rule <dest> <mask> <match> webcategory
<webgrp>{permit| deny}[<option1....option9>]
```

```
(AP)(Access Rule "<access-rule>")# rule <dest> <mask> <match> webreputation
<webrep>{permit|deny}[<option1....option9>]
```

Creating Custom Error Page for Web Access Blocked by AppRF Policies

You can create a list of URLs to which the users are redirected when they access blocked websites. You can define an access rule to use these redirect URLs and assign the rule to a user role in the WLAN network.

You can create a list of custom URLs and ACL rules for blocked websites either through the SCALANCE W UI or the CLI.

Creating a List of Error Page URLs

To create a list of error page URLs:

In the SCALANCE W UI

1. Navigate to **Security > Custom Blocked Page URL**.
2. Click **New** and enter the URL that you want to block.
3. Repeat the procedure to add more URLs. You can add up to 8 URLs to the blocked page list.
4. Click **OK**.

In the CLI

```
(AP)(config)# dpi-error-page-url <idx> <url>
```

Configuring ACL Rules to Redirect Blocked HTTP Websites to a Custom Error Page URL

To redirect blocked HTTP websites to a custom error page URL:

In the SCALANCE W UI

1. Navigate to **Security > Roles**.
2. Select any WLAN SSID or Wired profile role, and click **New** in the Access Rules section.
3. In the **New Rule** window, select the rule type as **Blocked Page URL**.
4. Select the URLs from the existing list of custom redirect URLs. To add a new URL, click **New**.
5. Click **OK**.
6. Click **OK** in the **Roles** tab to save the changes

In the CLI

To configure an ACL rule to redirect blocked HTTP websites to a custom error page URL:

```
(AP)(config)# wlan access-rule <access_rule_name>

(AP) (Access Rule "<access_rule_name>")# dpi-error-page-url <idx>
```

Configuring ACL Rules to Redirect Blocked HTTPS Websites to a Custom Blocked Page URL

Note

Before you configure an ACL rule for a specific WLAN SSID or Wired profile to redirect HTTPS websites to a custom error page, you must ensure that the Blocked Page URL rule is configured for the HTTP websites blocked for the same WLAN SSID or Wired profile. In this scenario, all the blocked HTTP and HTTPS websites will be redirected to the custom error page URL

To redirect blocked HTTPS websites to a custom error page URL

In the SCALANCE W UI

1. Navigate to **Security > Roles**.
2. Select any WLAN SSID or Wired profile role, and click **New** in the Access Rules section.
3. In the **New Rule** window, select the rule type as **Redirect Blocked HTTPS**.
4. Click **OK**.
5. Click **OK** in the **Roles** tab to save the changes

In the CLI

To configure an ACL rule to redirect blocked HTTPS to a custom error page URL:

```
(AP)(config)# wlan access-rule <access_rule_name>

(AP) (Access Rule "<access_rule_name>")# dpi-error-page-url <idx>

(AP) (Access Rule "<access_rule_name>")# redirect-blocked-https-traffic
```

15.3 Configuring User Roles

Every client in the SCALANCE W network is associated with a user role that determines the network privileges for a client, the frequency of reauthentication, and the applicable bandwidth contracts.

Note

SCALANCE W allows you to configure up to 32 user roles. If the number of roles exceed 32, an error message is displayed.

The user role configuration on an AP involves the following procedures:

- Creating a User Role
- Assigning Bandwidth Contracts to User Roles
- Configuring Machine and User Authentication Roles

Creating a User Role

You can create a user role by using the SCALANCE W UI or the CLI.

In the SCALANCE W UI

To create a user role:

1. Click the **Security** link located directly above the Search bar in the SCALANCE W main window. The **Security** window is displayed.
2. Click the **Roles** tab. The Roles tab contents are displayed.
3. Under Roles, click **New**.
4. Enter a name for the new role and click **OK**.

Note

You can also create a user role when configuring wireless or wired network profiles. For more information, see Configuring Access Rules for a WLAN SSID Profile (Page 111) and Configuring Access Rules for a Wired Profile (Page 131).

In the CLI

To configure user roles and access rules:

```
(AP)(config)# wlan access-rule <access-rule-name>
```

```
(AP)(Access Rule <Name>)# rule <dest> <mask> <match> <protocol> <start-port> <end-
port> {permit|deny|src-nat [vlan <vlan_id>|tunnel]|dst-nat {<IP-address>
<port>|<port>}} [<option1…option9>]
```

Assigning Bandwidth Contracts to User Roles

The administrators can manage bandwidth utilization by assigning either maximum bandwidth rates, or bandwidth contracts to user roles. The administrator can assign a bandwidth contract configured in Kbps to upstream (client to the AP) or downstream (AP to clients) traffic for a user role.

By default, all users that belong to the same role share a configured bandwidth rate for upstream or downstream traffic. The assigned bandwidth will be served and shared among all the users. You can also assign bandwidth rate per user to provide every user a specific bandwidth within a range of 1–65,535 Kbps. If there is no bandwidth contract specified for a traffic direction, unlimited bandwidth is allowed.

The bandwidth contract for a user role can be applied to an AP or to a cluster.

Example

In a cluster of 5 APs with an upstream WAN limit of 100 Mbps, you must set the WAN limit to 20 Mbps for each AP, in order to meet the requirement of maintaining the WAN limit of 100 Mbps. However, clients cannot exceed 20 Mbps when needed, even if the cluster output is less than 100 Mbps.If you want to add more APs, you must re-calculate the WAN limit and manually apply it. It is recommended that you apply the WAN limit at cluster level as it is more flexible. Also, there is no need to manually re-calculate the WAN limit if additional APs are added or removed, in order to meet the upstream WAN constraints.

In the SCALANCE W UI

1. Click the **Security** link located directly above the Search bar in the SCALANCE W main window. The **Security** window is displayed.
2. Click the **Roles** tab. The Roles tab contents are displayed.
3. Create a new role (see Creating a User Role) or select an existing role
4. Under **Access Rules**, click **New**. The **New Rule** window is displayed.
5. Select **Bandwidth Contract** from the **Rule Type** drop-down list.
6. Specify the downstream and upstream rates in Kbps. If the assignment is specific for each user, select the **Peruser** check box
7. Click **OK**.
8. Associate the user role to a WLAN SSID or a wired profile

You can also create a user role and assign bandwidth contracts when configuring an SSID or a wired profile.

In the CLI

To assign a bandwidth contract in the CLI:

```
(AP)(config)# wlan access-rule <name>

(AP) (Access Rule <name>)# bandwidth-limit {downstream <kbps>|upstream <kbps>|peruser

{downstream <kbps>| upstream <kbps>}}
```

To associate the access rule to a wired profile:

```
(AP)(config)# wired-port-profile <name>

(AP)(wired ap profile <name>)# access-rule-name <access-rule-name>
```

Configuring Machine and User Authentication Roles

You can assign different rights to clients based on whether their hardware device supports machine authentication. Machine authentication is only supported on Windows devices, so that this can be used to distinguish between Windows devices and other devices such as iPads.

You can create any of the following types of rules:

- **Machine Auth only** role—This indicates a Windows machine with no user logged in. The device supports machine authentication and has a valid RADIUS account, but a user has not yet logged in and authenticated.
- **User Auth only** role—This indicates a known user or a non-Windows device. The device does not support machine authentication or does not have a RADIUS account, but the user is logged in and authenticated.

When a device does both machine and user authentication, the user obtains the default role or the derived role based on the RADIUS attribute.

You can configure machine authentication with role-based access control using the SCALANCE W UI or the CLI.

In the SCALANCE W UI

To configure machine authentication with role-based access control:

1. In the **Access** tab of the WLAN wizard (**New WLAN** or **Edit <WLAN-profile>**) or in the wired profile configuration window (**New Wired Network** or **Edit Wired Network**), under **Roles**, create **Machine auth only** and **User auth only** roles.
2. Configure access rules for these roles by selecting the role, and applying the rule. For more information on configuring access rules, see Configuring ACL Rules for Network Services. (Page 220)
3. Select **Enforce Machine Authentication** and select the **Machine auth only** and **User auth only** roles.
4. Click **Finish** to apply these changes

In the CLI

To configure machine and user authentication roles for a WLAN SSID:

```
(AP)(config)# wlan ssid-profile <name>

(AP)(SSID Profile <name>)# set-role-machine-auth <machine_only> <user_only>
```

To configure machine and user authentication roles for a wired profile:

```
(AP)(config)# wired-port-profile <name>

(AP)(wired ap profile <name>)# set-role-machine-auth <machine_only> <user_only>
```

15.4 Configuring Derivation Rules

SCALANCE W allows you to configure role and VLAN derivation-rules. You can configure these rules to assign a user role or a VLAN to the clients connecting to an SSID or a wired profile.

15.4.1 Understanding Role Assignment Rule

When an SSID or a wired profile is created, a default role for the clients connecting to this SSID or wired profile is assigned. You can assign a user role to the clients connecting to an SSID by any of the following methods.

The role assigned by some methods may take precedence over the roles assigned by the other methods.

RADIUS VSA Attributes

The user role can be derived from VSA for RADIUS server authentication. The role derived from an VSA takes precedence over roles defined by other methods.

MAC-Address Attribute

The first three octets in a MAC address are known as OUI, and are purchased from the IEEE, Incorporated RA. This identifier uniquely identifies a vendor, manufacturer, or other organization (referred to by the IEEE as the “assignee”) globally and effectively reserves a block of each possible type of derivative identifier (such as MAC addresses) for the exclusive use of the assignee.

APs use the OUI part of a MAC address to identify the device manufacturer and can be configured to assign a desired role for users who have completed 802.1X authentication and MAC authentication. The user role can be derived from the user attributes after a client associates with an AP. You can configure rules to assign a user role to clients that match a MAC-address-based criteria. For example, you can assign a voice role to any client with a MAC address starting with a0:a1:a2.

Roles Based on Client Authentication

The user role can be the default user role configured for an authentication method, such as 802.1X authentication. For each authentication method, you can configure a default role for the clients who are successfully authenticated using that method.

15.4.2 Understanding Device Identification

The device identification feature allows you to assign a user role or VLAN to a specific device type by identifying a DHCP option and signature for that device. If you create a user role with the **DHCP-Option** rule type, the first two characters in the attribute value must represent the hexadecimal value of the DHCP option that this rule should match with, while the rest of the characters in the attribute value indicate the DHCP signature the rule should match with. To create a rule that matches DHCP option 12 (host name), the first two characters of the in the attribute value must be the hexadecimal value of 12, which is 0C. To create a rule that matches DHCP option 55, the first two characters in the attribute value must be the hexadecimal value of 55, which is 37

The following table describes some of the DHCP options that are useful for assigning a user role or VLAN:

Table 15- 1 DHCP Option Values

DHCP Option	Description	Decimal Value	Hexadecimal Value
Hostname	The name of the client device.	12	0C
Parameter Request List	The configuration values requested by the client.	55	37
Vendor Class Identifier	Vendors use the option to convey configuration information about the client to the Server.	60	3C
Client Identifier	Clients use this option to uniquely identify themselve sand value corresponds to the MAC address of client.	61	3D
Client FQDN	The FQDN name of the client with the domain name.	81	51

DHCP Option and DHCP Fingerprinting

The DHCP fingerprinting allows you to identify the operating system of a device by looking at the options in the DHCP frame. Based on the operating system type, a role can be assigned to the device.

For example, to create a role assignment rule with the DHCP option, select **equals** from the **Operator** drop- down list and enter 370103060F77FC in the **String** text box. Since 370103060F77FC is the fingerprint for Apple iOS devices such as iPad and iPhone, AP assigns Apple iOS devices to the role that you choose.

Table 15- 2 *Validated DHCP Fingerprint*

Device	DHCP Option	DHCP Fingerprint
Apple iOS	Option 55	370103060F77FC
Android	Option 60	3C64686370636420342E302E3135
Blackberry	Option 60	3C426C61636B4265727279
Windows 7/Vista Desktop	Option 55	37010f03062c2e2f1f2179f92b
Windows XP (SP3, Home, Professional)	Option 55	37010f03062c2e2f1f21f92b
Windows Mobile	Option 60	3c4d6963726f736f66742057696e646f777320434500
Windows 7 Phone	Option 55	370103060f2c2e2f
Apple Mac OS X	Option 55	370103060f775ffc2c2e2f

15.4.3 Creating a Role Derivation Rule

You can configure rules for determining the role that is assigned for each authenticated client

Note

When creating more than one role assignment rule, the first matching rule in the rule list is applied.

You can create a role assignment rule by using the SCALANCE W UI or the CLI.

In the SCALANCE W UI

1. Navigate to the WLAN wizard or the Wired settings window:
   - To configure access rules for a WLAN SSID, in the **Network** tab, click **New** to create a new network profile or **edit** to modify an existing profile.
   - To configure access rules for a wired profile, go to **More > Wired**. In the **Wired** window, click **New** under **Wired Networks** to create a new network or click **Edit** to select an existing profile.
2. Click the **Access** tab.
3. Under **Role Assignment Rules**, click **New**. The **New Role Assignment** window allows you to define a match method by which the string in *Operand* is matched with the attribute value returned by the authentication server.
4. Select the attribute that matches with the rule from the **Attribute** drop-down list. The list of supported attributes includes RADIUS attributes, dhcp-option, dot1x-authentication-type, mac-address, and mac- address-and-dhcp-options. For information on a list of RADIUS attributes, see RADIUS Server Authentication with VSA (Page 182).
5. Select the operator from the **Operator** drop-down list. The following types of operators are supported:
   - **contains**—The rule is applied only if the attribute value contains the string specified in *Operand*.
   - **Is the role**—The rule is applied if the attribute value is the role.
   - **equals**—The rule is applied only if the attribute value is equal to the string specified in *Operand*.
   - **not-equals**—The rule is applied only if the attribute value is not equal to the string specified in *Operand*.
   - **starts-with**—The rule is applied only if the attribute value starts with the string specified in *Operand*.
   - **ends-with**—The rule is applied only if the attribute value ends with the string specified in *Operand*.
   - **matches-regular-expression**—The rule is applied only if the attribute value matches the Regex pattern specified in *Operand*. This operator is available only if the **mac-address-and-dhcp-options** attribute is selected in the **Attribute** drop-down list. The **mac-address-and-dhcp-options** attribute and **matches-regular-expression** are applicable only for the WLAN clients.
6. Enter the string to match the attribute in the **String** text box.

7. Select the appropriate role from the **Role** drop-down list.
8. Click **OK**.

Note

When **Enforce Machine Authentication** is enabled, both the device and the user must be authenticated for the role assignment rule to apply.

Note

Each device type may not have a unique DHCP fingerprint signature. For example, devices from different manufacturers may use vendor class identifiers that begin with similar strings. If you create a DHCP Option rule that uses the **starts-with** condition instead of the **equals** condition, the rule may assign a role or VLAN to more than one device type.

In the CLI

To configure role assignment rules for a WLAN SSID:

```
(AP)(config)# wlan ssid-profile <name>
```

```
(AP)(SSID Profile <name>)# set-role <attribute>{{equals|not-equals|starts-with|ends-with|contains|matches-regular-expression} <operator><role>|value-of}
```

To configure role assignment rules for a wired profile:

```
(AP)(config)# wired-port-profile <name>
```

```
(AP)(wired ap profile <name>)# set-role <attribute>{{equals|not-equal|starts-with|ends-with|contains}<operator> <role>|value-of}
```

Example

```
(AP)(config)# wlan ssid-profile Profile1
```

```
(AP)(SSID Profile "Profile1")# set-role mac-address-and-dhcp-options matches-regular-expression \bring\b Profile1
```

15.4.4 Understanding VLAN Assignment

You can assign VLANs to a client based on the following configuration conditions:

The default VLAN configured for the WLAN can be assigned to a client.

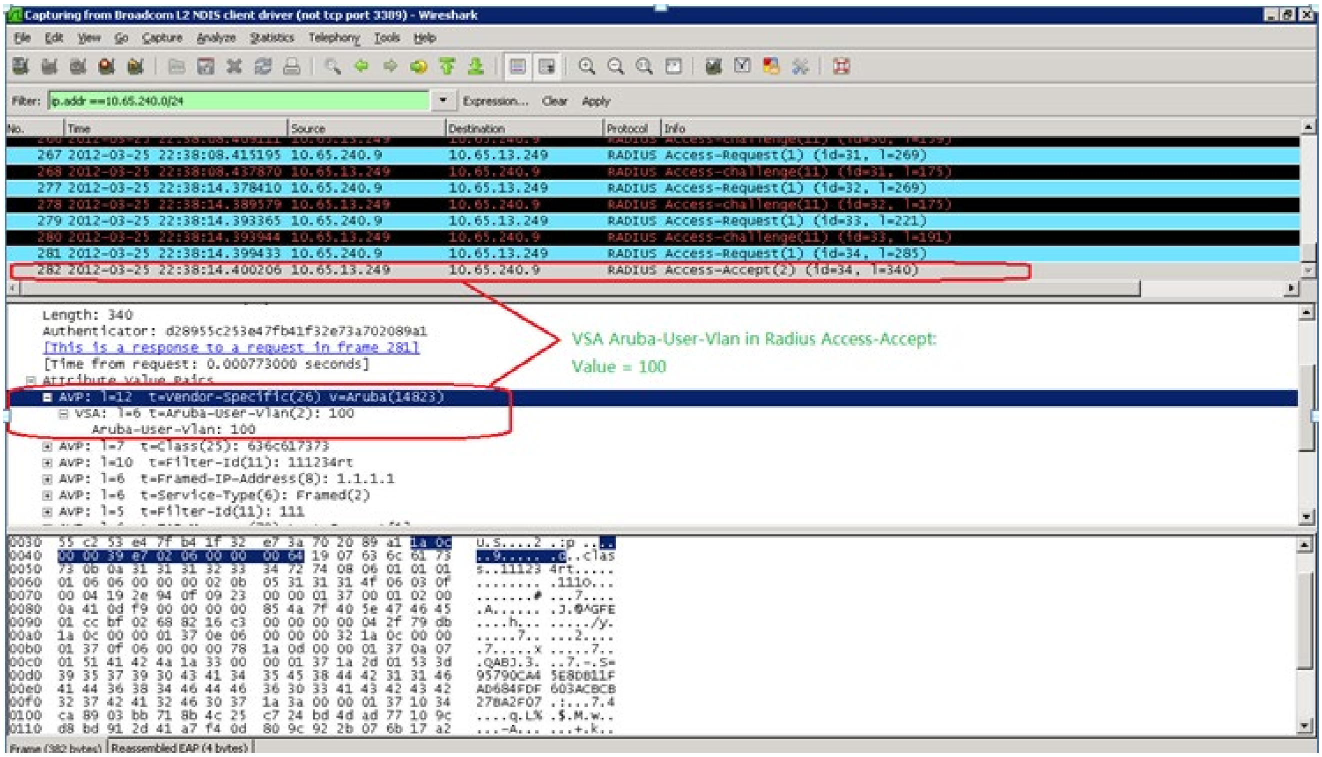
- If VLANs are configured for a WLAN SSID or an Ethernet port profile, the VLAN for the client can be derived before the authentication, from the rules configured for these profiles.
- If a rule derives a specific VLAN, it is prioritized over the user roles that may have a VLAN configured.
- The user VLANs can be derived from the default roles configured for 802.1X authentication or MAC authentication.
- After client authentication, the VLAN can be derived from VSA for RADIUS server authentication.
- The DHCP-based VLANs can be derived for captive portal authentication

Note

SCALANCE W supports role derivation based on the DHCP option for captive portal authentication. When the captive portal authentication is successful, the role derivation based on the DHCP option assigns a new user role to the guest users, instead of the pre-authenticated role.

VSA

When an external RADIUS server is used, the user VLAN can be derived from the VSA. The VSA is then carried in an *Access-Accept* packet from the RADIUS server. The AP can analyze the return message and derive the value of the VLAN which it assigns to the user.


Capturing from Broadcom L2 NDIS client driver (not tcp port 3389) - Wireshark
File
Edit
View
Go
Capture
Analyze
Statistics
Telephony
Tools
Help
Expression...
Clear
Apply
Frame (382 bytes)
Reassembled EAP (4 bytes)

Filter: ip.addr ==10.65.240.0/24

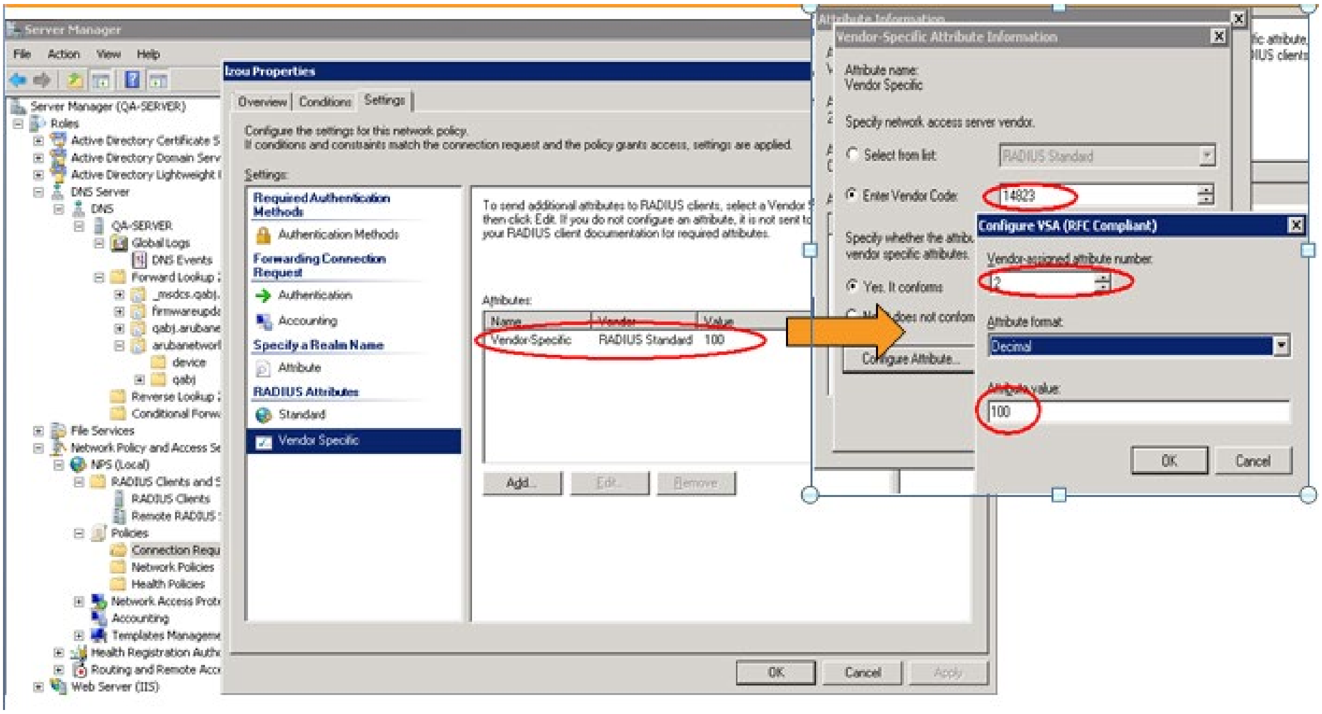
```
No.  Time                        Source          Destination     Protocol Info
267 2012-03-25 22:38:08.415195 10.65.240.9    10.65.13.249    RADIUS Access-Request(1) (id=31, l=269)
268 2012-03-25 22:38:08.437870 10.65.13.249   10.65.240.9     RADIUS Access-challenge(11) (id=31, l=175)
277 2012-03-25 22:38:14.378410 10.65.240.9    10.65.13.249    RADIUS Access-Request(1) (id=32, l=269)
278 2012-03-25 22:38:14.389579 10.65.13.249   10.65.240.9     RADIUS Access-challenge(11) (id=32, l=175)
279 2012-03-25 22:38:14.393365 10.65.240.9    10.65.13.249    RADIUS Access-Request(1) (id=33, l=221)
280 2012-03-25 22:38:14.393944 10.65.13.249   10.65.240.9     RADIUS Access-challenge(11) (id=33, l=191)
281 2012-03-25 22:38:14.399433 10.65.240.9    10.65.13.249    RADIUS Access-Request(1) (id=34, l=285)
282 2012-03-25 22:38:14.400206 10.65.13.249   10.65.240.9     RADIUS Access-Accept(2) (id=34, l=340)
```

```
    Length: 340
    Authenticator: d28955c253e47fb41f32e73a702089a1
    [This is a response to a request in frame 281]
    [Time from request: 0.000773000 seconds]
  ⊟ Attribute Value Pairs
    ⊟ AVP: l=12  t=Vendor-Specific(26) v=Aruba(14823)
      ⊟ VSA: l=6 t=Aruba-User-Vlan(2): 100
          Aruba-User-Vlan: 100
    ⊞ AVP: l=7  t=Class(25): 636c617373
    ⊞ AVP: l=10  t=Filter-Id(11): 111234rt
    ⊞ AVP: l=6  t=Framed-IP-Address(8): 1.1.1.1
    ⊞ AVP: l=6  t=Service-Type(6): Framed(2)
    ⊞ AVP: l=5  t=Filter-Id(11): 111
```

VSA Aruba-User-Vlan in Radius Access-Accept:
Value = 100

```
0030  55 c2 53 e4 7f b4 1f 32  e7 3a 70 20 89 a1 1a 0c   U.S....2 .:p ....
0040  00 00 39 e7 02 06 00 00  00 64 19 07 63 6c 61 73   ..9..... .d..clas
0050  73 0b 0a 31 31 31 32 33  34 72 74 08 06 01 01 01   s..11123 4rt.....
0060  01 06 06 00 00 00 02 0b  05 31 31 31 4f 06 03 0f   ........ .111o...
0070  00 04 19 2e 94 0f 09 23  00 00 01 37 00 01 02 00   .......# ...7....
0080  0a 41 0d f9 00 00 00 00  85 4a 7f 40 5e 47 46 45   .A...... .J.@^GFE
0090  01 cc bf 02 68 82 16 c3  00 00 00 00 04 2f 79 db   ....h... ...../y.
00a0  1a 0c 00 00 01 37 0e 06  00 00 00 32 1a 0c 00 00   .....7.. ...2....
00b0  01 37 0f 06 00 00 00 78  1a 0d 00 00 01 37 0a 07   .7.....x .....7..
00c0  01 51 41 42 4a 1a 33 00  00 01 37 1a 2d 01 53 3d   .QABJ.3. ..7.-.S=
00d0  39 35 37 39 30 43 41 34  35 45 38 44 42 31 31 46   95790CA4 5E8DB11F
00e0  41 44 36 38 34 46 44 46  36 30 33 41 43 42 43 42   AD684FDF 603ACBCB
00f0  32 37 42 41 32 46 30 37  1a 3a 00 00 01 37 10 34   27BA2F07 .:...7.4
0100  ca 89 03 bb 71 8b 4c 25  c7 24 bd 4d ad 77 10 9c   ....q.L% .$.M.w..
0110  d8 bd 91 2d 41 a7 f4 0d  80 9c 92 2b 07 6b 17 a2   ...-A... ...+.k..
```

Figure 15-1 RADIUS Access-Accept Packets with VSA



Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.

Settings:

To send additional attributes to RADIUS clients, select a Vendor S then click Edit. If you do not configure an attribute, it is not sent to your RADIUS client documentation for required attributes.

Attributes:

Name	Vendor	Value
Vendor-Specific	RADIUS Standard	100

Attribute name:
Vendor Specific

Specify network access server vendor.

○ Select from list: RADIUS Standard

● Enter Vendor Code: 14823

Specify whether the attrib vendor specific attributes.

● Yes. It conforms

○ No. It does not conform

Vendor-assigned attribute number: 2

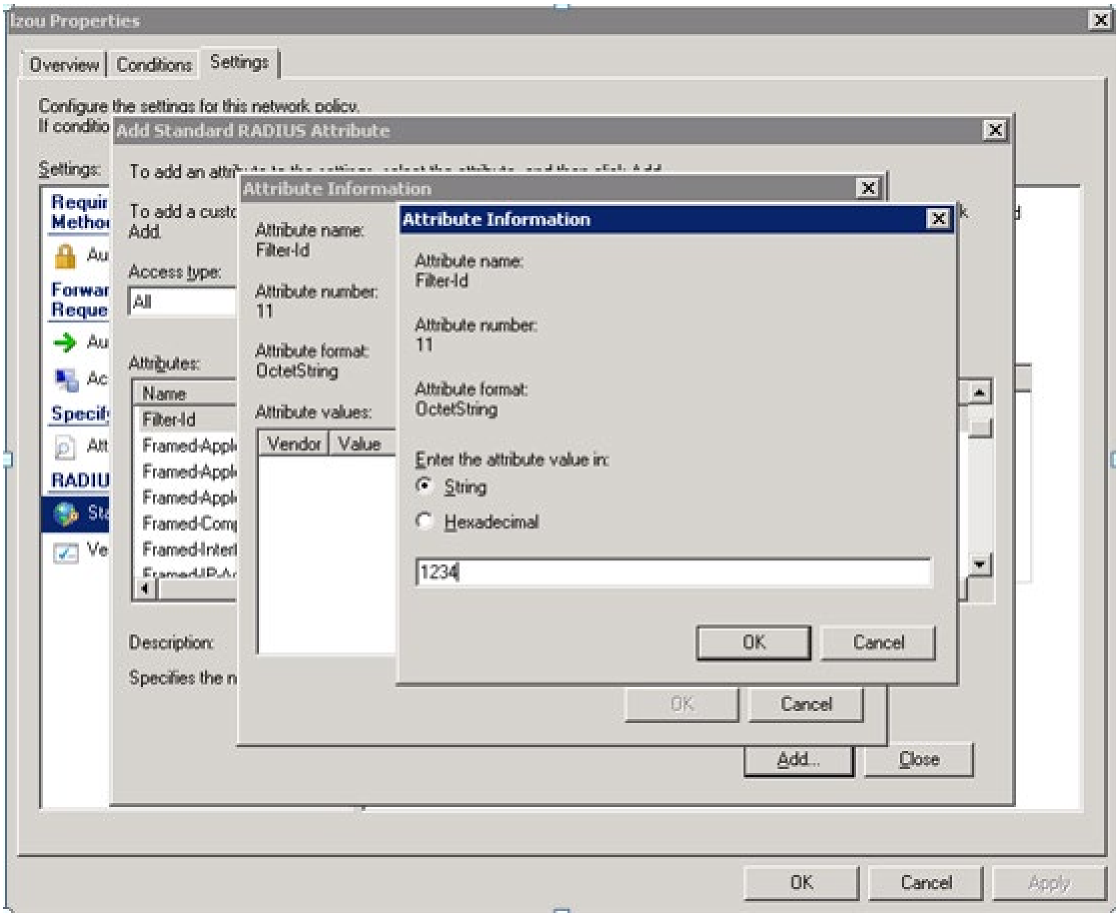
Attribute format: Decimal

Attribute value: 100

Figure 15-2 Configure VSA on a RADIUS Server

VLAN Assignment Based on Derivation Rules

When an external RADIUS server is used for authentication, the RADIUS server may return a reply message for authentication. If the RADIUS server supports return attributes, and sets an attribute value to the reply message, the AP can analyze the return message and match attributes with a user pre-defined VLAN derivation rule. If the rule is matched, the VLAN value defined by the rule is assigned to the user. For a complete list of RADIUS server attributes, see RADIUS Server Authentication with VSA (Page 188).



Attribute Information

Attribute name:
Filter-Id

Attribute number:
11

Attribute format:
OctetString

Enter the attribute value in:
● String
○ Hexadecimal

1234

Figure 15-3 Configuring RADIUS Attributes on the RADIUS Server

User Role

If the VSA and VLAN derivation rules are not matching, then the user VLAN can be derived by a user role.

VLANs Created for an SSID

If the VSA and VLAN derivation rules are not matching, and the User Role does not contain a VLAN, the user VLAN can be derived by VLANs configured for an SSID or an Ethernet port profile.

15.4.5 Configuring VLAN Derivation Rules

The VLAN derivation rules allow administrators to assign a VLAN to the AP clients based on the attributes returned by the RADIUS server.

You can configure VLAN derivation rules for an SSID profile by using the SCALANCE W UI or the CLI.

In the SCALANCE W UI

To configure VLAN derivation rules:

1. Perform the following steps:
   - To configure VLAN derivation rule for a WLAN SSID profile, navigate to **Network > New > New WLAN > VLAN** or **Network > edit > Edit <WLAN-profile> > VLAN**. Select the **Dynamic** option under the Client VLAN assignment**.**
   - To configure VLAN derivation rule for a wired network profile, navigate to **Wired > New > New Wired Network > VLAN** or **Wired > Edit > Edit Wired Network > VLAN**. The **VLAN** tab contents are displayed.
2. Click **New** to create a VLAN assignment rule. The **New VLAN Assignment Rule** window is displayed. In this window, you can define a match method by which the string in *Operand* is matched with the attribute values returned by the authentication server.
3. Select the attribute from the **Attribute** drop-down list. The list of supported attributes includes RADIUS attributes, dhcp-option, dot1x-authentication-type, mac-address, and mac-address-and-dhcp-options. For information on a list of RADIUS attributes, see RADIUS Server Authentication with VSA. (Page 188)
4. Select the operator from the **Operator** drop-down list. The following types of operators are supported:
   - **contains**—The rule is applied only if the attribute value contains the string specified in *Operand*.
   - **Is the VLAN**—The rule is applied if the VLAN is the same as the one returned by the RADIUS attribute.
   - **equals**—The rule is applied only if the attribute value is equal to the string specified in *Operand*.
   - **not equals** —The rule is applied only if the attribute value is not equal to the string specified in *Operand.*
   - **starts-with**—The rule is applied only if the attribute value starts with the string specified in *Operand*.
   - **ends-with**—The rule is applied only if the attribute value ends with the string specified in *Operand*.
5. Enter the string to match the attribute in the **String** text box.
6. Select the appropriate VLAN ID from the **VLAN** drop-down list.
7. Click **OK**.
8. Ensure that the required security and access parameters are configured.
9. Click **Finish** to apply the changes.

In the CLI

To create a VLAN assignment rule for a WLAN SSID:

```
(AP)(config)# wlan ssid-profile <name>
```

```
(AP)(SSID Profile <name>)# set-vlan <attribute>{equals|not-equals|starts-with|ends-
with|contains}<operator><VLAN-ID>|value-of}
```

To configure a VLAN assignment rule for a wired profile:

```
(AP)(config)# wired-port-profile <nname>
```

```
(AP)(wired ap profile <name>)# set-vlan <attribute>{equals|not-equals|starts-
with|ends-with|contains}<operator><VLAN-ID>|value-of}
```

Example

```
(AP)(config)# wlan ssid-profile Profile1
```

```
(AP)(SSID Profile "Profile1")# set-vlan mac-address-and-dhcp-options matches-regular-
expression ..link 100
```

15.5 Using Advanced Expressions in Role and VLAN Derivation Rules

For complex policies of role and VLAN derivation using device DHCP fingerprints, you can use a Regex to match with the combined string of the MAC address and the DHCP options. The combined string is formed by concatenating the hexadecimal presentation of the MAC address and all of the DHCP options sent by a particular device. The Regex is a powerful pattern description language that can be used to perform advanced pattern matching of the above string.

If the combined device fingerprint string matches the specified Regex, the role or VLAN can be set to the WLAN client.

The following table lists some of the most commonly used Regex, which can be used in user role and user VLAN derivation rules:

Table 15- 3 Regular Expressions

Operator	Description
.	Matches any character. For example, l..k matches lack, lark, link, lock, look, Lync, and so on.
\	Matches the character that follows the backslash. For example, \192.\.0\.. matches IP address ranges that start with 192.0, such as 192.0.1.1. The expression looks up only for the single characters that match.
[ ]	Matches any one character listed between the brackets. For example, [bc]lock matches block and clock.
\b	Matches the words that begin and end with the given expression. For example, \bdown matches downlink, linkdown, shutdown.
\B	Matches the middle of a word. For example, \Bvice matches services, devices, serviceID, deviceID, and so on.
^	Matches the characters at starting position in a string. For example, ^bcd matches bcde or bcdf, but not abcd.
[^]	Matches any characters that are not listed between the brackets. For example, [^u]link matches downlink, link, but not uplink.

Operator	Description
?	Matches any one occurrence of the pattern. For example, ?est matches best, nest, rest, test, and so on.
$	Matches the end of an input string. For example, eth$ matches Eth, but not Ethernet.
*	Matches the declared element multiple times if it exists. For example, eth* matches all occurrences of eth, such as Eth, Ethernet, Eth0, and so on.
+	Matches the declared element one or more times. For example, aa+ matches occurrences of aa and aaa.
( )	Matches nested characters. For example, (192)* matches any number of the character string 192.
|	Matches the character patterns on either side of the vertical bar. You can use this expression to construct a series of options.
\<	Matches the beginning of the word. For example, \<wire matches wired, wireless, and so on.
\>	Matches the end of the word. For example, \>list matches blacklist, whitelist, and so on.
{n}	Where n is an integer. Matches the declared element exactly n times. For example, {2}link matches uplink, but not downlink.
{n,}	Where n is an integer. Matches the declared element at n times. For example, {2,}ink matches downlink, but not uplink.

For information on how to use regular expressions in role and VLAN derivation rules, see the following topics:

- Creating a Role Derivation Rule (Page 243)
- Configuring VLAN Derivation Rules (Page 249)

15.6 Configuring a User Role for VLAN Derivation

Creating a User VLAN Role

You can create a user role for VLAN derivation using the SCALANCE W UI or the CLI.

In the SCALANCE W UI

To configure a user role for VLAN derivation:

1. Click the **Security** link located directly above the Search bar in the SCALANCE W main window.
2. Click the **Roles** tab. The Roles tab contents are displayed.
3. Under **Roles**, click **New**.
4. Enter a name for the new role and click **OK**.
5. Under **Access rules**, click **New**.
6. Select the **Rule type** as **VLAN assignment**.
7. Enter the ID of the VLAN in the **VLAN ID** text box.
8. Click **OK**.

In the CLI

To create a VLAN role:

```
(AP)(config)# wlan access-rule <rule-name>

(AP)(Access Rule <rule-name>)# vlan 200
```

Assigning User VLAN Roles to a Network Profile

You can configure user VLAN roles for a network profile using SCALANCE W UI or the CLI.

In the SCALANCE W UI

To assign a user VLAN role:

1. **Click** Network > New > New WLAN > Access **or click** Network > edit > Edit <WLAN-profile> > Access**.**
2. On the **Access** tab, ensure that the slider is at the **Role-based** option.
3. Click **New** under the **New Role Assignment** and configure the following parameters:
   – Select the attribute from the **Attribute** drop-down list.
   – Select the operator to match attribute from the **Operator** drop-down list.
   – Enter the string to match in the **String** text box.
   – Select the role to be assigned from the **Role** text box.
4. Click **OK**.

In the CLI

To assign VLAN role to a WLAN profile:

```
(AP)(config)# wlan ssid-profile <name>

(AP)(SSID Profile <name>)# set-role <attribute>{{equals <operator> <role>|not-equals
<operator> <role>|starts-with <operator> <role>|ends-with <operator> <role>|contains
<operator> <role>}|value-of}
```

DHCP Configuration 16

16.1 Configuring DHCP Scopes

The virtual controller supports different modes of DHCP address assignment. With each DHCP address assignment mode, various client traffic forwarding modes are associated. For more information on client traffic forwarding modes for AP-VPN, see AP-VPN Forwarding Modes (Page 283).

Note

When using a local DHCP scope in an AP cluster, ensure that the VLANs configured for this DHCP scope is allowed in the uplink switch.

Note

In a single AP network, when using a client DHCP scope for wired clients, ensure that client VLAN is not added in the allowed VLAN list for the port to which the AP Ethernet 0 port is connected.

16.1.1 Configuring Local DHCP Scopes

You can configure Local; Local, L2; and Local, L3 DHCP scopes through the SCALANCE W UI or the CLI.

- **Local**—In this mode, the virtual controller acts as both the DHCP server and the default gateway. The configured subnet and the corresponding DHCP scope are independent of the subnets configured in other AP clusters. The virtual controller assigns an IP address from a local subnet and forwards traffic to both **corporate** and **non-corporate** destinations. The network address is translated appropriately and the packet is forwarded through the IPsec tunnel or through the uplink. This DHCP assignment mode is used in the NAT forwarding mode.
- **Local, L2**—In this mode, the virtual controller acts as a DHCP server and the gateway located outside the AP.
- **Local, L3**—This DHCP assignment mode is used with the L3 forwarding mode. In this mode, the virtual controller acts as a DHCP server and the gateway, and assigns an IP address from the local subnet. The AP routes the packets sent by clients on its uplink. The Local, L3 subnets can access corporate network through the IPsec tunnel. The network address for all client traffic, which is generated in the Local, L3 subnets and destined to the corporate network, is translated at the source with the tunnel inner IP. However, if corporate access to Local, L3 is not required, you can configure ACL rules to deny access.

In the SCALANCE W UI

To configure a Local or a Local, L3 DHCP scope:

1. Click **More > DHCP Server**. The **DHCP Server** window is displayed.
2. To configure a **Local**; **Local, L2**; or **Local, L3** DHCP scopes, click **New** under **Local DHCP Scopes**. The **New DHCP Scope** window is displayed.
3. Based on the type of DHCP scope selected, configure the following parameters.

Parameter	**Description**
Name	Enter a name for the DHCP scope.
Type	Select any of the following options: • **Local**—On selecting **Local**, the DHCP server for local branch network is used for keeping the scope of the subnet local to the AP. In the NAT mode, the traffic is forwarded through the IPsec tunnel or the uplink. • **Local, L2**—On selecting **Local, L2**, the virtual controller acts as a DHCP server and a default gateway in the local network that is used. • **Local, L3**—On selecting **Local, L3**, the virtual controller acts as a DHCP server and a gateway. In this mode, the network address for traffic destined to the corporate network is translated at the source with the inner IP of the IPsec tunnel and is forwarded through the IPsec tunnel. The traffic destined to the non-corporate network is routed.
VLAN	Specify a VLAN ID. To use this subnet, ensure that the VLAN ID specified here is assigned to an SSID profile. For more information on SSID profile configuration, see Configuring VLAN Settings for a WLAN SSID Profile (Page 101) and Configuring VLAN for a Wired Profile (Page 127).
Network	Specify the network to use.
Netmask	If **Local**; **Local, L2**; or **Local, L3** is selected, specify the subnet mask. The subnet mask and the network determine the size of the subnet.
Excluded address	Specify a range of IP addresses to exclude. You can add up to two exclusion ranges. Based on the size of the subnet and the value configured for **Excluded address**, the IP addresses either before or after the defined range are excluded.
Default Router	If **Local, L2** is selected for type of DHCP scope, specify the IP address of the default router.
DNS Server	If required, specify the IP address of a DNS server for the **Local**; **Local, L2**; and **Local, L3** scopes.
Domain Name	If required, specify the domain name for the **Local**; **Local, L2**; and **Local, L3** scopes.
Lease Time	Specify a lease time for the client in minutes within a range of 2–1440 minutes. The default value is 720 minutes.
Option	Specify the type and a value for the DHCP option. You can configure the organization-specific DHCP options supported by the DHCP server. For example, 176, 242, and 161. Click **+** to add multiple DHCP options.

4. Click **OK**.

In the CLI

To configure a Local DHCP scope:

```
(AP)(config)# ip dhcp <profile-name>
```

```
(AP)(DHCP Profile <profile-name>)# server-type <local>
(AP)(DHCP Profile <profile-name>)# server-vlan <vlan-ID>
(AP)(DHCP Profile <profile-name>)# subnet <IP-address>
(AP)(DHCP Profile <profile-name>)# subnet-mask <subnet-mask>
(AP)(DHCP Profile <profile-name>)# dns-server <name>
(AP)(DHCP Profile <profile-name>)# domain-name <domain-name>
(AP)(DHCP Profile <profile-name>)# lease-time <seconds>
(AP)(DHCP Profile <profile-name>)# option <type> <value>
```

To configure a Local, L2 DHCP scope:

```
(AP)(config)# ip dhcp <profile-name>
(AP)(DHCP Profile <profile-name>)# server-type <local,l2>
(AP)(DHCP Profile <profile-name>)# server-vlan <vlan-ID>
(AP)(DHCP Profile <profile-name>)# subnet <IP-address>
(AP)(DHCP Profile <profile-name>)# subnet-mask <subnet-mask>
(AP)(DHCP Profile <profile-name>)# exclude-address <IP-address>
(AP)(DHCP Profile <profile-name>)# default-router
(AP)(DHCP Profile <profile-name>)# dns-server <name>
(AP)(DHCP Profile <profile-name>)# domain-name <domain-name>
(AP)(DHCP Profile <profile-name>)# lease-time <seconds>
(AP)(DHCP Profile <profile-name>)# option <type> <value>
```

To configure a Local, L3 DHCP scope:

```
(AP)(config)# ip dhcp <profile-name>
(AP)(DHCP Profile <profile-name>)# server-type <local,l3>
(AP)(DHCP Profile <profile-name>)# server-vlan <vlan-ID>
(AP)(DHCP Profile <profile-name>)# subnet <IP-address>
(AP)(DHCP Profile <profile-name>)# subnet-mask <subnet-mask>
(AP)(DHCP Profile <profile-name>)# exclude-address <IP-address>
(AP)(DHCP Profile <profile-name>)# dns-server <name>
(AP)(DHCP Profile <profile-name>)# domain-name <domain-name>
(AP)(DHCP Profile <profile-name>)# lease-time <seconds>
(AP)(DHCP Profile <profile-name>)# option <type> <value>
```

VLAN and Default Router Settings

SCALANCE W supports DHCP scopes in which both, the DHCP server and the default gateway on a virtual controller can configure a default gateway IP address. For the Centralized,L3, Local, Local,L2, and Local,L3 scopes, an option is introduced to configure a VLAN IP address to the existing service VLAN of a DHCP pool. This feature can prevent changes that may occur in DHCP range exclusions.

You can configure a local DHCP profile by using the SCALANCE W UI or CLI.

In the SCALANCE W UI

To configure a default router and VLAN parameters in a local DHCP profile:

1. Click **More > DHCP Server**. The **DHCP Server** window is displayed.
2. To configure a local DHCP scope, click **New** under **Local DHCP Scopes**. The **New DHCP Scope** window is displayed.
3. Select the **Type** and configure the parameters available in the SCALANCE W UI. The **Default router** parameter can be set on Local and Local, L3 profiles. The **VLAN IP** and **VLAN Mask** parameters can be set only on the Local, L2 profile.
4. Click **OK**.

In the CLI

To configure VLAN IP in a Local DHCP profile:

```
(AP)(config)# ip dhcp <profile-name>
```

```
(AP)(DHCP Profile <profile-name>)# vlan-ip <VLAN_IP> mask <VLAN mask>
```

To configure a default router in a Local DHCP profile:

```
(AP)(config)# ip dhcp <profile-name>
```

```
(AP)(DHCP Profile <profile-name>)# default-router <default_router>
```

Note

The value of the VLAN IP and default router for the Local or Local,l3 profile must be the same.

16.1.2 Configuring Distributed DHCP Scopes

SCALANCE W allows you to configure the DHCP address assignment for the branches connected to the corporate network through VPN. You can configure the range of DHCP IP addresses used in the branches and the number of client addresses allowed per branch. You can also specify the IP addresses that must be excluded from those assigned to clients, so that they are assigned statically.

SCALANCE W supports the following distributed DHCP scopes:

- **Distributed, L2**—In this mode, the virtual controller acts as the DHCP server, but the default gateway is in the data center. Based on the number of clients specified for each branch, the range of IP addresses is divided. Based on the IP address range and client count configuration, the DHCP server in the virtual controller controls a scope that is a subset of the complete IP address range for the subnet distributed across all the branches. This DHCP assignment mode is used with the L2 forwarding mode.

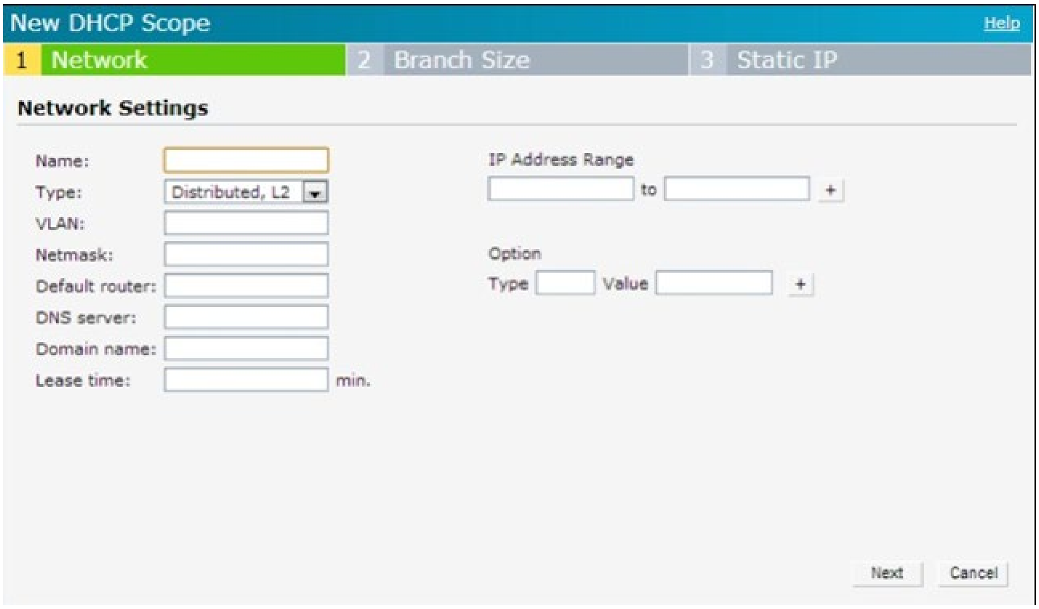
- **Distributed, L3**—In this mode, the virtual controller acts as the DHCP server and the default gateway.
- Based on the number of clients specified for each branch, the range of IP addresses is divided. Based on the IP address range and client count configuration, the DHCP server in the virtual controller is configured with a unique subnet and a corresponding scope.

You can configure distributed DHCP scopes such as Distributed, L2 or Distributed, L3 by using the SCALANCE W UI or the CLI.

In the SCALANCE W UI

To configure distributed DHCP scopes such as Distributed, L2 or Distributed, L3:

1. Click **More > DHCP Server**. The **DHCP Server** window is displayed.
2. To configure a distributed DHCP mode, click **New** under **Distributed DHCP Scopes**. The **New DHCP Scope** window is displayed. The following figure shows the contents of the **New DHCP Scope** window.



Network Settings

Name:
Type: Distributed, L2
VLAN:
Netmask:
Default router:
DNS server:
Domain name:
Lease time: min.

IP Address Range
to +

Option
Type Value +

Figure 16-1 New DHCP Scope: Distributed DHCP Mode

3. Based on the type of distributed DHCP scope, configure the following parameters:

Parameter	Description
Name	Enter a name for the DHCP scope.
Type	Select any of the following options: • **Distributed, L2**—On selecting **Distributed, L2**, the virtual controller acts as the DHCP server but the default gateway is in the data center. Traffic is bridged into VPN tunnel. • **Distributed, L3**—On selecting **Distributed, L3**, the virtual controller acts as both DHCP server and default gateway. Traffic is routed into the VPN tunnel.
VLAN	Specify a VLAN ID. To use this subnet, ensure that the VLAN ID specified here is assigned to an SSID profile. For more information on SSID profile configuration, see Configuring VLAN Settings for a WLAN SSID Profile (Page 101) and Configuring VLAN for a Wired Profile (Page 127).
Netmask	If **Distributed, L2** is selected for the type of DHCP scope, specify the subnet mask. The subnet mask and the network determine the size of subnet.
Default router	If **Distributed, L2** is selected for the type of DHCP scope, specify the IP address of the default router.
DNS server	If required, specify the IP address of a DNS server. You can configure up to two DNS servers at the same time. Use commas to separate the DNS servers.
Domain name	If required, specify the domain name.
Lease time	Specify a lease time for the client in minutes within a range of 2–1440 minutes. The default value is 720 minutes.
Dynamic DNS	Select the **Dynamic DNS** check box to enable dynamic DNS on the Distributed, L3 client. **Key**—Enter the TSIG shared secret key.
IP Address Range	Specify a range of IP addresses to use. To add another range, click the + icon. You can specify up to four different ranges of IP addresses. • For the **Distributed, L2** mode, ensure that all IP ranges are in the same subnet as the default router. On specifying the IP address ranges, a subnet validation is performed to ensure that the specified ranges of IP address are in the same subnet as the default router and subnet mask. The configured IP range is divided into blocks based on the configured client count. • For the **Distributed, L3** mode, you can configure any discontinuous IP ranges. The configured IP range is divided into multiple IP subnets that are sufficient to accommodate the configured client count. **NOTE:** You can allocate multiple branch IDs per subnet. The AP generates a subnet name from the DHCP IP configuration, which the controller can use as a subnet identifier. If static subnets are configured in each branch, all of them are assigned the with ID 0, which is mapped directly to the configured static subnet.
Option	Specify the type and a value for the DHCP option. You can configure the organization-specific DHCP options supported by the DHCP server. For example, 176, 242, 161, and so on. To add multiple DHCP options, click the + icon. You can add up to eight DHCP options.

4. Click **Next**
5. Specify the number of clients to use per branch. The client count configured for a branch determines the use of IP addresses from the IP address range defined for a DHCP scope. For example, if 20 IP addresses are available in an IP address range configured for a DHCP scope and a client count of 9 is configured, only a few IP addresses (in this example, 9) from this range will be used and allocated to a branch. The AP does not allow the administrators to assign the remaining IP addresses to another branch, although a lower value is configured for the client count.
6. Click **Next**. The **Static IP** tab is displayed.
7. Specify the number of first and last IP addresses to reserve in the subnet.
8. Click **Finish**

In the CLI

To configure a Distributed, L2 DHCP scope:

```
(AP)(config)# ip dhcp <profile-name>
(AP)(DHCP Profile <profile-name>)# ip dhcp server-type <Distributed,L2>
(AP)(DHCP Profile <profile-name>)# server-vlan <vlan-ID>
(AP)(DHCP Profile <profile-name>)# subnet-mask <subnet-mask>
(AP)(DHCP Profile <profile-name>)# default-router <IP-address>
(AP)(DHCP Profile <profile-name>)# client-count <number
(AP)(DHCP Profile <profile-name>)# dns-server <name>
(AP)(DHCP Profile <profile-name>)# domain-name <domain-name>
(AP)(DHCP Profile <profile-name>)# lease-time <seconds>
(AP)(DHCP Profile <profile-name>)# ip-range <start-IP> <end-IP>
(AP)(DHCP Profile <profile-name>)# reserve {first|last} <count>
(AP)(DHCP Profile <profile-name>)# option <type> <value>
```

To configure a Distributed, L3 DHCP scope:

```
(AP)(config)# ip dhcp <profile-name>
(AP)(DHCP Profile <profile-name>)# ip dhcp server-type <Distributed,L3>
(AP)(DHCP Profile <profile-name>)# server-vlan <vlan-ID>
(AP)(DHCP Profile <profile-name>)# client-count <number>
(AP)(DHCP Profile <profile-name>)# dns-server <name>
(AP)(DHCP Profile <profile-name>)# domain-name <domain-name>
(AP)(DHCP Profile <profile-name>)# lease-time <seconds>
(AP)(DHCP Profile <profile-name>)# dynamic-dns [key <TSIG KEY>]
(AP)(DHCP Profile <profile-name>)# ip-range <start-IP> <end-IP>
(AP)(DHCP Profile <profile-name>)# reserve {first|last} <count>
(AP)(DHCP Profile <profile-name>)# option <type> <value>
```

```
(AP)(DHCP Profile <profile-name>)# end
```

16.1.3 Configuring Centralized DHCP Scopes

When a centralized DHCP scope is configured, the following points are to be noted:

- The virtual controller does not assign an IP address to the client and the DHCP traffic is directly forwarded to the DHCP server.
- For Centralized, L2 clients, the virtual controller bridges the DHCP traffic to the controller over the VPN or GRE tunnel. The IP address is obtained from the DHCP server behind the controller serving the VLAN or GRE of the client. This DHCP assignment mode also allows you to add the DHCP option 82 to the DHCP traffic forwarded to the controller.
- For Centralized, L3 clients, the virtual controller acts as a DHCP relay agent that forwards the DHCP traffic to the DHCP server located either in the corporate or local network. The Centralized, L3 VLAN IP is used as the source IP. The IP address is obtained from the DHCP server.

You can configure a centralized DHCP scope through the SCALANCE W UI or the CLI.

In the SCALANCE W UI

To configure a centralized DHCP scope:

1. Click **More > DHCP Server**. The **DHCP Server** window is displayed.
2. To configure a centralized DHCP scope, click **New** under **Centralized DHCP Scopes**. The **New DHCP Scope** window is displayed.

3. To configure a centralized profile, select the profile type as **Centralized, L2** or **Centralized, L3** and configure the following parameters.:

Parameter	**Description**
Name	Enter a name for the DHCP scope.
Type	Set the type as follows: • **Centralized, L2** for the Centralized, L2 profile • **Centralized, L3** for the Centralized, L3 profile
VLAN	Specify a VLAN ID. To use this subnet, ensure that the VLAN ID specified here is assigned to an SSID profile. For more information on SSID profile configuration, see Configuring VLAN Settings for a WLAN SSID Profile (Page 101) and Configuring VLAN for a Wired Profile (Page 127).
Split tunnel	Set this to **Enabled** or **Disabled** for split tunnel functionality for the Centralized, L2 subnet. Enabling split tunnel allows a VPN user to access a public network and a local LAN or WAN network at the same time through the same physical network connection. For example, a user can use a remote access VPN software client connecting to a corporate network using a home wireless network. The user with split tunneling enabled is able to connect to file servers, database servers, mail servers, and other servers on the corporate network through the VPN connection. When the user connects to Internet resources (websites, FTP sites, and so on), the connection request goes directly to the gateway provided by the home network. The split-DNS functionality intercepts DNS requests from clients for non-corporate domains (as configured in Enterprise Domains list) and forwards to the AP's own DNS server. When split-tunnel is disabled, all the traffic including the corporate and Internet traffic is tunneled irrespective of the routing profile specifications. If the GRE tunnel is down and when the corporate network is not reachable, the client traffic is dropped.
DHCP relay	If you are configuring a Centralized, L2 DHCP profile, you can select **Enabled** to allow the APs to intercept the broadcast packets and relay DHCP requests to the centralized DHCP server. **NOTE:** The **DHCP relay** option is not available for Centralized, L3 profile configuration.
Helper address	Specify the IP address of the DHCP server. **NOTE:** For Centralized, L2 DHCP profiles, the **Helper address** option is displayed only when DHCP relay is enabled.
VLAN IP	Specify the Centralized, L3 DHCP subnet gateway IP.
VLAN Mask	Specify the subnet mask of the Centralized, L3 DHCP subnet gateway IP.
Option82	Select **Alcatel** to enable DHCP Option 82 and allow clients to send DHCP packets with the Option 82 string. The Option 82 string is available only in the Alcatel (ALU) format. The ALU format for the Option 82 string consists of the following: • Remote Circuit ID; X AP-MAC; SSID; SSID-Type • Remote Agent; X IDUE-MAC **NOTE:** The Option 82 string is specific to Alcatel and is not configurable.

4. Click **OK**.

The following table describes the behavior of the DHCP Relay Agent and Option 82 in the AP.

Table 16- 1 DHCP Relay and Option 82

DHCP Relay	Option 82	Result
Enabled	Enabled	DHCP packet relayed with the ALU-specific Option 82 string
Enabled	Disabled	DHCP packet relayed without the ALU-specific Option 82 string
Disabled	Enabled	DHCP packet not relayed, but broadcast with the ALU-specific Option 82 string
Disabled	Disabled	DHCP packet not relayed, but broadcast without the ALU-specific Option 82 string

In the CLI

To configure a Centralized, L2 DHCP profile:

```
(AP)(config)# ip dhcp <profile-name>

(AP)(DHCP Profile <profile-name>)# server-type <centralized>

(AP)(DHCP Profile <profile-name>)# server-vlan <vlan-ID>

(AP)(DHCP Profile <profile-name>)# option82 alu

(AP)(DHCP Profile <profile-name>)# disable-split-tunnel
```

To configure a Centralized, L3 DHCP profile:

```
(AP)(config)# ip dhcp <profile-name>

(AP)(DHCP Profile <profile-name>)# server-type <centralized>

(AP)(DHCP Profile <profile-name>)# server-vlan <vlan-ID>

(AP)(DHCP Profile <profile-name>)# dhcp-relay

(AP)(DHCP Profile <profile-name>)# dhcp-server <DHCP-relay-server>

(AP)(DHCP Profile <profile-name>)# vlan-ip <DHCP IP address> mask <VLAN mask>
```

16.2 Configuring the Default DHCP Scope for Client IP Assignment

The DHCP server is a built-in server, used for networks in which clients are assigned IP address by the virtual controller. You can customize the DHCP pool subnet and address range to provide simultaneous access to more number of clients. The largest address pool supported is 2048. The default size of the IP address pool is 512.

Note

When a DHCP server is configured and if the **Client IP assignment** parameter for an SSID profile is set to **Virtual Controller Assigned**, the virtual controller assigns the IP addresses to the WLAN or the wired clients. By default, the AP automatically determines a suitable DHCP pool for **Virtual Controller Assigned** networks.

APs typically select the 172.31.98.0/23 subnet. If the IP address of the AP is within the 172.31.98.0/23 subnet, the AP selects the 10.254.98.0/23 subnet. However, this mechanism does not guarantee that it would avoid all possible conflicts with the wired network. If your wired network uses either 172.31.98.0/23 or 10.254.98.0/23, and you experience problems with the **Virtual Controller Assigned** networks, manually configure the DHCP pool by following the steps described in this section.

You can configure a domain name, DNS server, and DHCP server for client IP assignment using the SCALANCE W UI or the CLI.

In the Web UI

To configure a DHCP pool:

1. Navigate to **More > DHCP Server**. The **DHCP Server** tab
2. Enter the domain name of the client in the **Domain name** text box.
3. Enter the IP addresses of the DNS servers separated by a comma (,) in the **DNS server(s)** text box.
4. Enter the duration of the DHCP lease in the **Lease time** text box. Select any of the following values from the drop-down list next to **Lease time**:
   - **Minutes**—For minutes, specify a value between 2 and 59.
   - **Hours**—For hours, specify a value between 1 and 23.
   - **Days** —For days, specify a value between 1 and 30.

   The default lease time is 0.
5. Enter the network range for the client IP addresses in the **Network** text box. The system generates a network range automatically that is sufficient for 254 addresses. If you want to provide simultaneous access to more number of clients, specify a larger range.
6. Specify the subnet mask details for the network range in the **Mask** text box.
7. Click **OK** to apply the changes.

In the CLI

To configure a DHCP pool:

```
(AP)(config)# ip dhcp pool
```

```
(AP)(DHCP)# domain-name <domain>
```

```
(AP)(DHCP)# dns-server <DNS-IP-address>

(AP)(DHCP)# lease-time <minutes>

(AP)(DHCP)# subnet <IP-address>

(AP)(DHCP)# subnet-mask <subnet-mask>
```

To view the DHCP database:

```
(AP)# show ip dhcp database
```

Configuring Time-Based Services 17

17.1 Time Range Profiles

APs allow you to enable or disable an SSID for users at a particular time of the day. You can now create a time range profile and assign it to a WLAN SSID, so that user access to the Internet or network is restricted during a specific time period.

APs support the configuration of both absolute and periodic time range profiles. You can configure an absolute time range profile to execute during a specific timeframe or create a periodic profile to execute at regular intervals based on the periodicity specified in the configuration.

The following configuration conditions apply to the time-based services:

- Time-based services require an active NTP server connection. APs use the default NTP server for time synchronization. However, the administrators can also configure an NTP server on the AP. To verify the time synchronization between the NTP server and the AP, execute the **show time-range** command and check if the time on the NTP server is in synchronization with the local time. For more information on NTP server configuration, see NTP Server.
- For a time range profile configured to **enable** the SSID on the AP:
  - l When the timer starts, if the current time is greater than the start time and lesser than the end time, the SSID will be brought UP. If the SSID is already UP, then there is no effect on the SSID.
  - l When the timer ends, if the current time is greater than the end time, the SSID is brought DOWN. If the SSID is already DOWN, then there is no effect on the SSID.
- For a time range profile configured to **disable** the SSID on the AP:
  - When the timer starts, if the current time is greater than the start time and lesser than the end time, the SSID will be brought DOWN. If the SSID is already DOWN, then there is no effect on the SSID.
  - When the timer ends, if the current time is greater than the end time, the SSID is brought UP. If the SSID is already UP, then there is no effect on the SSID.

17.2 Configuring a Time Range Profile

You can create time range profiles using the SCALANCE W UI or the CLI.

In the SCALANCE W UI

To create a time range profile:

1. Navigate to **System > Show advanced options > Time Based Services**.
2. Click **New** under **Time Range Profiles**. The **New Profile** window for creating time range profiles is displayed.

3. Configure the parameters listed in the following table:

Parameter	Description
Name	Specify a name for the time range profile.
Type	Select the type of time range profile. **Periodic**—When configured, the state of the AP changes based on the time range configured in the profile. **Absolute**—When configured, the state of the AP changes during a specific date, day, and time.
Period Type	For periodic time range profiles, specify a periodic interval (day/weekday/weekend/daily) at which the time range profile must be applied.
Start Day and End Day	For absolute time range profiles, specify the start day and the end day to configure a specific time period during which the time range profile is applied. **NOTE:** The year selected for Start Day and End Day cannot exceed the year 2037.
Start Time	Select the start time for the time range profile in the hh:mm format.
End Time	Select the end time for the time range profile in hh:mm format.

4. Click **OK**

In the CLI

To create an absolute time range profile:

```
(AP)(config)# time-range <name> absolute start <startday> <starttime> end
<endday><endtime>
```

To configure a periodic time range profile:

```
(AP)(config)# time-range <name> periodic
{<startday>|daily|weekday|weekend}<starttime> to <endtime>
```

17.3 Applying a Time Range Profile to a WLAN SSID

To apply a time range profile to a WLAN SSID using the SCALANCE W UI:

1. Navigate to the WLAN SSID profile configuration wizard
   – Click **Network > New** or
   – Select an existing WLAN SSID and click **edit.**
2. Click **Show advanced options**.

3. Click **Edit**, select a time range profile from the list, then select a value from the **Status** drop-down list, and then click **OK**.
   – When a time range profile is enabled on an SSID, the SSID is made available to the users for the configured time range. For example, if the specified time range is 12:00–13:00, the SSID becomes available only between 12 PM and 1 PM on a given day.
   – If a time range is disabled, the SSID becomes unavailable for the configured time range. For example, if the configured time range is 14:00–17:00, the SSID is made unavailable from 2 PM to 5 PM on a given day.
4. Click **Next** and then click **Finish**.

Note

If the SSID has two time range profiles enabled with an overlapping duration, the time range profile will be executed as per the configuration conditions described earlier in this chapter. For example, if profile1 has 9AM-12PM as the duration and profile2 has 10AM-11AM as the duration and both are enabled on the SSID, the SSID becomes available only in the time range 9AM-11AM.

In the CLI

To enable a time range profile on an SSID:

```
(AP)(config)# wlan ssid-profile <name>

(AP)(SSID Profile "<name>")# time-range <name> enable
```

To disable a time range profile on an SSID:

```
(AP)(config)# wlan ssid-profile <name>

(AP)(SSID Profile "<name>")# time-range <name> disable
```

17.4 Verifying the Configuration

To view the time range profiles created on an AP:

```
(AP) # show time-range Time Range Summary
```

To verify if the time range profile is enabled on an SSID:

```
(AP)# show time-profile Time Range SSID Profile
```

Dynamic DNS Registration 18

18.1 Enabling Dynamic DNS

APs support the dynamic DNS feature which enables updating the host name of the AP and the DL3 clients connected to it. In a scenario where the public IP address is dynamically handed to the AP by the ISP, the connectivity to the AP is lost when there is a change in the public IP address. Similarly, in case of DL3 clients, where the AP acts as a DHCP server, the host becomes unreachable when the dynamically assigned IP address is changed. The dynamic DNS feature eliminates these issues by configuring a host name, thus providing a uniform approach to access the AP and the DL3 clients. The IP address of the AP and the DL3 client is mapped to the host name and this gets automatically updated to the DNS server each time the IP address is changed.

You can enable Dynamic DNS using the SCALANCE W UI or the CLI.

In the SCALANCE W UI

To enable dynamic DNS:

1. Navigate to **Services > Dynamic DNS**.

Parameter	Description	Example
Key	Configures a Transaction Signature shared secret key to secure the dynamic updates. The following algorithm names are supported: • hmac-md5 (used by default if algo-name is not specified) • hmac-sha1 • hmac-sha256 • **NOTE:** When a **key** is configured, the update is successful only if AP and DNS server clocks are in sync.	`hmac-sha1:siemensddns:16YuLPdH21rQ6PuK9udsVLtJw3Y=`
Server IP	Enter the server IP address of the DNS server to which the client updates are sent. **NOTE**: If the DNS server IP address is not specified in the Dynamic DNS configuration window, the AP updates will be sent to the APs DNS server instead.	`10.17.132.85`
Interval	Specify the time interval (in secs) at which the DNS updates are to be synced to the server. The default time interval is 12 hours, minimum time interval is 15 minutes, and maximum time interval is 100 days.	`900`

2. Click **OK.**

In the CLI

To enable dynamic DNS on an AP

```
(AP)(config)# dynamic-dns-ap
```

To configure a TSIG key and server IP address:

```
(AP)(config)# dynamic-dns-ap key <algo-name:keyname:keystring>
```

```
(AP)(config)# dynamic-dns-ap server <ddns_server>
```

To configure a time interval:

```
(AP)(config)# dynamic-dns-interval <ddns_interval>
```

18.2 Configuring Dynamic DNS Updates for Clients

You can enable DDNS updates when creating or editing a DHCP scope for **Distributed, L3** clients. When enabled, the DDNS updates of the clients are periodically sent during the specified time to the DNS server that is configured in the DHCP profile. For the DL3 clients, if the DNS server IP is not configured in the DHCP profile, the client updates will be dropped. The DDNS updates are secured by using TSIG shared secret keys, when communicating between the client and the server. For more information, refer to Enabling Dynamic DNS (Page 269) and Configuring Distributed DHCP Scopes (Page 256).

In the SCALANCE W UI

To enable DDNS for clients:

1. Navigate to **More > DHCP Servers**, select the **Distributed, L3** DHCP Scope under **Distributed DHCP Scopes** and click **Edit**.
2. Select the **Dynamic DNS** check box.
3. Enter the TSIG shared secret **key**.
4. Click **Next** and then click **Finish**.

In the CLI

To enable DDNS for AP clients:

```
(AP)(config)# ip dhcp <profile name>
```

```
(AP)(DHCP profile "<name>")# dynamic-dns
```

```
(AP)(DHCP profile "<name>")# dynamic-dns key <algo-name:keyname:keystring>
```

18.3 Verifying the Configuration

To view the DDNS status on an AP:

```
(AP)# show ddns
```

To view the list of DDNS clients:

```
(AP)# show ddns clients
```

Note

DHCP profile name is None for the Master AP update sent.

Note

The command displays the **Key** in the encrypted format.

Note

You can also configure dynamic DNS on an AP or clients using the privileged execution mode in the CLI. For more information, refer to the **show ddns clients** command in the latest *SCALANCE W CLI Function Manual*.

VPN Configuration 19

19.1 Understanding VPN Features

As APs use a virtual controller architecture, the AP network does not require a physical controller to provide the configured WLAN services. However, a physical controller is required for terminating VPN tunnels from the AP networks at branch locations to data centers, where the controller acts as a VPN concentrator.

When a VPN is configured, the AP acting as the virtual controller creates a VPN tunnel to an Aruba Mobility Controller in your corporate office. The controller acts as a VPN endpoint and does not supply the AP with any configuration.

The VPN features are recommended for the following setups:

Enterprises with many branches that do not have a dedicated VPN connection to the corporate office.

- Branch offices that require multiple APs.
- Individuals working from home and, connecting to the VPN.
- The survivability feature of APs with the VPN connectivity of Remote APs allows you to provide corporate connectivity on non-corporate networks.

Supported VPN Protocols

SCALANCE W supports the following VPN protocols for remote access:

Table 19- 1 VPN Protocols

VPN Protocol	Description
Aruba IPsec	IPsec is a protocol suite that secures IP communications by authenticating and encrypting each IP packet of a communication session. You can configure an IPsec tunnel to ensure that the data flow between the networks is encrypted. However, you can configure a split-tunnel to encrypt only the corporate traffic. When IPsec is configured, ensure that you add the AP MAC addresses to the whitelist database stored on the controller or an external server. IPsec supports Local, L2, and L3 modes of AP-VPN operations. **NOTE:** The APs support IPsec only with Aruba Controllers.
Layer-2 GRE	GRE is a tunnel protocol for encapsulating multicast, broadcast, and L2 packets between a GRE- capable device and an endpoint. APs support the configuration of L2 GRE tunnel with an Aruba controller to encapsulate the packets sent and received by the AP. You can use the GRE configuration for L2 deployments when there is no encryption requirement between the AP and controller for client traffic. APs support two types of GRE configuration: • **Manual GRE**—The manual GRE configuration sends unencrypted client traffic with an additional GRE header and does not support failover. When manual GRE is configured on the AP, ensure that the GRE tunnel settings are enabled on the controller. • **Aruba GRE**—With Aruba GRE, no configuration on the controller is required except for adding the AP MAC addresses to the whitelist database stored on the controller or an external server. Aruba GRE reduces manual configuration when **Per-AP tunnel** configuration is required and supports failover between two GRE endpoints. **NOTE:** APs support manual and Aruba GRE configuration only for L2 mode of operations. Aruba GRE configuration is supported only on Aruba Controllers.

Diffie-Hellman Algorithm

Diffie-Hellman is a key agreement algorithm that allows two parties to agree upon a shared secret, and is used within IKE to securely establish session keys.

SCALANCE W supports the following Diffie-Hellman groups:

- Group 2: 1024-bit Diffie–Hellman prime modulus group
- Group 14: 2048-bit Diffie–Hellman prime modulus group

By default, APs attempt to use Diffie–Hellman Group 2 to set up an AP VPN connection. If the controller rejects Diffie–Hellman Group 2, the APs can use Diffie–Hellman Group 14.

Note

Diffie–Hellman Group 2 is not permitted if FIPS mode is enabled on an AP.

19.2 Configuring a Tunnel from an AP to a Mobility Controller

AP supports the configuration of tunneling protocols such as GRE and IPsec. This section describes the procedure for configuring VPN host settings on an AP to enable communication with a controller in a remote location:

- Configuring an IPsec Tunnel (Page 275)
- Configuring an L2-GRE Tunnel (Page 277)

19.2.1 Configuring an IPsec Tunnel

An IPsec tunnel is configured to ensure that the data flow between the networks is encrypted. When configured, the IPsec tunnel to the controller secures corporate data.

You can configure an IPsec tunnel from the virtual controller using the SCALANCE W UI or the CLI.

In the Web UI

To configure a tunnel for IPsec protocol:

1. Click the **More > VPN** link in the SCALANCE W UI. The **Tunneling** window is displayed.
2. Select **Aruba IPSec** from the **Protocol** drop-down list.
3. Enter the IP address or fully qualified domain name (FQDN) for the primary VPN/IPsec endpoint in the **Primary host** text box.
4. Enter the IP address or FQDN for the backup VPN/IPsec endpoint in the **Backup host** text box. This entry is optional. When you specify the primary and backup host details, the other details are displayed.
5. Specify the following parameters. A sample configuration is shown in Figure *IPsec Configuration*.
   - To allow the VPN tunnel to switch back to the primary host when it becomes available again, select
   - **Enabled** from the **Preemption** drop-down list. This step is optional.
   - If **Preemption** is enabled, specify a value in seconds for **Hold time**. When preemption is enabled and the primary host comes up, the VPN tunnel switches back to the primary host after the specified hold- time. The default value for **Hold time** is 600 seconds.
   - To allow the AP to create a backup VPN tunnel to the controller along with the primary tunnel, and maintain both the primary and backup tunnels separately, select **Enabled** from the **Fast failover** drop-down list. When fast failover is enabled and if the primary tunnel fails, the AP can switch the data stream to the backup tunnel. This reduces the total failover time to less than one minute.
   - To disconnect all wired and wireless users when the system switches during VPN tunnel transition from primary to backup and backup to primary, set **Reconnect User On Failover** to **Enabled**.
   - To configure an interval during which the wired and wireless users are disconnected during a VPN tunnel switch, specify a value in seconds for **Reconnect Time On**

Failover within a range of 30–900 seconds. By default, the reconnection duration is set to 60 seconds.

– Specify a value in seconds for **Secs between test packets**. Based on the configured frequency, the AP can verify if an active VPN connection is available. The default value is 5 seconds, which means that the AP sends one packet to the controller every 5 seconds.

– Enter a value for **Max allowed test packet loss** to define a number for lost packets, exceeding which the AP can determine that the VPN connection is unavailable. The default value is 2.

6. Click **Next** to create routing profiles. When the IPsec tunnel configuration is completed, the packets that are sent from and received by an AP are encrypted.

In the CLI

To configure an IPsec VPN tunnel:

```
(AP)(config)# vpn primary <name>

(AP)(config)# vpn backup <name>

(AP)(config)# vpn fast-failover

(AP)(config)# vpn hold-time <seconds>

(AP)(config)# vpn preemption

(AP)(config)# vpn monitor-pkt-send-freq <frequency>

(AP)(config)# vpn monitor-pkt-lost-cnt <count>

(AP)(config)# vpn reconnect-user-on-failover

(AP)(config)# vpn reconnect-time-on-failover <down_time>
```

Example

```
(AP)(config)# vpn primary 192.0.2.18

(AP)(config)# vpn backup 192.0.2.20

(AP)(config)# vpn fast-failover

(AP)(config)# vpn preemption


(AP)(config)# ip dhcp distl2

(AP)(DHCP Profile "distL2")# server-type Distributed,L2

(AP)(DHCP Profile "distL2")# server-vlan 2

(AP)(DHCP Profile "distL2")# ip-range 10.15.205.0 10.15.205.255

(AP)(DHCP Profile "distL2")# subnet-mask 255.255.255.0

(AP)(DHCP Profile "distL2")# lease-time 86400

(AP)(DHCP Profile "distL2")# default-router 10.15.205.254

(AP)(DHCP Profile "distL2")# dns-server 10.13.6.110,10.1.1.50

(AP)(DHCP Profile "distL2")# domain-name siemens.com
```

```
(AP)(DHCP Profile "distL2")# client-count 5


(AP)(config)# ip dhcp local

(AP)(DHCP Profile "local")# server-type Local

(AP)(DHCP Profile "local")# server-vlan 200

(AP)(DHCP Profile "local")# subnet 172.16.200.1

(AP)(DHCP Profile "local")# subnet-mask 255.255.255.0

(AP)(DHCP Profile "local")# lease-time 86400

(AP)(DHCP Profile "local")# dns-server 10.13.6.110,10.1.1.50 (AP)(DHCP Profile
"local")# domain-name siemens.com
```

To view the VPN configuration:

```
(AP)# show vpn config
```

19.2.2 Configuring an L2-GRE Tunnel

Configuring Manual GRE Parameters

You can configure a GRE tunnel between the AP and the controller using either the virtual controller IP or the AP IP, based on the following AP settings:

- If a virtual controller IP is configured and if **Per-AP tunnel** is disabled, use virtual controller IP.
- If a virtual controller IP is not configured or if **Per-AP tunnel** is enabled, use the AP IP.

In the SCALANCE W UI

To configure a GRE tunnel:

1. Click the **More > VPN** link located directly above the Search bar in the SCALANCE W UI. The **Tunneling** window is displayed.
2. Select **Manual GRE** from the **Protocol** drop-down list.

3. Specify the following parameters.
   - Enter an IP address or an FQDN for the main VPN or GRE endpoint in the **Host** text box.
   - Enter a value in the **GRE type** text box.
   - Select **Enabled** or **Disabled** from the **Per-AP tunnel** drop-down list. Enable this option to create a GRE tunnel from each AP to the VPN or GRE endpoint rather than the tunnels created just from the master AP. When enabled, the traffic to the corporate network is sent through a Layer-2 GRE tunnel from the AP itself and need not be forwarded through the master AP.

Note

By default, the **Per-AP tunnel** option is disabled.

4. Click **Next** to continue. When the GRE tunnel configuration is completed on both the AP and the controller, the packets sent from and received by an AP are encapsulated, but not encrypted.

In the CLI

To configure a manual GRE VPN tunnel:

```
(AP)(config)# gre primary <name>

(AP)(config)# gre type <type>

(AP)(config)# gre per-ap-tunnel
```

To view VPN configuration details:

```
(AP)# show vpn config
```

To configure GRE tunnel on the controller:

```
(AP)(config)# interface tunnel <Number>

(AP)(config-tunnel)# description <Description>

(AP)(config-tunnel)# tunnel mode gre <ID>

(AP)(config-tunnel)# tunnel source <controller-IP>

(AP)(config-tunnel)# tunnel destination <AP-IP>

(AP)(config-tunnel)# trusted

(AP)(config-tunnel)# tunnel vlan <allowed-VLAN>
```

Configuring Aruba GRE Parameters

The Aruba GRE feature uses the IPsec connection between the AP and the controller to send the control information for setting up a GRE tunnel. When Aruba GRE configuration is enabled, a single IPsec tunnel between the AP cluster and the controller, and one or several GRE tunnels are created based on the Per-AP tunnel configuration on the AP. For Aruba GRE, no manual configuration is required on the controller to create the GRE tunnel.

Note

Aruba GRE is supported only on Aruba Controllers running ArubaOS 6.4.x.x or later versions.

Note

APs can send IPsec and GRE heartbeat packets to Aruba Controllers. By default, APs verify the status of heartbeat messages every 5 seconds, and look for lost packets 6 times before marking down the IPsec tunnel.

However, these time intervals can be modified.

In the SCALANCE W UI

To configure Aruba GRE:

1. Click the **More > VPN** link located directly above the Search bar in the SCALANCE W UI. The **Tunneling** window is displayed.
2. Select **Aruba GRE** from the **Protocol** drop-down list.
3. Enter the IP address or the FQDN for the main VPN or IPsec endpoint in the **Primary host** text box.
4. Enter the IP address or the FQDN for the backup VPN or IPsec endpoint in the **Backup host** text box. This entry is optional. When you enter the primary host IP address and backup host IP address, other details are displayed.
5. Specify the following parameters.
   - To allow the VPN tunnel to switch back to the primary host when it becomes available again, select **Enabled** from the **Preemption** drop-down list. This step is optional
   - If **Preemption** is enabled, specify a value in seconds for **Hold time**. When preemption is enabled and the primary host comes up, the VPN tunnel switches to the primary host after the specified hold time. The default value for **Hold time** is 600 seconds.
   - To allow the AP to create a backup VPN tunnel to the controller along with the primary tunnel, and maintain both the primary and backup tunnels separately, select **Enabled** from the **Fast failover** drop-down list. If this option is enabled, when the primary tunnel fails, the AP can switch the data stream to the backup tunnel. This reduces the total failover time to less than one minute.
   - To disconnect all wired and wireless users when the system switches during VPN tunnel transition from primary to backup and backup to primary, set **Reconnect user on failover** to **Enabled**.
   - To configure an interval for which wired and wireless users are disconnected during a VPN tunnel switch, specify a value in seconds for **Reconnect time on failover** within

the range of 30–900 seconds. By default, the reconnection duration is set to 60 seconds.

– Specify a value in seconds for **Secs between test packets**. Based on the configured frequency, the AP can verify if an active VPN connection is available. The default value is 5 seconds, which means that the AP sends one packet to the controller every 5 seconds.

– Enter a value for **Max allowed test packet loss** to define a number for lost packets, exceeding which the AP can determine that the VPN connection is unavailable. The default value is 2.

6. Click **Next** to continue.

In the CLI

To enable Aruba GRE tunnel:

```
(AP)(config)# vpn gre-outside

(AP)(config)# vpn primary <name/IP-address>

(AP)(config)# vpn backup <<name/IP-address>>

(AP)(config)# vpn fast-failover

(AP)(config)# vpn hold-time <seconds>

(AP)(config)# vpn preemption

(AP)(config)# vpn monitor-pkt-send-freq <frequency>

(AP)(config)# vpn monitor-pkt-lost-cnt <count>

(AP)(config)# vpn reconnect-user-on-failover

(AP)(config)# vpn reconnect-time-on-failover <down_time>
```

To view VPN configuration details:

```
(AP)# show vpn config
```

19.2.3 Support for AP-VPN Termination on Mobility Controller Virtual Appliance

AP-VPN is supported on Mobility Controller Virtual Appliance by using default self-signed certificate. For AP to establish IPsec connection with Mobility Controller Virtual Appliance, the controller presents a default self-signed certificate which is uploaded on the AP using Activate.

Note

Mobility Masters (Mobility Master Hardware Appliance, Mobility Master Virtual Appliance, and Master Controller Mode) do not support any AP termination including Campus APs, Remote APs and AP-VPN tunnels.

VPN features are ideal for:

- enterprises with many branches that do not have a dedicated VPN connection to the Head Quarter.
- branch offices that require multiple APs.
- individuals working from home, connecting to the VPN.

This new architecture and form factor seamlessly adds the survivability feature of APs with the VPN connectivity of RAPs — providing corporate connectivity to branches.

19.3 Configuring Routing Profiles

APs can terminate a single VPN connection on an Aruba Mobility Controller. The routing profile defines the corporate subnets which need to be tunneled through IPsec. You can configure routing profiles for policy based routing into the VPN tunnel using the SCALANCE W UI or the CLI.

In the SCALANCE W UI

To configure a routing profile:

1. Click **Routing** in the **Tunneling** window.
2. Click **New**.
3. Update the following parameters:
   - **Destination**— Specify the destination network that is reachable through the VPN tunnel. This defines the IP or subnet that must reach through the IPsec tunnel. Traffic to the IP or subnet defined here will be forwarded through the IPsec tunnel.
   - **Netmask**—Specify the subnet mask to the destination.
   - **Gateway**—Specify the gateway to which the traffic must be routed. This IP address must be the controller IP address on which the VPN connection is terminated. If you have a primary and backup host, configure two routes with the same destination and netmask, but ensure that the gateway is the primary controller IP for one route and the backup controller IP for the second route.
   - **Metric**—The default metric value is 15. Specify a metric value for the datapath route. When two routes or more routes with the same network destination are available for data forwarding, the route with the least metric value takes preference.
4. Repeat step 3 to create the required number of routing profiles.
5. Click **OK**.
6. Click **Finish**.

In the CLI

```
(AP)(config)# routing-profile
```

```
(AP)(Routing-profile)# route <destination> <mask> <gateway> {<metric>}
```

Note

Routing profile is primarily used for AP-VPN scenarios, to control which traffic should flow between the master AP and the VPN tunnel, and which traffic should flow outside of the tunnel.

AP-VPN Deployment 20

20.1 Understanding AP-VPN Architecture

The AP-VPN architecture includes the following two components:

- APs at branch sites
- Controller at the datacenter

The master AP at the branch site acts as the VPN endpoint and the controller at the datacenter acts as the VPN concentrator. When an AP is set up for VPN, it forms an IPsec tunnel to the controller to secure sensitive corporate data. IPsec authentication and authorization between the controller and the APs are based on the RAP whitelist configured on the controller.

Note

Only the master AP in an AP cluster forms the VPN tunnel.

From the controller perspective, the master APs that form the VPN tunnel are considered as VPN clients. The controller terminates VPN tunnels and routes or switches the VPN traffic. The AP cluster creates an IPsec or GRE VPN tunnel from the virtual controller to a Mobility Controller in a branch office. The controller only acts as an IPsec or GRE VPN endpoint and it does not configure the AP.

AP-VPN Scalability Limits

The controller scalability in AP-VPN architecture depends on factors such as AP-VPN branches, route limit, and VLAN limit.

The following table provides the AP-VPN scalability information for various controller platforms

Table 20- 1 AP-VPN Scalability

Platforms	**AP VPN Branches** **(Preferred)**	**Route Limit**	**VLAN Limit**
7240	8192	32769	4094
7220	4096	32769	4094
7210	2048	32765	4094
7205	1024	16381	2048
7030	256	8189	256
7024	128	4093	128
7240	32,000	32,000	128,000
7010	128	4093	128

Platforms	AP VPN Branches (Preferred)	Route Limit	VLAN Limit
7008	64	4093	128
7005	64	4093	128

- **AP-VPN Branches**—The number of AP-VPN branches that can be terminated on a given controller platform.
- **Route Limit**—The number of L3 routes supported on the controller
- **VLAN Limit**—The number of VLANs supported on the controller.

AP-VPN Forwarding Modes

The forwarding modes determine whether the DHCP server and default gateway for clients reside in the branch or at the datacenter. These modes do not determine the firewall processing or traffic forwarding functionality. The Virtual controller enables different DHCP pools (various assignment modes) in addition to allocating IP subnets for each branch.

The Virtual controller allows different modes of forwarding traffic from the clients on a VLAN based on the DHCP scope configured on the AP.

For the AP-VPN deployments, the following forwarding modes are supported:

- Local mode
- L2 Switching mode
- L3 routing mode

The DHCP scopes associated with these forwarding modes are described in the following sections.

Note

Ensure that VLAN 1 is not configured for any of the DHCP scopes as it is reserved for a different purpose.

Local Mode

In this mode, the AP cluster at that branch has a local subnet and the master AP of the cluster acts as the DHCP server and gateway for clients. The local mode provides access to the corporate network using the inner IP of the IPsec tunnel. The network address for traffic destined to the corporate network is translated at the source with the inner IP of the IPsec tunnel and is forwarded through the IPsec tunnel. The traffic destined to the non-corporate network is translated using the IP address of the AP and is forwarded through the uplink

Note

When the local mode is used for forwarding client traffic, hosts on the corporate network cannot establish connections to the clients on the AP, because the source addresses of the clients are translated.

Local, L2 Mode

In this mode, the AP cluster at that branch has a local subnet and the master AP of the cluster acts as the DHCP server. The default gateway is located outside the AP and the network address for the client traffic is not translated at source. In the Local, L2 mode, access to the corporate network is supported only in a single AP cluster. The traffic to the non-corporate network is locally bridged.

Local, L3 Mode

In this mode, the network address for traffic destined to the corporate network is translated at the source with the inner IP of the IPsec tunnel and is forwarded through the IPsec tunnel. The traffic destined to the non- corporate network is routed.

Distributed, L2 Mode

In this mode, the AP assigns an IP address from the configured subnet and forwards traffic to both corporate and non-corporate destinations. Clients receive the corporate IP with virtual controller as the DHCP server. The default gateway for the client still resides in the datacenter and hence this mode is an L2 extension of corporate VLAN to remote site. Either the controller or an upstream router can be the gateway for the clients. Client traffic destined to datacenter resources is forwarded by the master AP (through the IPsec tunnel) to the client's default gateway in the datacenter.

When an AP registers with the controller, the controller automatically adds the VPN tunnel associated to this AP into the VLAN multicast table. This allows the clients connecting to the L2 mode VLAN to be part of the same L2 broadcast domain on the controller.

Distributed, L3 Mode

The Distributed, L3 mode contains all broadcast and multicast traffic to a branch. The Distributed, L3 mode reduces the cost and eliminates the complexity associated with the classic site-to-site VPN. However, this mode is very similar to a classic site-to-site IPsec VPN where two VPN endpoints connect individual networks together over a public network.

In Distributed, L3 mode, each branch location is assigned a dedicated subnet. The master AP in the branch manages the dedicated subnet and acts as the DHCP server and gateway for clients. Client traffic destined to datacenter resources is routed to the controller through the IPsec tunnel, which then routes the traffic to the appropriate corporate destinations.

When an AP registers with the controller, the controller adds a route to enable the routing of traffic from the corporate network to clients on this subnet in the branch.

Centralized, L2 Mode

The Centralized, L2 mode extends the corporate VLAN or broadcast domain to remote branches. The DHCP server and the gateway for the clients reside in the datacenter. Either the controller or an upstream router can be the gateway for the clients. For DHCP services in Centralized, L2 mode, Siemens recommends using an external DHCP server and not the DHCP server on the controller. Client traffic destined to datacenter resources is forwarded by the master AP (through the IPsec tunnel) to the client's default gateway in the datacenter.

Centralized, L3 Mode

For Centralized, L3 clients, the virtual controller acts as a DHCP relay agent that forwards the DHCP traffic to the DHCP server located behind the controller in the corporate network and reachable through the IPsec tunnel. The Centralized, L3 VLAN IP is used as the source IP. The IP address is obtained from the DHCP server.

DHCP Scope and VPN Forwarding Modes Mapping

The following table provides a summary of the DHCP scope and VPN forwarding modes mapping:

Table 20- 2 DHCP Scope and VPN Forwarding Modes Matrix

Options	Local	Local, L2	Local, L3	Centralize d, L2	Centralize d, L3	Distribute d, L2	Distribute d, L3
DHCP server	Virtual controller	Virtual controller	Virtual controller	DHCP Server in the Datacenter	DHCP Server in the Datacenter and Virtual controller acts as a relay agent	Virtual controller	Virtual controller
Default Gateway for clients	Virtual controller	Default Gateway in the local network	Virtual controller	Controller or a router in the Datacenter	Virtual controller	Controller or a router in the Datacenter	Virtual controller
Corporate Traffic	Source- NAT is performed with inner IP of the IPsec tunnel	Not applicable	Source- NAT is performed with inner IP of the IPsec tunnel	L2 reachable	Routed	L2 reachable	Routed
Internet Traffic	Source- NAT is performed with local IP of the Virtual controller	Locally bridged	Routed	Source-NAT is performed with local IP of the Virtual controller	Source-NAT is performed with local IP of the Virtual controller	Source-NAT is performed with local IP of the Virtual controller	Source-NAT is performed with local IP of the Virtual controller
Branch access from datacenter	No	No	No	Yes	Yes	Yes	Yes

20.2 Configuring AP and Controller for AP-VPN Operations

This section describes the configuration procedures for the AP and the controller to realize generic use cases. For information on specific deployment scenarios, see AP-VPN Deployment Scenarios (Page 297).

Note

This section describes the configuration procedures to perform on the AP for generic use cases. For information on specific deployment scenarios, see AP-VPN Deployment Scenarios (Page 297).

20.2.1 Configuring an AP Network for AP-VPN Operations

An AP network requires the following configurations for AP-VPN operations.

1. Defining the VPN Host Settings
2. Configuring Routing Profiles
3. Configuring DHCP Profiles
4. Configuring an SSID or Wired Port
5. Enabling Dynamic RADIUS Proxy
6. Configuring Enterprise Domains

Defining the VPN Host Settings

The VPN endpoint on which a master AP terminates its VPN tunnel is considered as the host. A master AP in an AP network can be configured with a primary and backup host to provide VPN redundancy. You can define VPN host settings through **More > VPN > Controller** in the UI.

You can configure the following VPN profiles for the AP-VPN operations. For more information, see Configuring a Tunnel from an AP to a Mobility Controller (Page 275).

- IPsec
- Manual GRE
- Aruba GRE

Configuring Routing Profiles

The routing profile on the AP determines whether the traffic destined to a subnet must be tunneled through IPsec or bridged locally. If the routing profile is empty, the client traffic will always be bridged locally. For example, if the routing profile is configured to tunnel 10.0.0.0 /8, the traffic destined to 10.0.0.0 /8 will be forwarded through the IPsec tunnel and the traffic to all other destinations is bridged locally.

You can also configure a routing profile with 0.0.0.0 as gateway to allow both the client and AP traffic to be routed through a non-tunnel route. If the gateway is in the same subnet as uplink IP address, it is used as a static gateway entry. A static route can be added to all master and slave APs for these destinations.

The VPN traffic from the local subnet of AP or the Virtual controller IP address in the local subnet is not routed to tunnel, but will be switched to the relevant VLAN. For example, when a 0.0.0.0/0.0.0.0 routing profile is defined, to bypass certain IPs, you can add a route to the IP by defining 0.0.0.0 as the destination, thereby forcing the traffic to be routed through the default gateway of the AP.

You can configure routing profiles through **More > VPN > Controller** UI. For step-by-step procedural information on configuring routing profile, see Configuring Routing Profiles (Page 281).

Note

The AP network has only one active tunnel even when fast failover is enabled. At any given time, traffic can be tunneled only to one VPN host.

Configuring DHCP Profiles

You can create DHCP profiles to determine the AP-VPN mode of operation. An AP network can have multiple DHCP profiles configured for different modes of AP-VPN. You can configure up to eight DHCP profiles. For more information on the AP-VPN modes of operation, see AP-VPN Forwarding Modes (Page 283).

You can create any of the following types of DHCP profiles for the AP-VPN operations:

- Local
- Local, L2
- Local, L3
- Distributed, L2 n Distributed, L3 n Centralized, L2 n Centralized, L3

For more information on configuring DHCP profiles, see Configuring DHCP Scopes (Page 253).

Note

A Centralized, L2 or Distributed, L2 VLAN or subnet cannot be used to serve APs in a hierarchical mode of deployment. Ensure that the physical IP of the APs connecting to the master AP in hierarchical mode of deployment is not on a VLAN or subnet that is in Centralized, L2 or Distributed, L2 mode of operation. For information on hierarchical mode of deployment, see Understanding Hierarchical Deployment (Page 137).

Configuring an SSID or Wired Port Profile

For a client to connect to the AP-VPN network, an SSID or wired port profile on an AP must be configured with appropriate AP-VPN mode of operation. The VLAN configuration in an SSID or wired port profile determines whether an SSID or wired port is configured for the AP-VPN operations.

To configure an SSID or wired port for a specific AP-VPN mode, the VLAN ID defined in the SSID or wired port profile must match the VLAN ID defined in the DHCP profile configuration. If the VLAN assignment for an SSID or wired port profile is set to Virtual controller assigned, custom, or a static VLAN ID that does not match the VLAN ID configured in the DHCP profiles, the AP-VPN operations are affected. For example, if a local DHCP profile is configured with a VLAN ID of 200, the VLAN configuration on the SSID must be set to a static VLAN ID 200.

Note

Ensure that the VLAN assignment for an SSID or wired port profile is not set to default as the VPN tunnel is not supported on the default VLAN.

Note

An AP will not send a registration request to the controller if **SetMeUp** is configured on the AP.

For information on enabling dynamic RADIUS proxy, see Configuring Dynamic RADIUS Proxy Parameters (Page 196)and Configuring a Wired Profile (Page 125).

Enabling Dynamic RADIUS Proxy

The RADIUS server can be deployed at different locations and VLANs. In most cases, a centralized RADIUS or local server is used to authenticate users. However, some user networks can use a local RADIUS server for employee authentication and a centralized RADIUS-based captive portal server for guest authentication. To ensure that the RADIUS traffic is routed to the required RADIUS server, the dynamic RADIUS proxy feature must be enabled. When enabled, dynamic RADIUS proxy ensures that all the RADIUS traffic is sourced from the Virtual controller IP or inner IP of the AP IPsec tunnel depending on the RADIUS server IP and routing profile.

Note

Ensure that a static Virtual controller IP is configured before enabling dynamic RADIUS proxy in order to tunnel the RADIUS traffic to the central RADIUS server in the datacenter.

For information on enabling dynamic RADIUS proxy, see Configuring Dynamic RADIUS Proxy Parameters (Page 196).

Configuring Enterprise Domains

By default, all the DNS requests from a client are forwarded to the client's DNS server. In a typical AP deployment without VPN configuration, client DNS requests are resolved by the DNS server of clients. For the AP-VPN scenario, the enterprise domain settings on the AP are used to determine how client DNS requests are routed. For information on how to configure enterprise domains, see Configuring Enterprise Domains (Page 290).

20.2.2 Configuring a Controller for AP-VPN Operations

Controllers provide an ability to terminate the IPsec and GRE VPN tunnels from the AP and provide corporate connectivity to the branch network.

For AP-VPN operations, ensure that the following configuration and verification procedures are completed on the controller:

- OSPF Configuration
- VPN Configuration
- Branch-ID Allocation
- Branch Status Verification

Note

This section describes the configuration procedures for the controller to realize generic use cases. For information on specific deployment scenarios, see AP-VPN Deployment Scenarios (Page 297).

OSPF Configuration

OSPF is a dynamic IGP based on IETF RFC 2328. The premise of OSPF is that the shortest or fastest routing path is used. The implementation of OSPFv2 allows controllers to deploy effectively in a Layer 3 topology. The controllers can act as the default gateway for all clients and forward user packets to the upstream router.

Each AP-VPN can be defined a separate subnet derived from the corporate intranet pool to allow AP-VPN devices to work independently. For sample topology , refer to the *ArubaOS User Guide*.

To configure general OSPF settings from the controller, perform the following steps:

1. Navigate to the **Configuration >IP** page. The Area and Excluded subnets are displayed in table format. If not explicitly specified for OSPF, the router ID defaults to the switch IP.
2. Click **Add** to add an area.
3. Configure the OSPF interface settings in the Configuration screen. If OSPF is enabled, the parameters contain the correct default values. You can edit the OSPF values only when you enable OSPF on the interface.

OSPF monitoring is available from an IP Routing sub-section (**Controller > IP Routing > Routing**). Both Static and OSPF routes are available in table format. OSPF Interfaces and Neighboring information is available from the **OSPF** tab.

The Interface information includes transmit (TX) and receive (RX) statistics.

To redistribute AP-VPN routes into the OSPF process:

```
(AP)(config) # router ospf redistribute rapng-vpn
```

To verify if the redistribution of the AP-VPN is enabled:

```
(host) #show ip ospf redistribute
```

To configure aggregate route for AP-VPN routes:

```
(host)(config) # router ospf aggregate-route rapng-vpn
```

To view the aggregated routes for AP-VPN routes:

```
(host) #show ip ospf rapng-vpn aggregate-routes RAPNG VPN aggregate routes

--------------------------

Prefix Mask Contributing routes Cost

------ ---- ------------------- ----

201.201.200.0 255.255.252.0 5 268779624

100.100.2.0 255.255.255.0 1 10
```

To verify the details of a configured aggregated route:

```
(host) # show ip ospf rapng-vpn aggregated-routes <net> <mask>

(host) # show ip ospf rapng-vpn aggregate-routes 100.100.2.0 255.255.255.0

Contributing routes of RAPNG VPN aggregate route

------------------------------------------------

Prefix Mask Next-Hop Cost

------ ---- -------- ----

100.100.2.64 255.255.255.224 5.5.0.10 10
```

To view the aggregated routes for AP-VPN routes:

```
(host) #show ip ospf rapng-vpn aggregate-routes

--------------------------

Prefix Mask Contributing routes Cost

------ ---- ------------------- ----

201.201.200.0 255.255.252.0 5 268779624

100.100.2.0 255.255.255.0 1 10
```

To verify the details of a configured aggregated route:

```
(AP) # show ip ospf rapng-vpn aggregated-routes <net> <mask>

(AP) # show ip ospf rapng-vpn aggregate-routes 100.100.2.0 255.255.255.0

Contributing routes of RAPNG VPN aggregate route

------------------------------------------------

Prefix Mask Next-Hop Cost

------ ---- -------- ----

100.100.2.64 255.255.255.224 5.5.0.10 10
```

To view all the redistributed routes:

```
(host)# show ip ospf database

OSPF Database Table
-------------------

Area ID LSA Type       Link ID         Adv Router      Age     Seq#          Checksum
------- --------       -------         ----------      ---     ----          --------
0.0.0.15 ROUTER        9.9.9.9         9.9.9.9         159     0x80000016    0xee92


0.0.0.15   ROUTER         10.15.148.12    10.15.148.12    166    0x80000016    0x4c0d
0.0.0.15   NETWORK        10.15.148.12    10.15.148.12    167    0x80000001    0x9674
0.0.0.15   NSSA           12.12.2.0       9.9.9.9         29     0x80000003    0x7b54
0.0.0.15   NSSA           12.12.12.0      9.9.9.9         164    0x80000008    0x63a
0.0.0.15   NSSA           12.12.12.32     9.9.9.9         164    0x80000008    0x7b8
0.0.0.15   NSSA           50.40.40.0      9.9.9.9         164    0x80000007    0x8ed4
0.0.0.15   NSSA           51.41.41.128    9.9.9.9         164    0x80000007    0x68f6
0.0.0.15   NSSA           53.43.43.32     9.9.9.9         164    0x80000007    0x2633
0.0.0.15   NSSA           54.44.44.16     9.9.9.9         164    0x80000007    0x353
N/A        AS EXTERNAL    12.12.2.0       9.9.9.9         29     0x80000003    0x8c06
N/A        AS EXTERNAL    12.12.12.0      9.9.9.9         169    0x80000001    0x25e4
N/A        AS EXTERNAL    12.12.12.32     9.9.9.9         169    0x80000001    0x2663
N/A        AS EXTERNAL    50.40.40.0      9.9.9.9         169    0x80000001    0xab80
N/A        AS EXTERNAL    51.41.41.128    9.9.9.9         169    0x80000001    0x85a2
N/A        AS EXTERNAL    53.43.43.32     9.9.9.9         169    0x80000001    0x43de
N/A        AS EXTERNAL    54.44.44.16     9.9.9.9         169    0x80000001    0x20fe
```

To verify if the redistributed routes are installed or not:

```
(host)# show ip route

Codes: C - connected, O - OSPF, R - RIP, S - static

M - mgmt, U - route usable, * - candidate default, V - RAPNG VPN

Gateway of last resort is Imported from DHCP to network 0.0.0.0 at cost 10

Gateway of last resort is Imported from CELL to network 0.0.0.0 at cost 10

Gateway of last resort is Imported from PPPOE to network 0.0.0.0 at cost 10

Gateway of last resort is 10.15.148.254 to network 0.0.0.0 at cost 1

S* 0.0.0.0/0 [1/0] via 10.15.148.254*

V 12.12.2.0/24 [10/0] ipsec map

V 12.12.12.0/25 [10/0] ipsec map

V 12.12.12.32/27 [10/0] ipsec map

V 50.40.40.0/24 [10/0] ipsec map

V 51.41.41.128/25 [10/0] ipsec map

V 53.43.43.32/27 [10/0] ipsec map

V 54.44.44.16/28 [10/0] ipsec map

C 9.9.9.0/24 is directly connected, VLAN9

C 10.15.148.0/24 is directly connected, VLAN1

C 43.43.43.0/24 is directly connected, VLAN132

C 42.42.42.0/24 is directly connected, VLAN123
```

```
C 44.44.44.0/24 is directly connected, VLAN125

C 182.82.82.12/32 is an ipsec map 10.15.149.69-182.82.82.12

C 182.82.82.14/32 is an ipsec map 10.17.87.126-182.82.82.14
```

VPN Configuration

The following VPN configuration steps on the controller enable the APs to terminate their VPN connection on the controller:

Whitelist Database Configuration

The whitelist database is a list of the MAC addresses of the APs that are allowed to establish VPN connections with the controller. This list can be either stored in the controller database or on an external server.

You can use the following CLI command to configure the whitelist database entries if the controller is acting as the whitelist database:

```
(host)# whitelist-db rap add mac-address 00:11:22:33:44:55 ap-group test
```

The **ap-group** parameter is not used for any configuration, but needs to be configured. The parameter can be any valid string.

If an external server is used as the location for the whitelist database, add the MAC addresses of the valid APs in the external database or external directory server and then configure a RADIUS server to authenticate the APs using the entries in the external database or external directory server.

If you are using the Windows 2003 server, perform the following steps to configure the external whitelist database on it. There are equivalent steps available for the Windows Server 2008 and other RADIUS servers.

1. Add the MAC addresses of all the APs in the Active Directory of the RADIUS server:
   - Open the **Active Directory and Computers** window, add a new user and specify the MAC address (without the colon delimiter) of the AP for the username and password, respectively.
   - Right-click the user that you have just created and click **Properties**.
   - On the **Dial-in** tab, select **Allow access** in the **Remote Access Permission** section and click **OK.**
   - Repeat Step a through Step c for all APs
2. Define the remote access policy in the IAS:

- In the **Internet Authentication Service** window, select **Remote Access Policies**.
- Launch the wizard to configure a new remote access policy.
- Define filters and select **grant remote access permission** in the **Permissions** window.
- Right-click the policy that you have just created and select **Properties**.
- In the **Settings** tab, select the policy condition, and click **Edit Profile**.
- In the **Advanced** tab, select **Vendor Specific**, and click **Add** to add a new VSAs.
- Add a new VSA and click **OK**.
- In the **IP** tab, provide the IP address of the AP and click **OK**.

VPN Local Pool Configuration

The VPN local pool is used to assign an IP address to the AP after successful XAUTH VPN.

```
(host) # ip local pool "rapngpool" <startip> <endip>
```

Role Assignment for the Authenticated APs

Define a role that includes an Source-NAT rule to allow connections to the RADIUS server and for the Dynamic RADIUS Proxy in the AP to work. This role is assigned to APs after successful authentication

```
(host) (config) #ip access-list session iaprole

(host) (config-sess-iaprole)#any host <radius-server-ip> any src-nat (host) (config-
sess-iaprole)#any any any permit

(host) (config-sess-iaprole)#! (host) (config) #user-role iaprole

(host) (config-role) #session-acl iaprole
```

VPN Profile Configuration

The VPN profile configuration defines the server used to authenticate the AP (internal or an external server) and the role assigned to the AP after successful authentication.

```
(host) (config) #aaa authentication vpn default-iap

(host) (VPN Authentication Profile "default-iap") #server-group default

(host) (VPN Authentication Profile "default-iap") #default-role iaprole
```

Branch-ID Allocation

For branches deployed in Distributed, L3 and Distributed, L2 modes, the master AP in the branch and the controller should agree upon a subnet or IP addresses to be used for DHCP services in the branch. The process or protocol used by the master AP and the controller to determine the subnet or IP addresses used in a branch is called BID allocation. The BID allocation process is not essential for branches deployed in local or Centralized, L2 mode. The following are some of the key functions of the BID allocation process:

- Determines the IP addresses used in a branch for Distributed, L2 mode
- Determines the subnet used in a branch for Distributed, L3 mode
- Avoids IP address or subnet overlap (that is, avoids IP conflict)
- Ensures that a branch is allocated the same subnet or range of IP addresses irrespective of which AP in the branch becomes the master in the AP cluster

Branch Status Verification

To view the details of the branch information connected to the controller, execute the **show iap table**

command.

Example

This example shows the details of the branches connected to the controller:

```
(host) #show iap table long

IAP Branch Table
----------------

Name            VC MAC Address    Status  Inner IP       Assigned Subnet  Assigned Vlan
----            --------------    ------  --------       ---------------  -------------
Tokyo-CB:D3:16  6c:f3:7f:cc:42:f8 DOWN    0.0.0.0

Paris-CB:D3:16  6c:f3:7f:cc:3d:04 UP      10.15.207.140  10.15.206.99/29  2
LA              6c:f3:7f:cc:42:25 UP      10.15.207.111  10.15.206.24/29  2
Munich          d8:c7:c8:cb:d3:16 DOWN    0.0.0.0

London-c0:e1    6c:f3:7f:c0:e1:b1 UP      10.15.207.120  10.15.206.64/29  2
SCALANCE W-CB:D36c:f3:7f:cc:42:1e DOWN    0.0.0.0

Delhi           6c:f3:7f:cc:42:ca DOWN    0.0.0.0

Singapore       6c:f3:7f:cc:42:cb UP      10.15.207.122  10.15.206.120/29 2


Key         Bid(Subnet Name)
---         ----------------
b3c65c...

b3c65c...

b3c65c...   2(10.15.205.0-10.15.205.250,5),1(10.15.206.1-10.15.206.252,5)
a2a65c...   0
b3c65c...   7(10.15.205.0-10.15.205.250,5),8(10.15.206.1-10.15.206.252,5)
b3c65c...

b3c65c...   1(10.15.205.0-10.15.205.250,5),2(10.15.206.1-10.15.206.252,5)
b3c65c...   14(10.15.205.0-10.15.205.250,5),15(10.15.206.1-10.15.206.252,5)
```

The output of this command provides the following information:

Table 20- 3 Branch Details

Parameter	**Description**
Name	Displays the name of the branch.
VC MAC Address	Displays the MAC address of the virtual controller of the branch.
Status	Displays the current status of the branch (UP or DOWN).
Inner IP	Displays the internal VPN IP of the branch.
Assigned Subnet	Displays the subnet mask assigned to the branch.
Assigned Vlan	Displays the VLAN ID assigned to the branch.
Key	Displays the key for the branch, which is unique to each branch.
Bid(Subnet Name)	Displays the Branch ID (BID) of the subnet. In the example above, the controller displays bid-per-subnet-per-branch i.e., for "LA" branch, BID "2" for the ip-range "10.15.205.0-10.15.205.250" with client count per branch "5"). If a branch has multiple subnets, it can have multiple BIDs. If a branch is in **UP** state and does not have a **Bid(Subnet Name)**, it means that the AP is connected to a controller, which did not assign any BID for any subnet. In the above example, "Paris-CB:D3:16" branch is **UP** and does not have a **Bid(Subnet Name)**. This means that either the AP is connected to a backup controller or it is connected to a primary controller without any Distributed, L2 or Distributed, L3 subnets.

Note

The **show iap table** command output does not display the **Key** and **Bid(Subnet Name)** details.

AP-VPN Deployment Scenarios 21

This section describes the most common AP-VPN deployment models and provides information to carry out the necessary configuration procedures. The examples in this section refer to more than one DHCP profile and wired port configuration in addition to wireless SSID configuration. All these are optional. In most networks, a single DHCP profile and wireless SSID configuration referring to a DHCP profile is sufficient.

The following scenarios are described in this section:

Scenario 1—IPsec: Single Datacenter Deployment with No Redundancy (Page 297)

Scenario 2—IPsec: Single Datacenter with Multiple Controllers for Redundancy (Page 302)

Scenario 3—IPsec: Multiple Datacenter Deployment with Primary and Backup Controllers for Redundancy (Page 308)

Scenario 4—GRE: Single Datacenter Deployment with No Redundancy (Page 314)

21.1 Scenario 1 - IPsec: Single Datacenter Deployment with No Redundancy

This scenario includes the following configuration elements:

1. Single VPN primary configuration using IPsec.
2. Split-tunneling of client traffic.
3. Split-tunneling of DNS traffic from clients.
4. Distributed, L3 and Centralized, L2 mode DHCP.
5. RADIUS server within corporate network and authentication survivability for branch survivability.
6. Wired and wireless users in L2 and L3 modes, respectively.
7. Access rules defined for wired and wireless networks to permit all traffic.

Topology

The following figure shows the topology and the IP addressing scheme used in this scenario.

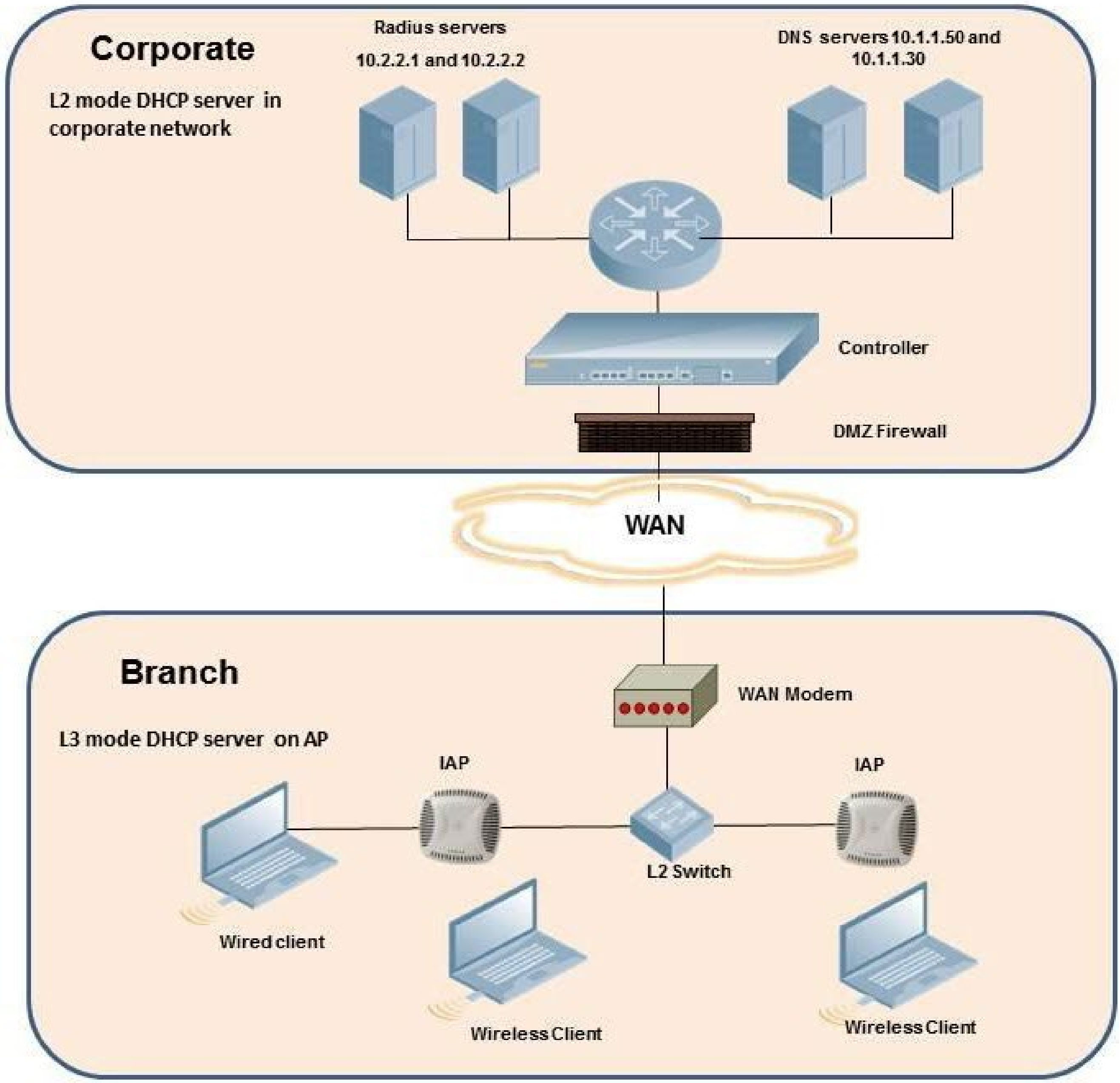


Figure 21-1 Scenario 1 - IPsec: Single datacenter Deployment with No Redundancy

The following IP addresses are used in the examples for this scenario:

- 10.0.0.0/8 is the corporate network
- 10.20.0.0/16 subnet is reserved for L2 mode
- 10.30.0.0/16 subnet is reserved for L3 mode
- Client count in each branch is 200

AP Configuration

The following table provides information on the configuration steps performed through the CLI with example values. For information on the UI procedures, see the topics referenced in the *UI Procedure* column.

Table 21- 1 AP Configuration for Scenario 1—IPsec: Single Datacenter Deployment with No Redundancy

Configuration Steps		**CLI Commands**	**UI Procedure**
1	Configure the primary host for VPN with the Public VRRP IP address of the controller.	`(AP)(config)# vpn primary <public VRRP IP ofcontroller>`	See Configuring an IPsec Tunnel (Page 275)

2	Configure a routing profile to tunnel all 10.0.0.0/8 subnet traffic to controller.	`(AP)(config)# routing- profile`
		`(AP)(routing-profile)# route 10.0.0.0 255.0.0.0 <public VRRP IP of controller>`
			See Configuring Routing Profiles (Page 281)

3	Configure Enterprise DNS for split DNS. The example in the next column uses a specific enterprise domain to only tunnel all DNS queries matching that domain to corporate.	`(AP)(config)# internal-domains`
		`(AP)(domains)# domain-name corpdomain.com`
			See Configuring Enterprise Domains (Page 287)

4	Configure Centralized, L2 and Distributed, L3 with VLAN 20 and VLAN 30, respectively.	**Centralized, L2 profile**
		`(AP)(config)# ip dhcp l2-dhcp`
		`(AP)(DHCP Profile "l2-dhcp")# server-type Centralized,L2`
		`(AP)(DHCP Profile "l2-dhcp")# server-vlan 20`
		Distributed, L3 profile
		`(AP)(config)# ip dhcp l3-dhcp`
		`(AP)(DHCP Profile "l3-dhcp")# server-type Distributed,L3`
		`(AP)(DHCP Profile "l3-dhcp")# server-vlan 30`
		`(AP)(DHCP Profile "l3-dhcp")# ip-range 10.30.0.0 10.30.255.255`
		`(AP)(DHCP Profile "l3-dhcp")# dns-server 10.1.1.50,10.1.1.30`
		`(AP)(DHCP Profile "l3-dhcp")# domain-name corpdomain.com`
		`(AP)(DHCP Profile "l3-dhcp")# client-count 200`
		NOTE: The IP range configuration on each branch will be the same. Each AP will derive a smaller subnet based on the client count scope using the Branch ID (BID) allocated by controller.
			See Configuring Centralized DHCP Scopes (Page 260)
			and Configuring Distributed DHCP Scopes (Page 256)

Configuration Steps		CLI Commands	UI Procedure

5	Create authentication servers for user authentication. The example in the next column assumes 802.1X SSID	`(AP)(config)# wlan auth-server server1`
		`(AP)(Auth Server "server1")# ip 10.2.2.1`
		`(AP)(Auth Server "server1")# port 1812`
		`(AP)(Auth Server "server1")# acctport 1813`
		`(AP)(Auth Server "server1")# key "presharedkey"`
		`(AP)(Auth Server "server1")# exit`
		
		`(AP)(config)# wlan auth-server server2`
		`(AP)(Auth Server "server2")# ip 10.2.2.2`
		`(AP)(Auth Server "server2")# port 1812`
		`(AP)(Auth Server "server2")# acctport 1813`
		`(AP)(Auth Server "server2")# key "presharedkey"`
			See Configuring an External Server for Authentication (Page 188)

6	Configure wired port and wireless SSIDs using the authentication servers.	Configure wired ports to operate in L2 mode and associate Centralized, L2 mode VLAN 20 to the wired port profile.
		`(AP)(config) # wired-port-profile wired-port`
		`(AP)(wired-port-profile "wired-port")# switchport-mode access`
		`(AP)(wired-port-profile "wired-port")# allowed-vlan all`
		`(AP)(wired-port-profile "wired-port")# native-vlan 20`
		`(AP)(wired-port-profile "wired-port")# no shutdown`
		`(AP)(wired-port-profile "wired-port")# access-rule-name wired-port`
		`(AP)(wired-port-profile "wired-port")# type employee`
		`(AP)(wired-port-profile "wired-port")# auth- server server1`
		`(AP)(wired-port-profile "wired-port")# auth- server server2`
		`(AP)(wired-port-profile "wired-port")# dot1x`
		`(AP)(wired-port-profile "wired-port")# exit`
		`(AP)(config)# enet1-port-profile wired-port`
		Configure a wireless SSID to operate in L3 mode and associate Distributed, L3 mode VLAN 30 to the WLAN SSID profile.
		`(AP)(config) # wlan ssid-profile wireless- ssid`
		`(AP)(SSID Profile "wireless-ssid")# enable (AP)(SSID Profile "wireless-ssid")# type employee`
		`(AP)(SSID Profile "wireless-ssid")# essid wireless-ssid`
		`(AP)(SSID Profile "wireless-ssid")# opmode wpa2-aes`
		`(AP)(SSID Profile "wireless-ssid")# vlan 30 (AP)(SSID Profile "wireless-ssid")# auth- server server1`
		`(AP)(SSID Profile "wireless-ssid")# auth- server server2`
		`(AP)(SSID Profile "wireless-ssid")# auth- survivability`
			See Configuring a Wired Profile (Page 125) and Wireless Network Profiles (Page 95)

7	Create access rule for wired and wireless authentication. In this example, the rule permits all traffic	**For wired profile:**
		`(AP)(config)# wlan access-rule wired-port`
		`(AP)(Access Rule "wired-port")# rule any any match any any any permit`
		
		For WLAN SSID:
		`(AP)(config)# wlan access-rule wireless-ssid`
		`(AP)(Access Rule "wireless-ssid")# rule any any match any any any permit`
			See Configuring ACL Rules for Network Services (Page 220)

NOTE: Ensure that you execute the **commit apply** command in the SCALANCE W CLI before saving the configuration and propagating changes across the AP cluster.			

AP-Connected Switch Configuration

Client VLANs defined in this example must be opened on the upstream switches in multiple AP deployments, as client traffic from the slave to the master is tagged with the client VLAN.

Datacenter Configuration

For information on controller configuration, see Configuring a Controller for AP-VPN Operations (Page 290). Ensure that the upstream router is configured with a static route pointing to the controller for the L3 VLAN.

21.2 Scenario 2 - IPsec: Single Datacenter with Multiple controllers for Redundancy

This scenario includes the following configuration elements:

- A VRRP instance between the master/standby-master pair, which is configured as the primary VPN IP address.
- Tunneling of all traffic to datacenter.
- Exception route to bypass tunneling of RADIUS and AirWave traffic, which are locally reachable in the branch and the Internet, respectively.
- All client DNS queries are tunneled to the controller.
- Distributed, L3 and Centralized, L2 mode DHCP on all branches. L3 is used by the employee network and L2 is used by the guest network with captive portal.
- Wired and wireless users in L2 and L3 modes.
- Access rules defined for wired and wireless networks.

Topology

The following figure shows the topology and the IP addressing scheme used in this scenario.

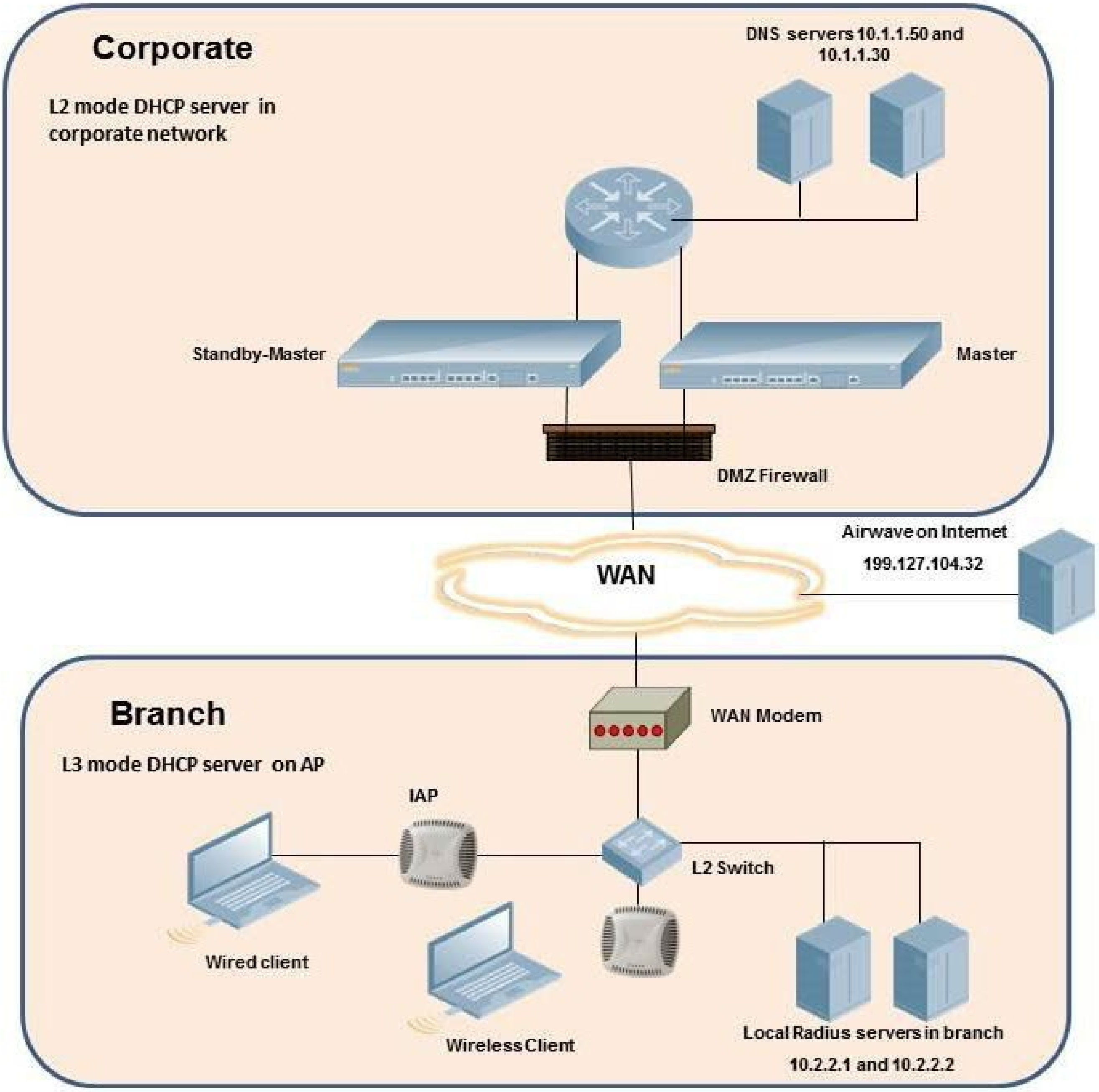


Figure 21-2 Scenario 2 - IPsec: Single Datacenter with Multiple controllers for Redundancy

The following IP addresses are used in the examples for this scenario:

- 10.0.0.0/8 is the corporate network
- 10.20.0.0/16 subnet is reserved for L2 mode – used for guest network
- 10.30.0.0/16 subnet is reserved for L3 mode
- Client count in each branch is 200
- 10.2.2.0/24 is a branch-owned subnet, which needs to override global routing profile
- 199.127.104.32 is used an example IP address of the AirWave server in the Internet

AP Configuration

The following table provides information on the configuration steps performed through the CLI with example values. For information on the UI procedures, see the topics referenced in the *UI Procedure* column.

Table 21- 2 AP Configuration for Scenario 2—IPsec: Single Datacenter with Multiple controllers for Redundancy

Configuration Steps		CLI Commands	UI Procedure
1	Configure the primary host for VPN with the Public VRRP IP address of the controller.	(AP)(config)# vpn primary <public VRRP IP of controller>	See Configuring an IPsec Tunnel (Page 275)
2	Configure routing profiles to tunnel traffic through IPsec.	(AP)(config)# routing-profile (AP)(routing-profile)# route 0.0.0.0 0.0.0.0 <public VRRP IP of controller>	See Configuring Routing Profiles (Page 281)
3	Define routing profile exception RADIUS server and AirWave IPs, since the design requirement for this solution requires local RADIUS authentication, even though the IP matches the routing profile destination.	(AP)(config)# routing-profile (AP)(routing-profile)# route 10.2.2.1 255.255.255.255 0.0.0.0 (AP)(routing-profile)# route 10.2.2.2 255.255.255.255 0.0.0.0(AP)(routing-profile)# route 199.127.104.32255.255.255.255 0.0.0.0	See Configuring Routing Profiles (Page 281)
4	Configure Enterprise DNS. The configuration example in the next column tunnels all DNS queries to the original DNS server of clients without proxying on AP.	(AP)(config)# internal-domains (AP)(domains)# domain-name *	See Configuring Enterprise Domains (Page 287)

Configuration Steps		CLI Commands	UI Procedure

5	Configure Centralized, L2and Distributed, L3 with VLAN 20 and VLAN 30,respectively.	**Centralized, L2 profile**
		`(AP)(config)# ip dhcp l2-dhcp`
		`(AP)(DHCP Profile "l2-dhcp")# server-type Centralized,L2`
		`(AP)(DHCP Profile "l2-dhcp")# server-vlan 20`
		Distributed, L3 profile
		`(AP)(config)# ip dhcp l3-dhcp`
		`(AP)(DHCP Profile "l3-dhcp")# server-typeDistributed,L3`
		`(AP)(DHCP Profile "l3-dhcp")# server-vlan 30`
		`(AP)(DHCP Profile "l3-dhcp")# ip-range10.30.0.0 10.30.255.255`
		`(AP)(DHCP Profile "l3-dhcp")# dns-server10.1.1.50,10.1.1.30`
		`(AP)(DHCP Profile "l3-dhcp")# domain-namecorpdomain.com`
		`(AP)(DHCP Profile "l3-dhcp")# client-count 200`
		NOTE: The IP range configuration on each branch will be the same. Each AP will derive a smaller subnet based on the client count scope using the BID allocated by controller.
			See Configuring Centralized DHCP Scopes
			(Page 260)and Configuring Distributed DHCP Scopes
			(Page 256)

6	Create authentication servers for user authentication. The example in the next column assumes 802.1X SSID.	`(AP)(config)# wlan auth-server server1`
		`(AP)(Auth Server "server1")# ip 10.2.2.1`
		`(AP)(Auth Server "server1")# port 1812`
		`(AP)(Auth Server "server1")# acctport 1813`
		`(AP)(Auth Server "server1")# key "presharedkey"`
		`(AP)(Auth Server "server1")# exit`
		
		`(AP)(config)# wlan auth-server server2`
		`(AP)(Auth Server "server2")# ip 10.2.2.2`
		`(AP)(Auth Server "server2")# port 1812`
		`(AP)(Auth Server "server2")# acctport 1813`
		`(AP)(Auth Server "server2")# key "presharedkey"`
			See Configuring an External Server for Authentication
			(Page 188)

Configuration Steps		CLI Commands	UI Procedure

7	Configure wired port and wireless SSIDs using the authentication servers.	Configure wired ports to operate in L3 mode and associate Distributed, L3 mode VLAN 30 to the wired port profile.
		`(AP)(config) # wired-port-profile wired-port`
		`(AP)(wired-port-profile "wired-port")# switchport-mode access`
		`(AP)(wired-port-profile "wired-port")# allowed-vlan all`
		`(AP)(wired-port-profile "wired-port")# native-vlan 30`
		`(AP)(wired-port-profile "wired-port")# no shutdown`
		`(AP)(wired-port-profile "wired-port")# access-rule-name wired-port`
		`(AP)(wired-port-profile "wired-port")# type employee`
		`(AP)(wired-port-profile "wired-port")# auth-server server1`
		`(AP)(wired-port-profile "wired-port")# auth-server server2`
		`(AP)(wired-port-profile "wired-port")# dot1x`
		`(AP)(wired-port-profile "wired-port")# exit`
		`(AP)(config)# enet1-port-profile wired-port`
		
		Configure a wireless SSID to operate in L2 mode and associate Centralized, L2 mode VLAN 20 to the WLAN SSID profile.
		`(AP)(config) # wlan ssid-profile guest`
		`(AP)(SSID Profile "guest")# enable`
		`(AP)(SSID Profile "guest")# type guest`
		`(AP)(SSID Profile "guest")# essid guest`
		`(AP)(SSID Profile "guest")# opmode opensystem`
		`(AP)(SSID Profile "guest")# vlan 20`
		`(AP)(SSID Profile "guest")# auth-server server1`
		`(AP)(SSID Profile "guest")# auth-server server2`
		`(AP)(SSID Profile "guest")# captive-portal internal`
		
		NOTE: This example uses internal captive portal use case using external authentication server. You can also use an external captive portal example.
		NOTE: The SSID type **guest** is used in this example to enable configuration of captive portal. However, corporate access through VPN tunnel is still allowed for this SSID because the VLAN associated to this SSID is a VPN-enabled VLAN (20 in this example).
			See Configuring a Wired Profile (Page 125) and Wireless Network Profiles (Page 95)

8	Create access rule for wired and wireless authentication. In this example, the rule permits all traffic.	**For wired profile:**
		`(AP)(config)# wlan access-rule wired-port`
		`(AP)(Access Rule "wired-port")# rule any any match any any any permit`
		
		For WLAN SSID:
		`(AP)(config)# wlan access-rule guest`
		`(AP)(Access Rule "guest")# rule any any match any any any permit`
			See Configuring ACL Rules for Network Services (Page 220)

NOTE: Ensure that you execute the **commit apply** command in the SCALANCE W CLI before saving the configuration and propagating changes across the AP cluster.			

AP-Connected Switch Configuration

Client VLANs defined in this example must be opened on the upstream switches in multiple AP deployments, as client traffic from the slave to the master is tagged with the client VLAN.

Datacenter Configuration

For information on controller configuration, see Configuring a Controller for AP-VPN Operations (Page 290). Ensure that the upstream router is configured with a static route pointing to the controller for the L3 VLAN.

21.3 Scenario 3 - IPsec: Multiple Datacenter Deployment with Primary and Backup Controllers for Redundancy

This scenario includes the following configuration elements:

- Multiple controller deployment model with controllers in different data centers operating as primary or backup VPN with **Fast Failover** and preemption enabled.
- Split-tunneling of traffic.
- Split-tunneling of client DNS traffic.
- Two Distributed, L3 mode DHCPs, one each for employee and contractors; and one Local mode DHCP server.
- RADIUS server within corporate network and authentication survivability enabled for branch survivability.
- Wired and wireless users in L3 and NAT modes, respectively.
- Access rules for wired and wireless users with source-NAT-based rule for contractor roles to bypass global routing profile.
- OSPF based route propagation on controller.

Topology

The following figure shows the topology and the IP addressing scheme used in this scenario.

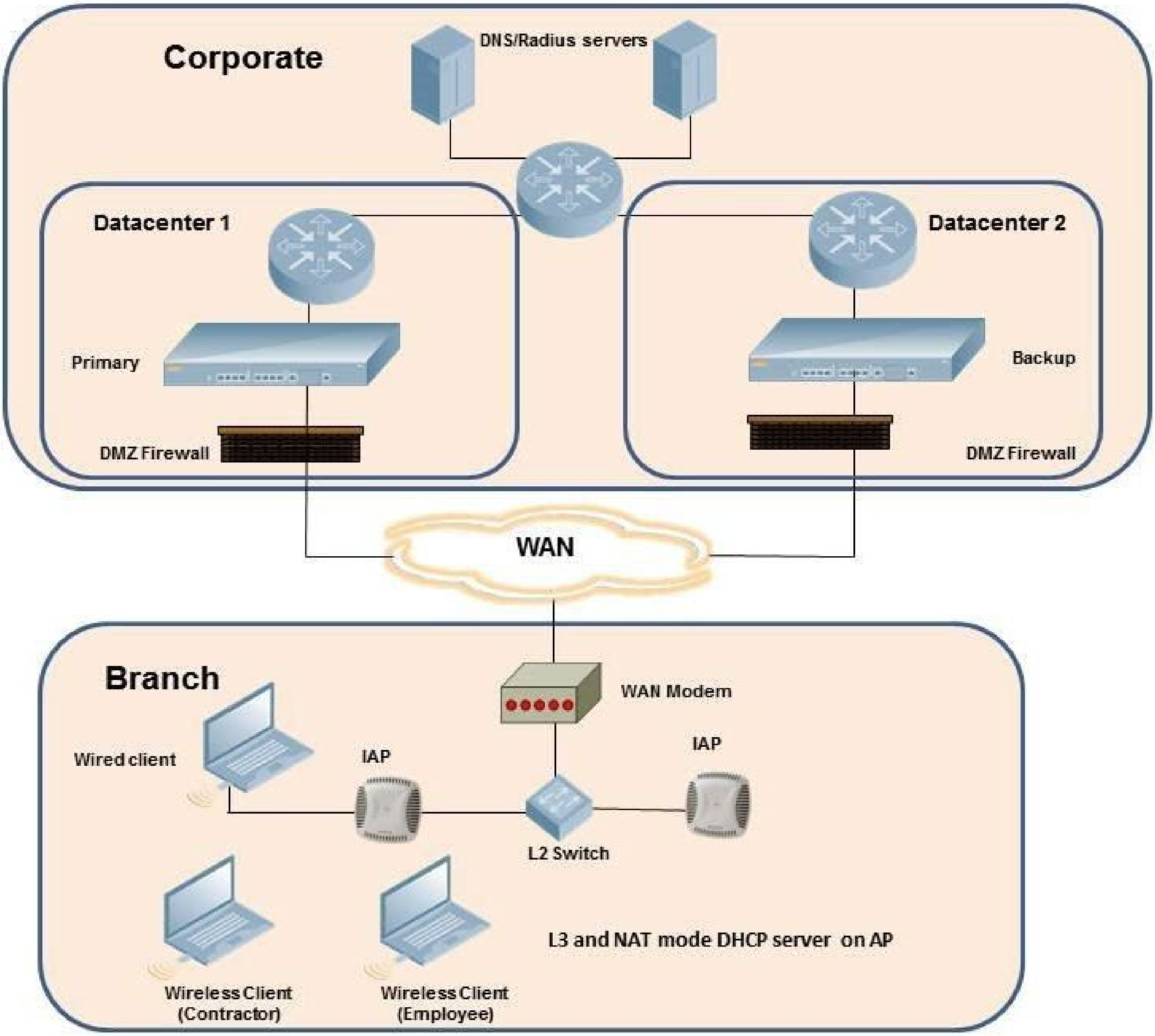


Figure 21-3 Scenario 3 - IPsec: Multiple Datacenter Deployment with Primary and Backup Controllers for Redundancy

The IP addressing scheme used in this example is as follows:

- 10.0.0.0/8 is the corporate network.
- 10.30.0.0/16 subnet is reserved for L3 mode –used by Employee SSID.
- 10.40.0.0/16 subnet is reserved for L3 mode –used by Contractor SSID.
- 172.16.20.0/24 subnet is used for NAT mode – used for wired network.
- Client count in each branch is 200.
- Contractors are only permitted to reach 10.16.0.0/16 network.

AP Configuration

This section provides information on configuration steps performed through the CLI and the UI.

Table 21- 3 AP Configuration for Scenario 3—IPsec: Multiple Datacenter Deployment

	Configuration Steps	CLI Commands	UI Procedure

1	Configure the primary IP address. This IP address is the Public IP address of the controller. **Fast Failover** is enabled for fast convergence.	`(AP)(config)# vpn primary <public IP of primary controller>`
		`(AP)(config) # vpn backup <public IP of backup controllers>`
		`(AP)(config)# vpn preemption`
		`(AP)(config)# vpn fast-failover`
			See Configuring an IPsec Tunnel (Page 275)

2	Configure routing profiles to tunnel traffic through IPsec.	`(AP)(config)# routing-profile`
		`(AP)(routing-profile)# route 0.0.0.0 0.0.0.0`
		`<public IP of primary controller>`
		`(AP)(routing-profile)# route 10.0.0.0 255.0.0.0 <public IP of backup controller>`
			See Configuring Routing Profiles (Page 281)

3	Configure Enterprise DNS for split DNS. The example in the next column uses a specific enterprise domain to tunnel all DNS queries matching that domain to corporate.	`(AP)(config)# internal-domains`
		`(AP)(domains)# domain-name corpdomain.com`
			See Configuring Enterprise Domains (Page 287)

	Configuration Steps	CLI Commands	UI Procedure

4	Configure Distributed, L3DHCP profiles with VLAN30 and VLAN 40.	**Distributed, L3 profile with VLAN 30**
		`(AP)(config)# ip dhcp l3-dhcp`
		`(AP)(DHCP profile "l3-dhcp")# server-type Distributed,L3`
		`(AP)(DHCP profile "l3-dhcp")# server-vlan 30`
		`(AP)(DHCP profile "l3-dhcp")# ip-range 10.30.0.0 10.30.255.255`
		`(AP)(DHCP profile "l3-dhcp")# dns-server 10.1.1.50,10.1.1.30`
		`(AP)(DHCP profile "l3-dhcp")# domain-namecorpdomain.com`
		`(AP)(DHCP profile "l3-dhcp")# client-count 200`
		Distributed, L3 profile with VLAN 40
		`(AP)(config)# ip dhcp l3-dhcp`
		`(AP)(DHCP profile "l3-dhcp")# server-type Distributed,L3`
		`(AP)(DHCP profile "l3-dhcp")# server-vlan 40`
		`(AP)(DHCP profile "l3-dhcp")# ip-range10.40.0.0 10.40.255.255`
		`(AP)(DHCP profile "l3-dhcp")# dns-server10.1.1.50,10.1.1.30`
		`(AP)(DHCP profile "l3-dhcp")# domain-name corpdomain.com`
		`(AP)(DHCP profile "l3-dhcp")# client-count 200`
		Local profile with VLAN 20
		`(AP)(config)# ip dhcp local`
		`(AP)(DHCP profile "local")# server-type Local`
		`(AP)(DHCP profile "local")# server-vlan 20`
		`(AP)(DHCP profile "local")# subnet 172.16.20.1`
		`(AP)(DHCP profile "local")# subnet-mask 255.255.255.0`
		`(AP)(DHCP profile "local")# lease-time 86400 (AP)(DHCP profile "local")# dns-server 10.1.1.30,10.1.1.50`
		`(AP)(DHCP profile "local")# domain-name siemens.com`
		
		NOTE: The IP range configuration on each branch will be the same. Each AP will derive a smaller subnet based on the client count scope using the BID allocated by the controller
			See Configuring Distributed DHCP Scopes (Page 256) and Configuring Local DHCP Scopes (Page 260)

5	5. Create authentication servers for user authentication. The example in the next column assumes 802.1X SSID.	`(AP)(config)# wlan auth-server server1`
		`(AP)(Auth Server "server1")# ip 10.2.2.1`
		`(AP)(Auth Server "server1")# port 1812`
		`(AP)(Auth Server "server1")# acctport 1813`
		`(AP)(Auth Server "server1")# key "presharedkey"`
		`(AP)(Auth Server "server1")# exit`
		`(AP)(config)# wlan auth-server server2`
		`(AP)(Auth Server "server1")# ip 10.2.2.2`
		`(AP)(Auth Server "server1")# port 1812`
		`(AP)(Auth Server "server1")# acctport 1813`
		`(AP)(Auth Server "server1")# key "presharedkey"`
			See Configuring an External Server for Authentication (Page 188)

	Configuration Steps	CLI Commands	UI Procedure
6	Configure wired port and wireless SSIDs using the authentication servers and access rules; enable authentication survivability.	Configure wired ports to operate in NAT mode and associate VLAN 20 to the wired port profile. (AP)(config) # wired-port-profile wired-port (AP)(wired-port-profile "wired-port")# switchport-mode access (AP)(wired-port-profile "wired-port")# allowed-vlan all (AP)(wired-port-profile "wired-port")# native-vlan 20 (AP)(wired-port-profile "wired-port")# no shutdown (AP)(wired-port-profile "wired-port")# access-rule-name wired-port (AP)(wired-port-profile "wired-port")# type employee (AP)(wired-port-profile "wired-port")# auth- server server1 (AP)(wired-port-profile "wired-port")# auth- server server2 (AP)(wired-port-profile "wired-port")# dot1x (AP)(wired-port-profile "wired-port")# exit (AP)(config)# enet1-port-profile wired-port Configure a wireless SSID to operate in L3 mode for employee and associate Distributed, L3 mode VLAN 30 to the WLAN SSID profile. (AP)(config) # wlan ssid-profile wireless-ssid (AP)(SSID Profile "wireless-ssid")# enable (AP)(SSID Profile "wireless-ssid")# type employee (AP)(SSID Profile "wireless-ssid")# essid wireless-ssid (AP)(SSID Profile "wireless-ssid")# opmode wpa2-aes (AP)(SSID Profile "wireless-ssid")# vlan 30 (AP)(SSID Profile "wireless-ssid")# auth-server server1 (AP)(SSID Profile "wireless-ssid")# auth-server server2 (AP)(SSID Profile "wireless-ssid")# auth-survivability Configure a wireless SSID to operate in L3 mode for contractor and associate Distributed, L3 mode VLAN 40 to the WLAN SSID profile. (AP)(config) # wlan ssid-profile wireless-ssid-contractor (AP)(SSID Profile "wireless-ssid- contractor")# enable (AP)(SSID Profile "wireless-ssid- contractor")# type contractor (AP)(SSID Profile "wireless-ssid- contractor")# essid wireless-ssid-contractor (AP)(SSID Profile "wireless-ssid- contractor")# opmode wpa2-aes (AP)(SSID Profile "wireless-ssid- contractor")# vlan 40 (AP)(SSID Profile "wireless-ssid- contractor")# auth-server server1 (AP)(SSID Profile "wireless-ssid- contractor")# auth-server server2 (AP)(SSID Profile "wireless-ssid- contractor")# auth-survivability	See Configuring a Wired Profile (Page 125) and Wireless Network Profiles (Page 95)

	Configuration Steps	CLI Commands	UI Procedure

7	Create access rule for wired and wireless authentication. In this example, the rule permits all traffic. For contractor SSID role, the rule allows only 10.16.0.0/16 network and all other traffic address is translated at the source and the global routing profile definition is bypassed.	**For wired profile:**
		`(AP)(config)# wlan access-rule wired-port`
		`(AP)(Access Rule "wired-port")# rule any any match any any any permit`
		For WLAN SSID employee roles:
		`(AP)(config)# wlan access-rule wireless-ssid-contractor`
		`(AP)(Access Rule "wireless-ssid-contractor")`
		`# rule 10.16.0.0 255.255.0.0 match any any any permit`
		`(AP)(Access Rule "wireless-ssid-contractor")`
		`# rule any any match any any any src-nat`
			See Configuring ACL Rules for Network Services (Page 220)

NOTE: Ensure that you execute the **commit apply** command in the SCALANCE W CLI before saving the configuration and propagating changes across the AP cluster.			

AP-Connected Switch Configuration

Client VLANs defined in this example must be opened on the upstream switches in multiple AP deployments, as client traffic from the slave to the master is tagged with the client VLAN.

Datacenter Configuration

For information on controller configuration, see Configuring a Controller for AP-VPN Operations (Page 290). The following OSPF configuration is required on the controller to redistribute AP-VPN routes to upstream routers:

```
(host)(config) # router ospf

(host)(config) # router ospf router-id <ID>

(host)(config) # router ospf area 0.0.0.0

(host)(config) # router ospf redistribute rapng-vpn
```

21.4 Scenario 4 - GRE: Single Datacenter Deployment with No Redundancy

This scenario includes the following configuration elements:

- Single VPN primary configuration using GRE
  - **Aruba GRE**, does not require any configuration on the Aruba Mobility Controller that acts as a GRE endpoint.
  - **Manual GRE**, which requires GRE tunnels to be explicitly configured on the GRE endpoint that can be an Aruba Mobility Controller or any device that supports GRE termination.
- Tunneling of all traffic to datacenter
- Centralized, L2 mode DHCP profile
- RADIUS server within corporate network and authentication survivability for branch survivability.
- Wired and wireless users in L2 mode
- Access rules defined for wired and wireless networks to permit all traffic

Topology

The following Figure shows the topology and the IP addressing scheme used in this scenario:

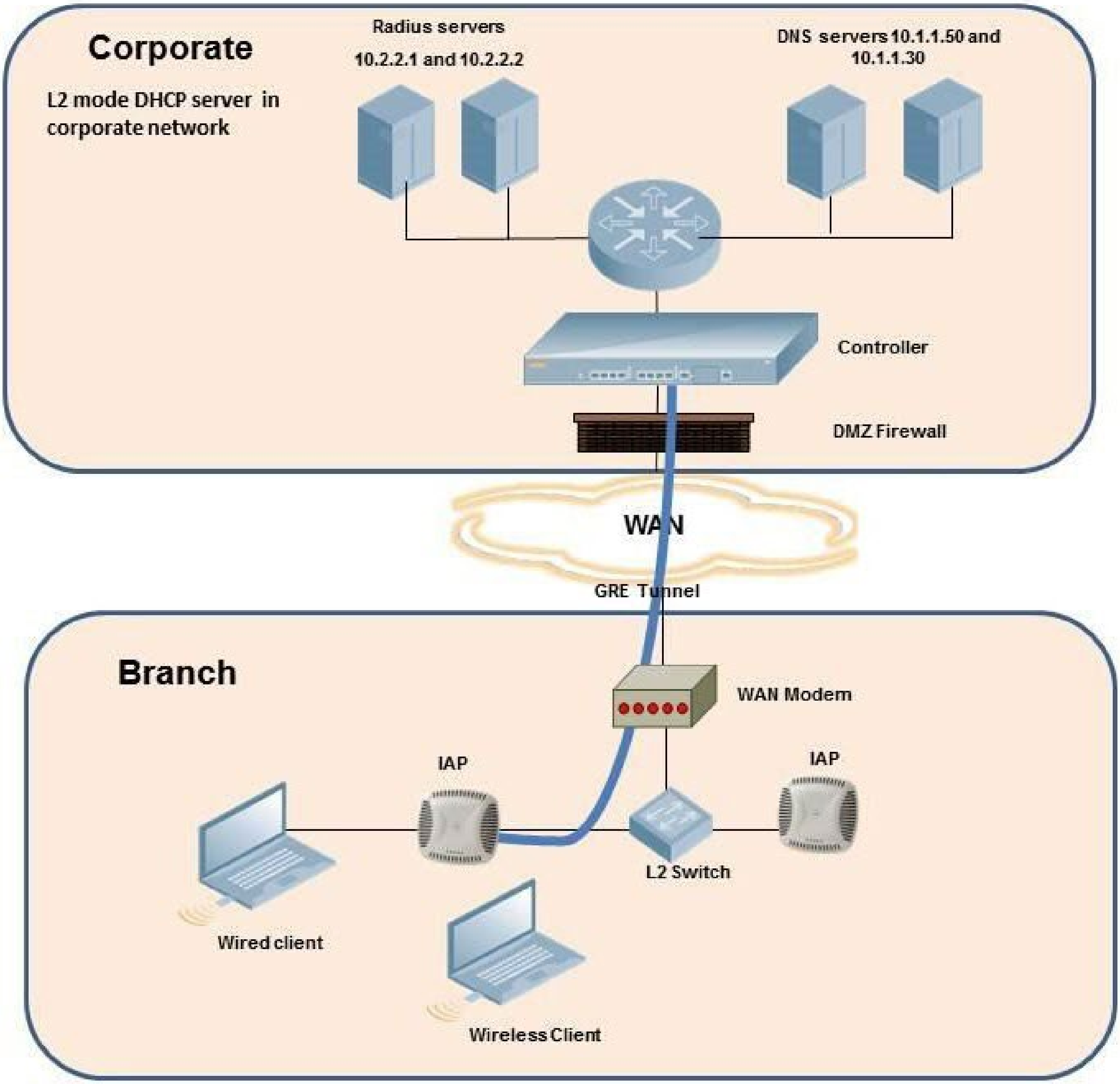


Figure 21-4 Scenario 4 - GRE: Single Datacenter Deployment with No Redundancy

The following IP addresses are used in the examples for this scenario:

- 10.0.0.0/8 is the corporate network.
- 10.20.0.0/16 subnet is reserved for L2 mode

AP Configuration

This section provides information on configuration steps performed by using the CLI and the UI.

Configuration Steps		CLI Commands	UI Procedure

1	Configure Aruba GRE or manual GRE
	• Aruba GRE uses an IPsec tunnel to facilitate controller configuration and requires VPN to be configured. This VPN tunnel is not used for any client traffic.
	• Manual GRE uses standard GRE tunnel configuration and requires controller configuration to complete the GRE tunnel.
		Aruba GRE configuration
		`(AP)(config)# vpn primary <controller-IP>`
		`(AP)(config)# vpn gre-outside`
		Manual GRE configuration
		`(AP)(config)# gre primary <controller-IP>`
		`(AP)(config)# gre type 80`
		Per-AP GRE tunnel configuration
		Optionally, per-AP GRE tunnel can also be enabled, which causes each AP to form an independent GRE tunnel to the GRE end- point. Aruba GRE requires each AP MAC to be present in the controller whitelist. Manual GRE requires GRE configuration for the IP of each AP on the controller.
		`(AP)(config)# gre per-ap-tunnel`
		NOTE: If a virtual controller IP is configured and per-AP GRE tunnel is disabled, AP uses virtual controller IP as the GRE source IP.
		For Manual GRE, this simplifies configuration on controller, since only the virtual controller IP destined GRE tunnel interface configuration is required**.**
			See Configuring Aruba GRE Parameters (Page 277)
			and Configuring Manual GRE Parameters (Page 277)

2	Configure routing profiles to tunnel traffic through GRE.	`(AP)(config)# routing-profile`
		`(AP)(routing-profile)# route 0.0.0.0 0.0.0.0 <IP of GRE-endpoint>`
			See Configuring Routing Profiles (Page 281)

3	Configure Enterprise DNS. The example in the next column tunnels all DNS queries to the client's original DNS server without proxying on AP.	`(AP)(config)# internal-domains`
		`(AP)(domains)# domain-name *`
			See Configuring Enterprise Domains (Page 287)

4	Configure Centralized, L2 DHCP profile with VLAN 20.	**Centralized, L2 DHCP profile VLAN 20**
		`(AP)(config)# ip dhcp l2-dhcp`
		`(AP)(DHCP profile "l2-dhcp")# server-type Centralized,L2`
		`(AP)(DHCP profile "l2-dhcp")# server-vlan 20`
			See Configuring Centralized DHCP Scopes (Page 260)

Configuration Steps		CLI Commands	UI Procedure

5	Create authentication servers for user authentication. The example in the next column assumes 802.1X SSID.	`(AP)(config)# wlan auth-server server1`
		`(AP)(Auth Server "server1")# ip 10.2.2.1`
		`(AP)(Auth Server "server1")# port 1812`
		`(AP)(Auth Server "server1")# acctport 1813`
		`(AP)(Auth Server "server1")# key "presharedkey"`
		`(AP)(Auth Server "server1")# exit`
		
		`(AP)(config)# wlan auth-server server2`
		`(AP)(Auth Server "server1")# ip 10.2.2.2`
		`(AP)(Auth Server "server1")# port 1812`
		`(AP)(Auth Server "server1")# acctport 1813`
		`(AP)(Auth Server "server1")# key "presharedkey"`
			See Configuring an External Server for Authentication

Configuration Steps		CLI Commands	UI Procedure

6	Configure wired and wireless SSIDs using the authentication servers and access rules; enable authentication survivability.	Configure wired ports to operate in Centralized, L2 mode and associate VLAN 20 to the wired port profile.
		`(AP)(config) # wired-port-profile wired- port`
		`(AP)(wired-port-profile "wired-port")# switchport-mode access`
		`(AP)(wired-port-profile "wired-port")# allowed-vlan all`
		`(AP)(wired-port-profile "wired-port")# native-vlan 20`
		`(AP)(wired-port-profile "wired-port")# no shutdown`
		`(AP)(wired-port-profile "wired-port")# access-rule-name wired-port`
		`(AP)(wired-port-profile "wired-port")# type employee`
		`(AP)(wired-port-profile "wired-port")# auth-server server1`
		`(AP)(wired-port-profile "wired-port")# auth-server server2`
		`(AP)(wired-port-profile "wired-port")# dot1x`
		`(AP)(wired-port-profile "wired-port")# exit`
		`(AP)(config)# enet1-port-profile wired-port`
		Configure a wireless SSID to operate in Centralized, L2 mode and associate VLAN 20 to the WLAN SSID profile.
		`(AP)(config) # wlan ssid-profile wireless- ssid`
		`(AP)(SSID Profile "wireless-ssid")# enable`
		`(AP)(SSID Profile "wireless-ssid")# type employee`
		`(AP)(SSID Profile "wireless-ssid")# essid wireless-ssid`
		`(AP)(SSID Profile "wireless-ssid")# opmode wpa2-aes`
		`(AP)(SSID Profile "wireless-ssid")# vlan 20`
		`(AP)(SSID Profile "wireless-ssid")# auth- server server1`
		`(AP)(SSID Profile "wireless-ssid")# auth- server server2`
		`(AP)(SSID Profile "wireless-ssid")# auth- survivability`
			See Configuring a Wired Profile (Page 125) and Wireless Network Profiles (Page 95)

7	Create access rule for wired and wireless authentication.	**For wired profile:**
		`(AP)(config)# wlan access-rule wired-port`
		`(AP)(Access Rule "wired-port")# rule any any match any any any permit`
		For WLAN SSID employee roles:
		`(AP)(config)# wlan access-rule wireless- ssid`
		`(AP)(Access Rule "wireless-ssid")# rule any any match any any any permit`
			See Configuring ACL Rules for Network Services (Page 220)

NOTE: Ensure that you execute the **commit apply** command in the SCALANCE W CLI before saving the configuration and propagating changes across the AP cluster			

AP-Connected Switch Configuration

Client VLANs defined in this example must be opened on the upstream switches in multiple AP deployments, as client traffic from the slave to the master is tagged with the client VLAN.

Datacenter Configuration

For information on controller configuration, see Configuring a Controller for AP-VPN Operations (Page 290). The following GRE configuration is required on the controller:

```
(host)(config)# interface tunnel <Number>

(host)(config-tunnel)# description <Description>

(host)(config-tunnel)# tunnel mode gre <ID>

(host)(config-tunnel)# tunnel source <controller-IP>

(host)(config-tunnel)# tunnel destination <AP-IP> (host)(config-tunnel)# trusted

(host)(config-tunnel)# tunnel vlan <allowed-VLAN>
```

Adaptive Radio Management 22

22.1 ARM Overview

ARM is an RF management technology that optimizes WLAN performance even in networks with the highest traffic by dynamically and intelligently choosing the best 802.11 channel and transmitting power for each AP in its current RF environment. ARM works with all standard clients, across all operating systems, while remaining in compliance with the IEEE 802.11 standards. It does not require any proprietary client software to achieve its performance goals. ARM ensures low-latency roaming, consistently high performance, and maximum client compatibility in a multi-channel environment. By ensuring a fair distribution of the available Wi-Fi bandwidth to mobile devices, ARM ensures that data, voice, and video applications have sufficient network resources at all times. ARM allows mixed 802.11a, 802.11b, 802.11g, 802.11n, and 802.11ac client types to interoperate at the highest performance levels.

Channel or Power Assignment

The channel or power assignment feature automatically assigns channel and power settings for all the APs in the network according to changes in the RF environment. This feature automates many setup tasks during network installation and the ongoing operations when RF conditions change.

Voice Aware Scanning

The Voice Aware scanning feature prevents an AP supporting an active voice call from scanning for other channels in the RF spectrum and allows the AP to resume scanning when there are no active voice calls. This significantly improves the voice quality when a call is in progress and simultaneously delivers the automated RF management functions. By default, this feature is enabled.

Load Aware Scanning

The Load Aware Scanning feature dynamically adjusts scanning function to maintain uninterrupted data transfer on resource-intensive systems when the network traffic exceeds a predefined threshold. The APs resume complete monitoring scans when the traffic drops to the normal levels. By default, this feature is enabled.

Monitoring the Network with ARM

When ARM is enabled, an AP dynamically scans all 802.11 channels within its 802.11 regulatory domain at regular intervals and sends reports to a virtual controller on WLAN network coverage, interference, and intrusion detection.

ARM Metrics

ARM computes coverage and interference metrics for each valid channel and chooses the best performing channel and transmit power settings for each AP RF environment. Each AP gathers other metrics on its ARM-assigned channel to provide a snapshot of the current RF health state.

22.2 Configuring ARM Features on an AP

22.2.1 Band Steering

The band steering feature assigns the dual-band capable clients to the 5 GHz band on dual-band APs. This feature reduces co-channel interference and increases available bandwidth for dual-band clients, because there are more channels on the 5 GHz band than that on the 2.4 GHz band. You can configure band steering parameters through the SCALANCE W UI or the CLI.

In the SCALANCE W UI

To configure band steering:

1. In the **RF > ARM > Show advanced options** tab view, configure the following parameters:

Parameter	Description
Prefer 5 GHz	Select this option to use band steering in the 5 GHz mode. On selecting this, the AP steers the client to the 5 GHz band (if the client is 5 GHz-capable), but allows the client connection on the 2.4 GHz band if the client persistently attempts for 2.4 GHz association.
Force 5 GHz	Select this option to enforce 5 GHz band steering mode on the APs.
Balance Bands	Select this option to allow the AP to balance the clients across the two radios to best utilize the available 2.4 GHz bandwidth. This feature takes into account the fact that the 5 GHz band has more channels than the 2.4 GHz band, and that the 5 GHz channels operate in 40 MHz, while the 2.4 GHz band operates in 20 MHz.
Disabled	Select this option if you want to allow the clients to select the band to use.

2. Click **OK.**

In the CLI

To configure band steering:

```
(AP)(config)# arm
```

```
(AP)(ARM)# band-steering-mode {<Prefer 5 GHz>| <Force 5 GHz>|<Balance
Bands>|<Disabled>}
```

22.2.2 Airtime Fairness Mode

The airtime fairness feature provides equal access to all clients on the wireless medium, regardless of client type, capability, or operating system, thus delivering uniform performance to all clients. This feature prevents the clients from monopolizing resources. You can configure airtime fairness mode parameters through the SCALANCE W UI or the CLI.

In the SCALANCE W UI

To configure band steering:

1. For **Airtime fairness mode** configuration, specify any of the following values under the **RF > ARM > Show advanced options** tab:

Parameter	Description
Default Access	Select this option to provide access based on client requests. When **Air Time Fairness** is set to default access, per-user and per-SSID bandwidth limits are not enforced.
Fair Access	Select this option to allocate Airtime evenly across all the clients.
Preferred Access	Select this option to set a preference where 802.11n clients are assigned more airtime than 802.11a/11g. The 802.11a/11g clients get more airtime than 802.11b. The ratio is 16:4:1.

2. Click **OK**.

In the CLI

```
(AP)(config)# arm
```

```
(AP)(ARM)# air-time-fairness-mode {<Default Access>| <Fair Access> | <Preferred
Access>
```

22.2.3 Client Match

The ARM client match feature continually monitors a client's RF neighborhood to provide ongoing client band steering and load balancing, and enhanced AP reassignment for roaming mobile clients. This feature supersedes the legacy band steering and spectrum load balancing features, which unlike client match, do not trigger AP changes for clients already associated to an AP. In addition to this, the Client Match feature provides the smartphone handoff assist function which helps smartphones to switch between 3G and 4G networks when the Wi-Fi connectivity is poor. The AP monitors the RSSI of the smartphone and checks if it remains under the threshold connectivity strength for a certain duration and deauthenticates the client.

Note

Legacy 802.11a, 802.11b, or 802.11g access points do not support the client match feature. When client match is enabled on 802.11n-capable access points, the client match feature overrides any settings configured for the legacy band steering, station handoff assist, or load balancing feature. 802.11ac-capable access points do not support the legacy band steering, station handoff assist, or load balancing settings; so these access points must be managed using client match.

When the client match feature is enabled on an AP, the AP measures the RF health of its associated clients. In the current release, the client match feature is supported only within an AP cluster. If any of the following trigger conditions is met, clients are moved from one AP to another for better performance and client experience:

- Dynamic Load Balancing—Client match balances clients across APs on different channels, based on the client load on the APs and the SNR levels the client detects from an underutilized AP. If an AP radio can support additional clients, the AP will participate in client match load balancing and clients can be directed to that AP radio, subject to the predefined SNR thresholds. For better load balancing, clients are steered from busy channels to idle channels.
- Sticky Clients—The client match feature also helps mobile clients that tend to stay associated to an AP despite low signal levels. APs using client match continually monitor the client's RSSI as the client roams between APs, and move the client to an AP when a better radio match can be found. This prevents mobile clients from remaining associated to the APs with less than ideal RSSI, which can cause poor connectivity and reduce performance for other clients associated with that AP.
- Band Steering—APs using the client match feature monitor the RSSI for clients that advertise a dual- band capability. If a client is currently associated to a 2.4 GHz radio and the AP detects that the client has a good RSSI from the 5 GHz radio, the AP steers the client to the 5 GHz radio, as long as the 5 GHz RSSI is not significantly worse than the 2.4 GHz RSSI, and the AP retains a suitable distribution of clients on each of its radios.
- Channel Utilization—Based on the percentage of channel utilization, clients are steered from a busy channel to an idle channel.
- Client Capability Match—Based on the client capability match, clients are steered to appropriate channel, for example, HT20, HT40, or VHT80

Note

The spectrum load balancing is integrated with the client match feature. Client match allows the APs in a cluster to be divided into several logical AP RF neighborhood called domains, which share the same clients. The network determines the distribution of clients and balances client load across channels, regardless of whether the AP is responding to the probe requests of wireless clients.

You can configure client match parameters in the SCALANCE W UI or the CLI. When client match is enabled, the dashboard in the main window displays the **Client Match** link on selecting an AP in the **Access Points** tab or a client in the **Clients** tab. Clicking this link provides a graphical representation of radio map view of an AP and the client distribution on an AP radio. For more information, see Client Match (Page 66).

In the SCALANCE W UI

To configure band steering:

1. For client match configuration, specify the following parameters in the **RF > ARM > Show advanced options** tab:

Parameter	Description
Client match	Select **Enabled** to enable the **Client match** feature on APs. When enabled, client count will be balanced among all the channels in the same band. For more information, see ARM Overview (Page 321). By default, the client match feature is disabled. **NOTE:** When client match is enabled, ensure that Scanning is enabled.
CM calculating interval	Specify a value for calculating the interval of Client match. The value specified for **CM calculating interval** determines the interval at which client match is calculated. The interval is specified in seconds and the default value is 30 seconds. You can specify a value within the range of 10–600.
CM neighbor matching %	Specify a value for **CM neighbor matching %**. This number takes into account the least similarity percentage to be considered as in the same virtual RF neighborhood of client match. You can specify a percentage value within the range of 20–100. The default value is 75%.
CM threshold	Specify a value for **CM threshold**. This number takes acceptance client count difference among all the channels of client match into account. When the client load on an AP reaches or exceeds the threshold, client match is enabled on that AP. You can specify a value within range of 1–255. The default value is 2.
SLB mode	Select a mode from the **SLB mode** drop-down list. The SLB mode determines the balancing strategy for client match. The following options are available: • Channel • Radio • Channel + Radio

2. Click **OK.**

In the CLI

```
(AP)(config)# arm

(AP)(ARM)# client-match calc-interval <seconds>

(AP)(ARM)# client-match calc-threshold <threshold>

(AP)(ARM)# client-match nb-matching <percentage>

(AP)(ARM)# client-match slb-mode 1
```

22.2.4 Access Point Control

You can configure access point control parameters through the SCALANCE W UI or the CLI.

In the SCALANCE W UI

1. For **Access Point Control**, specify the following parameters in the **RF > ARM > Show advanced options** tab:

Parameter	Description
Customize Valid Channels	Select this check box to customize valid channels for 2.4 GHz and 5 GHz. By default, the AP uses valid channels as defined by the Country Code (regulatory domain). On selecting the **Customize Valid Channels** check box, a list of valid channels for both 2.4 GHz and 5 GHz are displayed. The valid channel customization feature is disabled by default.,
Minimum Transmit Power	Specify the minimum transmission power. The value specified for **Minimum Transmit Power** indicates the minimum EIRP that can range from 3 dBm to 33 dBm in 3 dBm increments. If the minimum transmission EIRP setting configured on an AP is not supported by the AP model, this value is reduced to the highest supported power setting. The default value for minimum transmit power is 18 dBm.
Maximum Transmit Power	Specify the maximum transmission power. The value specified for **Maximum Transmit Power** indicates the maximum EIRP that can range from 3 dBm to 33 dBm in 3 dBm increments. If the maximum transmission EIRP configured on an AP is not supported by the AP model, the value is reduced to the highest supported power setting. The default value for maximum transmit power is 127 dBm.
Client aware	When **Enabled**, ARM does not change channels for the APs with active clients, except for high-priority events such as RADAR or excessive noise. This feature must be enabled in most deployments for a stable WLAN. If the Client Aware mode is **Disabled**, the AP may change to a more optimal channel, that may disrupt the current client traffic for a while. The Client aware option is **Enabled** by default. **NOTE:** When Client aware is disabled, channels can be changed even when the clients are active on a BSSID.
Scanning	Select **Enabled** so that the AP dynamically scans all 802.11 channels within its 802.11 regulatory domain at regular intervals and reports to the AP. This scanning report includes WLAN coverage, interference, and intrusion detection data. **NOTE:** For client match configuration, ensure that scanning is enabled.
Wide Channel Bands	Select a band to allow the APs to be placed in 40 MHz (wide band) channels. The **Wide Channel Bands** allows administrators to configure 40 MHz channels in the 2.4 GHz and 5 GHz bands. 40 MHz channels are two 20 MHz adjacent channels that are bonded together. A 40 MHz channel effectively doubles the frequency bandwidth available for data transmission.
80 MHz Support	Enables or disables the use of 80 MHz channels on APs. This feature allows ARM to assign 80 MHz channels on APs with 5 GHz radios, which support a VHT. This setting is enabled by default. **NOTE:** Only the APs that support 802.11ac can be configured with 80 MHz channels

2. Reboot the AP.
3. Click **OK.**

In the CLI

To configure access point control parameters:

```
(AP)(config)# arm
```

```
(AP)(ARM)# a-channels <5GHz-channels>
(AP)(ARM)# min-tx-power <power>
(AP)(ARM)# max-tx-power <power>
(AP)(ARM)# client-aware
(AP)(ARM)# wide-bands {<5GHz>|<2GHz>|<All>|<None>}
(AP)(ARM)# scanning
(AP)(ARM)# 80mhz-support
```

22.2.5 Verifying ARM Configuration

To view ARM configuration:

```
(AP)# show arm config
Minimum Transmit Power 18
Maximum Transmit Power 127
Band Steering Mode :prefer-5ghz Client Aware :enable
Scanning :enable
Wide Channel Bands :5ghz
80Mhz Support :enable
Air Time Fairness Mode :fair-access Client Match :disable
CM NB Matching Percent 75
CM Calculating Interval 30
CM SLB Threshold 2
CM SLB Balancing Mode :channel based CM max client match req 5
CM max adoption 5
Custom Channels :No
2.4 GHz Channels
----------------
Channel Status
------- ------
1       enable
2       disable
3       disable
4       disable
5       disable
6       enable
```

```
7       disable
8       disable
9       disable
10      disable
11      enable
12      disable
13      disable
1+      enable
2+      disable
3+      disable
4+      disable
5+      disable
6+      disable
7+      enable
5.0 GHz Channels
----------------
Channel Status
------- ------
36      enable
40      enable
44      enable
48      enable
52      enable
56      enable
60      enable
64      enable
149     enable
153     enable
157     enable
161     enable
165     enable
36+     enable
44+     enable
52+     disable
60+     disable
```

```
149+    enable

157+    enable

36E     enable

52E     enable

149E    enable
```

22.2.6 Client Match for Access Points in a Zone

When Client match is enabled, the decision to move a client from the home AP to a target AP is made at the radio level. However, this proves inefficient when client match is enabled on an AP or SSID operating in a specific zone, it could result in the client being moved to a target AP that does not have the same zone specific SSID as the home AP.

The decision to move a client from a home AP to a target AP will be made at the SSID level instead of the radio level, by adding the SSID name to the client match radio database. Client Match will check if the same SSID (zone specific SSID on Home AP) is available on the target AP before it moves the client. This ensures that client match works as expected when zone settings are configured on the AP.

Additionally, the maximum clients threshold and the current associated client number of the SSID is added to the client match radio database to prevent the clients from being moved to an SSID whose associated client number is already reached its limit.

You can use the following commands to view the SSID details stored in client match:

The **show ap client-match-ssid-table** command displays the client match SSID table for the current AP and its neighboring APs.

The **show ap client-match-ssid-table radio-mac <mac>** command displays the client match SSID table for a specific AP denoted by its mac address.

22.3 Configuring Radio Settings

The current Radio profile is displayed as **Default**. The default profile cannot be deleted. You can configure 2.4 GHz and 5 GHz radio settings for an AP either using the SCALANCE W UI or the CLI.

In the SCALANCE W UI

To configure radio settings:

1. Click the **RF** link located directly above the Search bar of the SCALANCE W main window.
2. Click **Show advanced options**. The advanced options are displayed.
3. Click the **Radio** tab.

4. Under the channel 2.4.GHz or 5 GHz, or both, configure the following parameters:

Parameter	Description
Zone	Enter the zone name for configuration. The same zone name can be configured on a 2.4 GHz and a 5 GHz radio profile. However, the same zone name cannot be configured on two2.4 GHz or two 5 GHz profiles.
Legacy only	Select **Enabled** to run the radio in non-802.11n mode. This option is set to **Disabled** by default.
802.11d / 802.11h	Select **Enabled** to allow the radio to advertise its 802.11d (Country Information) and 802.11h TPC capabilities. This option is set to **Disabled** by default.
Beacon interval	Enter the Beacon period for the AP in milliseconds. This indicates how often the802.11 beacon management frames are transmitted by the access point. You can specify a value within the range of 60-500. The default value is 100 milliseconds.
Interference immunity level	Select to increase the immunity level to improve performance in high-interference environments The default immunity level is 2. • **Level 0**—no ANI adaptation. • **Level 1**—Noise immunity only. This level enables power-based packet detection by controlling the amount of power increase that makes a radio aware that it has received a packet. • **Level 2**—Noise and spur immunity. This level also controls the detection of OFDM packets, and is the default setting for the Noise Immunity feature. • **Level 3**—Level 2 settings and weak OFDM immunity. This level minimizes false detects on the radio due to interference, but may also reduce radio sensitivity. This level is recommended for environments with a high-level of interference related to 2.4 GHz appliances such as cordless phones. • **Level 4**—Level 3 settings, and FIR immunity. At this level, the AP adjusts its sensitivity to in-band power, which can improve performance in environments with high and constant levels of noise interference. • **Level 5**—The AP completely disables PHY error reporting, improving performance by eliminating the time the AP would spend on PHY processing. **NOTE:** Increasing the immunity level makes the AP to lose a small amount of range.
Background spectrum monitoring	Select **Enabled** to allow the APs in access mode to continue with normal access service to clients, while performing additional function of monitoring RF interference (from both neighboring APs and non Wi-Fi sources such as, microwaves and cordless phones) on the channel they are currently serving clients.
Very high throughput	Ensure that this check box is selected to enable VHT on 802.11ac devices with 5 GHz radio. If VHT is enabled for the 5 GHz radio profile on an AP, it is automatically enabled for all SSIDs configured on an AP. By default, VHT is enabled on all SSIDs. If you want the 802.11ac APs to function as 802.11n APs, clear the check box to disable VHT on these devices.

Parameter	Description
Smart Antenna	This value is **Disabled** by default. Select **Enabled** to allow smart antenna polarization on the access points support the smart antenna feature. This feature helps optimize the selection of antenna polarization values based on data collected from the training of polarization pattern combinations. This feature identifies the clients most likely to benefit from smart antenna polarization, based on the average RSSI of the received frames and the number of streams. This feature uses frame-based antenna training, which allows the AP to cycle through training combinations and collect statistics without causing any impact on the client. At the end of the training sequence, the AP selects the best antenna polarization based on these collected statistics. The smart antenna feature does not support optimized antenna polarization for clients using Single-User or Multi-User transmit beamforming, and will use default polarization values for these clients
ARM/WIDS Override	By default, WIDS protection is on dynamic mode. If an AP is heavily loaded with client traffic and the CPU utilization exceeds the threshold limit, the WIDS processing is suspended. This causes more CPU cycles to handle the client traffic. When the CPU utilization is within the the threshold limit, the WIDS processing is resumed. When **ARM/WIDS Override** is off, the AP will always process frames for WIDS purposes even when it is heavily loaded with client traffic. When **ARM/WIDS Override** is on, the AP will stop process frames for WIDS purposes regardless of whether the AP is heavily loaded or not. The WIDS functionality will not take effect.

5. Click **OK.**

In the CLI

To configure 2.4 GHz radio settings:

```
(AP)(config)# rf dot11g-radio-profile

(AP)(RF dot11g Radio Profile)# beacon-interval <milliseconds>

(AP)(RF dot11g Radio Profile)# legacy-mode

(AP)(RF dot11g Radio Profile)# spectrum-monitor

(AP)(RF dot11g Radio Profile)# dot11h

(AP)(RF dot11g Radio Profile)# interference-immunity <level>

(AP)(RF dot11g Radio Profile)# csa-count <count>

(AP)(RF dot11g Radio Profile)# max-distance <count>

(AP)(RF dot11g Radio Profile)# max-tx-power <db>

(AP)(RF dot11g Radio Profile)# min-tx-power <db>

(AP)(RF dot11g Radio Profile)# smart-antenna
```

To configure 5 GHz radio settings:

```
(AP)(config)# rf dot11a-radio-profile

(AP)(RF dot11a Radio Profile)# beacon-interval <milliseconds>

(AP)(RF dot11a Radio Profile)# legacy-mode

(AP)(RF dot11a Radio Profile)# spectrum-monitor

(AP)(RF dot11a Radio Profile)# spectrum-band <type>
```

```
(AP)(RF dot11a Radio Profile)# dot11h
(AP)(RF dot11a Radio Profile)# interference-immunity <level>
(AP)(RF dot11a Radio Profile)# max-distance <count>
(AP)(RF dot11a Radio Profile)# max-tx-power <db>
(AP)(RF dot11a Radio Profile)# min-tx-power <db>
(AP)(RF dot11a Radio Profile)# smart-antenna
(AP)(RF dot11a Radio Profile)# csa-count <count>
```

To disable VHT on a 5 GHz radio profile:

```
(AP)(config)# rf dot11a-radio-profile
(AP)(RF dot11a Radio Profile)# very-high-throughput-disable
```

To view the radio configuration:

```
(AP)# show radio config


2.4 GHz:
Legacy Mode:enable Beacon Interval:100 802.11d/802.11h:enable
Interference Immunity Level:2 Channel Switch Announcement Count:0 MAX Distance:600
Channel Reuse Type:disable Channel Reuse Threshold:0
Background Spectrum Monitor:disable


5.0 GHz:
Legacy Mode:enable Beacon Interval:100 802.11d/802.11h:enable
Interference Immunity Level:2 Channel Switch Announcement Count:2 MAX Distance:600
Channel Reuse Type:disable Channel Reuse Threshold:0
Background Spectrum Monitor:disable Standalone Spectrum Band:5ghz-upper
```

Configuring Cell Size Reduction using the CLI

The Cell Size Reduction feature allows you to manage dense deployments and to increase overall system performance and capacity by shrinking an APs receive coverage area, thereby minimizing co-channel interference and optimizing channel reuse.

The default 0 dB reduction allows the radio to retain its current default Rx sensitivity value.

Values from 1 dB–55 dB reduce the power level that the radio can hear by that amount. If you configure this feature to use a non-default value, you must also reduce the radio’s transmission power to match its new received (Rx) power level. Failure to match a device’s Tx power level to its Rx power level can result in a configuration that allows the radio to send messages to a device that it cannot hear.

To configure Cell Size Reduction for 2.4 GHz radio profile in the CLI:

```
(AP)(config)# rf dot11g-radio-profile
```

```
(AP)(RF dot11g Radio Profile)# cell-size-reduction <reduction>
```

To configure Cell Size Reduction for 5 GHz radio profile in the CLI:

```
(AP)(config)# rf dot11a-radio-profile

(AP)(RF dot11a Radio Profile)# cell-size-reduction <reduction>
```

ARM Channel Selection using the CLI

APs can search for a new environment in a short span of time, so that the ARM is triggered to perform frequent scanning and selection of a valid channel for transmission.

By default, the ARM is triggered to scan all the channels every 10 seconds, and select the best channel for transmission. But when the AP is in a new environment, ARM is triggered to perform frequent scanning of the non-DFS channels every 200 milliseconds, and select the best available channel for transmission. The **ap- frequent-scan** command is introduced in the CLI to enable the APs to trigger frequent scanning of transmission signals on a radio profile.

Note

Wireless connection is affected for a few seconds when the frequent scanning of non-DFS channels is ongoing. The connection is re-established after the ARM selects a valid channel. Typically, a frequent scanning session lasts for less than 10 seconds.

Perform the following checks before scanning:

- The DFS channels must be skipped (this is done to avoid delays in scanning).
- The AP must be on stand-alone mode.
- The **client-aware** parameter must be disabled in the ARM profile.

In the CLI

The following example triggers ARM scanning on a 2.4 GHz frequency band radio profile:

```
(AP)# ap-frequent-scan 2.4
```

To verify the status of ARM scanning:

```
(AP)# show ap debug am-config
```

DPI and Application Visibility 23

23.1 DPI

AppRF is Aruba's custom-built Layer 7 firewall capability. It consists of an onboard DPI and a cloud-based Web Policy Enforcement service that allows creating firewall policies based on types of application. The WPE capabilities require the AP to have a WPE subscription.

APs with DPI capability analyze data packets to identify applications in use and allow you to create access rules to determine client access to applications, application categories, web categories, and website URLs based on web reputation. You can also define traffic-shaping policies such as bandwidth control and QoS per application for client roles. For example, you can block bandwidth-monopolizing applications on a guest role within an enterprise.

The AppRF feature provides application visibility for analyzing client traffic flow. APs support the power of both in-device packet flow identification and dynamically updated cloud-based web categorization.

23.2 Enabling Application Visibility

Enabling AppRF visibility allows you to view the AppRF statistics for an AP or the clients associated with an AP. Full URL visibility for HTTP sessions fed to ALE is exposed as northbound APIs which can be consumed by URL analytical engines for advanced client URL data mining and analytics.

You can enable AppRF visibility by using the SCALANCE W UI or the CLI.

In the SCALANCE W UI

To enable AppRF:

1. Navigate to **System > General**.
2. Select **All** from the **AppRF visibility** drop-down list to view both application and web categories charts or either **App** or **WebCC** to view their DPI graphs separately.
3. Click **OK**.

In the CLI

To enable AppRF visibility:

```
(AP)(config)# dpi [app|webcc]
```

23.3 Application Visibility

The AppRF graphs are based on DPI application and Web Policy Enforcement service, which provide application traffic summary for the client devices associated with an AP. The **AppRF** link above the activity panel of the dashboard is displayed only if **AppRF visibility** is enabled in the **System** window.

The AppRF dashboard presents four different graph areas with data graphs on all client traffic and content filters based on App Category, Web Category, and Web Reputation. Click each category to view the real-time client traffic data or usage trend in the last 15 minutes or 1 minute.

The **permit** and **deny** monitoring tabs in the All Traffic and Web Content sections provide enforcement visibility support.

- **Permit** represents the allowed or permitted traffic on the AP.
- **Deny** represents all the blocked URLs and traffic .

Application Categories Chart

The application categories chart displays details on the client traffic towards the application categories. By clicking the rectangle area, you can view the graphs and toggle between the chart and list views.

Applications Chart

The applications chart displays details on the client traffic towards the applications. By clicking the rectangular area, you can view the graphs and toggle between the chart and list views

Web Categories Charts

The web categories chart displays details about the client traffic to the web categories. By clicking the rectangle area, you can view the graphs and toggle between the chart and list views.

Web Reputation Charts

The web reputation chart displays details about the client traffic to the URLs that are assigned security ratings. By clicking in the rectangle area, you can view the graphs and toggle between the chart and list views.

23.4 Enabling URL Visibility

Enabling URL visibility allows the AP to extract the full URL information of the HTTP and HTTPS sessions and periodically log them on the ALE server. Full URL visibility for HTTP sessions fed to ALE are exposed as Northbound APIs, and are used by URL analytical engines for advanced client URL data mining and analysis.

You can enable URL visibility by using the SCALANCE W UI or the CLI:

In the SCALANCE W UI

To enable URL visibility:

1. Navigate to **System > General**.
2. Select **Enabled** from the **URL visibility** drop-down list.
3. Click **OK**.

In the CLI

To enable URL visibility:

```
(AP)(config)# url-visibility

(AP)(config)# end

(AP)# commit apply
```

23.5 Configuring ACL Rules for Application and Application Categories

This section describes the procedure for configuring access rules based on application and application categories. The Application and Application rules utilize the onboard DPI engine.

- For information on configuring access rules to control access to network services, see Configuring ACL Rules for Network Services (Page 220).
- For information on configuring access rules based on web categories and web reputation, see Configuring Web Policy Enforcement Service (Page 341).

In the SCALANCE W UI

To configure ACL rules for a user role:

1. Navigate to the **Security > Roles** tab. The **Roles** tab contents are displayed. You can also configure access rules for a wired or wireless client by using:
   – The WLAN wizard (**Network > WLAN SSID > Edit > Edit WLAN > Access**) or
   – The Wired profile (**More > Wired > Edit > Edit Wired Network > Access**) window.
2. Select the role for which you want to configure the access rules.
3. In the **Access rules** section, click **New** to add a new rule. The **New Rule** window is displayed.
4. Ensure that the rule type is set to **Access Control**.
5. To configure access to applications or application category, select a service category from the following list:
   – Application
   – Application category

6. Based on the selected service category, configure the following parameters:

Service Category	Description
Application	Select the applications to which you want to allow or deny access.
Application category	Select any of the following application categories to which you want to allow or deny access: • antivirus • authentication • cloud-file-storage • collaboration • encrypted • enterprise-apps • gaming • im-file-transfer • instant-messaging • mail-protocols • mobile-app-store • network-service • peer-to-peer • social-networking • standard • streaming • thin-client • tunneling • unified-communications • web • Webmail
Application Throttling	Application throttling allows you to set a bandwidth limit for an application, application category, web category, or for sites based on their web reputation. For example, you can limit the bandwidth rate for video streaming applications such as YouTube or Netflix, or assign a low bandwidth to high-risk sites. If your AP model does not support configuring access rules based on application or application category, you can create a rule based on web category or website reputation and assign bandwidth rates. To specify a bandwidth limit: 1. Select the **Application Throttling** check box. 2. Specify the downstream and upstream rates in Kbps.

Service Category	Description
Action	Select any of following actions: • Select **Allow** to allow access to users based on the access rule. • Select **Deny** to deny access to users based on the access rule. • Select **Destination-NAT** to allow changes to destination IP address. • Select **Source-NAT** to allow changes to the source IP address. • The destination-NAT and source-NAT actions apply only to the network services rules.
Destination	Select a destination option for the access rules for network services, applications, and application categories. You can allow or deny access to any the following destinations based on your requirements. • **to all destinations**—Access is allowed or denied to all destinations. • **to a particular server**—Access is allowed or denied to a particular server. After selecting this option, specify the IP address of the destination server. • **except to a particular server**—Access is allowed or denied to servers other than the specified server. After selecting this option, specify the IP address of the destination server. • **to a network**—Access is allowed or denied to a network. After selecting this option, specify the IP address and netmask for the destination network. • **except to a network**—Access is allowed or denied to networks other than the specified network. After selecting this option, specify the IP address and netmask of the destination network. • **to domain name**—Access is allowed or denied to the specified domains. After selecting this option, specify the domain name in the **Domain Name** text box. • **to master IP**—Access is allowed or denied to the master IP address.
Log	Select this check box to create a log entry when this rule is triggered. SCALANCE W supports firewall-based logging function. Firewall logs on the APs are generated as security logs.
Blacklist	Select the **Blacklist** check box to blacklist the client when this rule is triggered. The blacklisting lasts for the duration specified in **Auth failure blacklist time** on the Blacklisting tab of the **Security** window. For more information, see Blacklisting Clients (Page 213).
Disable scanning	Select **Disable scanning** check box to disable ARM scanning when this rule is triggered. The selection of the **Disable scanning** applies only if ARM scanning is enabled. For more information, see Configuring Radio Settings (Page 330).
DSCP tag	Select the **DSCP tag** check box to specify a DSCP value to prioritize traffic when this rule is triggered. Specify a value within the range of 0–63. To assign a higher priority, specify a higher value.
802.1p priority	Select the **802.1p priority** check box to specify an 802.1p priority. Specify a value between 0 and 7. To assign a higher priority, specify a higher value.

7. Click **OK** and then click **Finish**.

In the CLI

To configure access rules:

```
(AP)(config)# wlan access-rule <access-rule-name>

(AP)(Access Rule <Name>)#rule <dest> <mask> <match/invert> {app <app> {permit|deny}

|appcategory <appgrp>}[<option1....option9>]
```

Example

The following CLI example shows hoe to configure employee access rules:

```
(AP)(config)# wlan access-rule employee

(AP)(Access Rule "employee")# rule any any match app uoutube permit throttle-
downstream 256 throttle-up 256

(AP)(Access Rule "employee")# rule any any match appcategory collaboration permit
```

23.6 Configuring Web Policy Enforcement Service

You can configure the WPE service on an AP to block certain categories of websites based on your organization specifications by defining ACL rules by using the SCALANCE W UI or the CLI.

In the SCALANCE W UI

To configure WPE service:

1. Navigate to **Security > Roles**.
2. Select any WLAN SSID or wired profile role, and click **New** in the Access Rules section.
3. Select the rule type as **Access Control**.
4. To set an access policy based on the web category:
   - Under **Service**, select **Web category** and expand the **Web categories** drop-down list.
   - Select the categories to which you want to deny or allow access. You can also search for a web category and select the required option.
   - From the **Action** drop-down list, select **Allow** or **Deny** as required.
   - Click **OK**
5. To filter access based on the security ratings of the website

   Select **Web reputation** under **Service**.

   Move the slider to the required security rating level. Move the slider to select a specific web reputation value to deny access to websites with a reputation value lower than or equal to the configured value or to permit access to websites with a reputation value higher than or equal to the configured value. The following options are available:

   - Trustworthy—These are well known sites with strong security practices and may not expose the user to security risks. There is a very low probability that the user will be exposed to malicious links or payloads.
   - Low risk—These are benign sites and may not expose the user to security risks. There is a low probability that the user will be exposed to malicious links or payloads.
   - Moderate risk—These are generally benign sites, but may pose a security risk. There is some probability that the user will be exposed to malicious links or payloads.
   - Suspicious—These are suspicious sites. There is a higher than average probability that the user will be exposed to malicious links or payloads.
   - High risk—These are high-risk sites. There is a high probability that the user will be exposed to malicious links or payloads.

   From the **Action** drop-down list, select **Allow** or **Deny** as required.

   Note

   For a complete list of categories and information about each of these categories, visit the BrightCloud® Security Services web page at http://www.brightcloud.com/tools/change-request-url-ip.php.

6. To set a bandwidth limit based on web category or web reputation score, select **Application Throttling** check box and specify the downstream and upstream rates in Kbps.

For example, you can set a higher bandwidth for trusted sites and a low bandwidth rate for high-risk sites.

7. If required, select the following check boxes:
   - Log
   - Blacklist
   - Disable scanning
   - DSCP tag
   - 802.1p priority
8. Click **OK** on the **Roles** tab to save the changes to the role for which you defined ACL rules.

In the CLI

To control access based on web categories and security ratings:

```
(AP)(config)# wlan access-rule <access_rule>

(AP)(Access Rule "<access-rule>")# rule <dest> <mask> <match> webcategory <webgrp>

{permit | deny}[<option1....option9>]

(AP)(Access Rule "<access-rule>")# rule <dest> <mask> <match> webreputation <webrep>

{permit | deny}[<option1....option9>]
```

Example

The following CLI example shows how to set access rules based on the web category and the web reputation:

```
(AP)(config)# wlan access-rule URLFilter

(AP)(Access Rule "URLFilter")# rule any any match webcategory gambling deny

(AP)(Access Rule "URLFilter")# rule any any match webcategory training-and-tools
permit

(AP)(Access Rule "URLFilter")# rule any any match webreputation suspicious-sites deny
```

Voice and Video 24

This chapter explains the steps required to configure voice and video services on an AP for VoIP devices, SIP, SVP, H323, SCCP, Vocera, and Alcatel NOE phones, clients running Microsoft OCS, and Apple devices running the Facetime application.

This section includes the following topics:

- Wi-Fi Multimedia Traffic Management (Page 343)
- Media Classification for Voice and Video Calls (Page 347)
- Enabling Enhanced Voice Call Tracking (Page 349)

24.1 WMM Traffic Management

WMM is a WFA specification based on the IEEE 802.11e wireless QoS standard. WMM works with 802.11a, 802.11b, 802.11g, and 802.11n physical layer standards.

WMM supports the following ACs:

- Voice
- Video
- Best effort
- Background

The following table shows the mapping of the WMM access categories to 802.1p priority values. The 802.1p priority value is contained in a two-byte QoS control field in the WMM data frame.

Table 24- 1 WMM AC to 802.1p Priority Mapping

802.1p Priority	WMM Access Category
1	Background
2	
0	Best effort
3	
4	Video
5	
6	Voice
7	

In a non-WMM or hybrid environment, where some clients are not WMM-capable, you can configure an SSID with higher values for best effort and voice ACs, to allocate a higher bandwidth to clients transmitting best effort and voice traffic.

Configuring WMM for Wireless Clients

You can configure WMM for wireless clients by using the SCALANCE W UI or the CLI.

In the SCALANCE W UI

To configure the WMM for wireless clients:

1. Navigate to the WLAN wizard.
   – Click **Networks > New** or
   – Click **Networks**, and select the **WLAN SSID > edit**.
2. Click **Show advanced options** under **WLAN Settings**.
3. Specify a percentage value for the following WMM access categories in the corresponding **Share** text box. You can allocate a higher bandwidth for voice and video traffic than that for other types of traffic based on the network profile.
   – **Background WMM**—Allocates bandwidth for background traffic such as file downloads or print jobs.
   – **Best effort WMM**—Allocates bandwidth or best effort traffic such as traffic from legacy devices or traffic from applications or devices that do not support QoS.
   – **Video WMM**—Allocates bandwidth for video traffic generated from video streaming.
   – **Voice WMM**—Allocates bandwidth for voice traffic generated from the incoming and outgoing voice communication.
4. Click **Next** and complete the configuration as required

In the CLI

Configuring WMM for wireless clients:

```
(AP)(config)# wlan ssid-profile <name>

(AP)(SSID Profile <name>)# wmm-background-share <share>

(AP)(SSID Profile <name>)# wmm-best-effort-share <share>

(AP)(SSID Profile <name>)# wmm-video-share <share>

(AP)(SSID Profile <name>)# wmm-voice-share <share>
```

Mapping WMM ACs and DSCP Tags

The IEEE 802.11e standard defines the mapping between WMM ACs and DSCP tags. You can customize the mapping values between WMM ACs and DSCP tags to prioritize various traffic types and apply these changes to a WMM-enabled SSID profile.

DSCP classifies packets based on network policies and rules. The following table shows the default WMM AC to DSCP mappings and the recommended WMM AC to DSCP mappings.

Table 24- 2 WMM AC-DSCP Mapping

DSCP Value	WMM Access Category
8	Background
16	
0	Best effort
24	
32	Video
40	
48	Voice
56	

By customizing WMM AC mappings, all packets received are matched against the entries in the mapping table and prioritized accordingly. The mapping table contains information for upstream (client to AP) and downstream (AP to client) traffic.

You can configure different WMM to DSCP mapping values for each WMM AC when configuring an SSID profile by using the SCALANCE W UI or the CLI.

In the SCALANCE W UI

To configure DSCP mapping values:

1. Navigate to the WLAN wizard.
   - Click **Network > New** or
   - Click **Network**, and select the **WLAN SSID > edit**.
2. Click **Show advanced options** under **WLAN Settings**.
3. Specify the appropriate DSCP mapping value within a range of 0–63 for the following access categories in the **DSCP mapping** text box:
   - **Background WMM**—DSCP mapping for the background traffic.
   - **Best effort WMM**—DSCP mapping for the best-effort traffic.
   - **Video WMM**—DSCP mapping for the video traffic.
   - **Voice WMM**—DSCP mapping for the voice traffic.
4. Click **Next** and complete the configuration as required.

In the CLI

Configuring DSCP settings on an SSID:

```
(AP)(config)# wlan ssid-profile <name>

(AP)(SSID Profile <name>)# wmm-background-dscp <dscp>

(AP)(SSID Profile <name>)# wmm-best-effort-dscp <dscp>

(AP)(SSID Profile <name>)# wmm-video-dscp <dscp>

(AP)(SSID Profile <name>)# wmm-voice-dscp <dscp>
```

You can configure up to 8 DSCP mappings values within the range of 0-63. You can also configure a combination of multiple values separated by a comma, for example, **wmm-voice-dscp 46,44,42,41**

Configuring WMM U-APSD

To extend the battery life and enable power saving on WLAN clients, APs support U-APSD for the clients that support WMM. The U-APSD or the WMM Power Save feature is enabled by default on all SSIDs. When configured, U-APSD enables a client station to retrieve the unicast QoS traffic buffered in the AP by sending trigger frames. During the association or reassociation with the AP, the station indicates the WMM Access Categories for which U-APSD is enabled. In the current release, APs support U-APSD on all WMM ACs.

To disable U-APSD on an SSID:

```
(AP)(config)# wlan ssid-profile <ssid_profile>

(AP)(SSID Profile "<ssid_profile>")# wmm-uapsd-disable
```

To re-enable U-APSD on an SSID:

```
(AP)(config)# wlan ssid-profile <ssid_profile>

(AP)(SSID Profile "<ssid_profile>")# no wmm-uapsd-disable
```

24.2 Media Classification for Voice and Video Calls

SCALANCE W supports the following media classification types:

- Classify Media Flag
- STUN Based Media Classification

Classify Media Flag

Voice and video devices use a signaling protocol to establish, control, and terminate voice and video calls. These control or signaling sessions are usually permitted using predefined ACLs. If the control signaling packets are encrypted, the AP cannot determine the dynamic ports that are used for voice or video traffic. In these cases, the AP has to use an ACL with the classify-media option enabled to identify the voice or video flow based on a DPI and analysis of the actual traffic. SCALANCE W identifies and prioritizes voice and video traffic from applications such as Skype for Business, Apple Facetime, and Jabber.

Skype for Business uses SIP over TLS or HTTPS to establish, control, and terminate voice and video calls. Apple Facetime uses Extensible Messaging and Presence Protocol over TLS or HTTPS for these functions.

The following CLI example shows the media classification for VoIP calls:

```
(AP)(config)# wlan access-rule example_s4b_test

(AP)(example_s4b_test)# rule alias <domain_name_for_S4B_server> match tcp 443 443
permit log classify-media

(AP)(example_s4b_test)# rule any any match tcp 5060 5060 permit log classify-media

(AP)(example_s4b_test)# rule any any match tcp 5061 5061 permit log classify-media

(AP)(example_s4b_test)# rule any any match tcp 5223 5223 permit log classify-media

(AP)(example_s4b_test)# rule any any match any any any permit
```

STUN Based Media Classification

STUN based media classification requires the ACLs permitting signaling sessions without the **classify-media** flag. However, it requires an implicit deny firewall rule for UDP to be activated. All other traffic that should be allowed in the network must be explicitly configured using ACL rules. The AP automatically allows firewall sessions for voice and video calls made from Skype for Business and Apple Facetime. For all other S4B and Facetime applications like desktop sharing and file transfer, the corresponding ports must be explicitly opened by using ACL rules.

Before media transmission, a VOIP client initiates a Session Traversal Utilities for NAT connectivity check. Sessions created by STUN are subjected to media classification that classifies the media as RTP or non-RTP. The firewall automatically allows the RTP session on the AP and denies the non-RTP sessions.

The following CLI example shows the STUN based media classification for Skype for Business:

```
(AP)(config)#wlan access-rule example_s4b_test

(AP)(example_s4b_test)# rule alias <domain_name_for_S4B_server> match tcp 443 443
permit

(AP)(example_s4b_test)# rule any any match tcp 5223 5223 permit

(AP)(example_s4b_test)# rule any any match tcp 5061 5061 permit

(AP)(example_s4b_test)# rule any any match any any any deny

(AP)(example_s4b_test)# end

(AP)# commit apply
```

Note

The ToS values for calls prioritized using the above mentioned media classification types will always carry a ToS of 48 fora voice session and 40 for a video session

24.3 Enabling Enhanced Voice Call Tracking

SCALANCE W provides seamless support for tracking VoIP calls in the network by using SNMP to send the location details of the caller to the third-party server. This feature is currently applied for tracking Emergency 911 VoIP calls.

The Master AP identifies the location from where the VoIP call was placed and sends the details of the location to the third-party SNMP server. You must configure the third-party server as an SNMP host and enable SNMP traps to activate the voice call tracking feature on the AP. For more information on configuring a third-party server as an SNMP host, see Configuring SNMP (Page 439).

The Master AP will send the WLSXIAPVOICECLIENTLOCATIONUPDATE SNMP trap under the following scenarios:

- The VoIP call is successful.
- The VoIP client roams from one AP to another during an active call, the Master AP will identify the VoIP client and send out the WLSXIAPVOICECLIENTLOCATIONUPDATE trap to the emergency call server.

Note

The trap sending feature is not supported for L3 mobility.

The WLSXIAPVOICECLIENTLOCATIONUPDATE trap contains the following information:

Table 24- 3 SNMP Trap Details for VoIP Calls

Parameter	Description
wlsxTrapVcIpAddress	IP address of the VoIP client.
wlsxTrapVcMacAddress	MAC address of the VoIP client.
wlsxTrapAPMacAddress	MAC address of the AP which generated the trap.
wlsxTrapAPName	Name of the AP which generated the trap.

SNMP GET

In order to find the location of a particular emergency caller, the third-party SNMP server sends a query to the Master AP using SNMP GET. The Master AP responds back to the SNMP server with the location (AP Name) of the VoIP caller. Following are the key parameters in the response sent by the Master AP:

- VoIP Client IP Address
- VoIP Client MAC Address
- AP MAC Address
- AP Name

Services 25

25.1 Configuring AirGroup

AirGroup provides a unique enterprise-class capability that leverages zero configuration networking to enable AirGroup services from mobile devices efficiently. Zero configuration networking enables service discovery, address assignment, and name resolution for desktop computers, mobile devices, and network services. It is designed for flat, single-subnet IP networks such as wireless networking at home. The users can register their personal devices and define a group of users who can share the registered devices. Administrators can register and manage an organization's shared devices such as printers and grant global access to each device, or restrict access according to the username, role, or user location.

In large universities and enterprise networks, it is common for devices to connect to the network across VLANs. As a result, user devices on a specific VLAN cannot discover a service that resides on another VLAN. As the addresses used by the protocol are link-scope multicast addresses, each query or advertisement can only be forwarded on its respective VLAN, but not across different VLANs. Broadcast and multicast traffic are usually filtered out from a WLAN network to preserve the airtime and battery life. This inhibits the performance of AirGroup services that rely on multicast traffic. AirGroup addresses this challenge with AirGroup technology.

The distributed AirGroup architecture allows each AP to handle mDNS and DLNA queries and responses individually instead of overloading a network with these tasks. This results in a scalable AirGroup solution.

The AirGroup solution supports both wired and wireless devices. An AirGroup device can be registered by an administrator or a guest user.

1. The AirGroup administrator gives an end user the AirGroup operator role, which authorizes the user to register the client devices on the ClearPass Policy Manager platform. APs maintain information for all AirGroup services. AP queries ClearPass Policy Manager to map each device’s access privileges to the available services and responds to the query made by a device based on contextual data such as user role, username, and location

The following figure illustrates how AirGroup enables personal sharing of Apple devices.

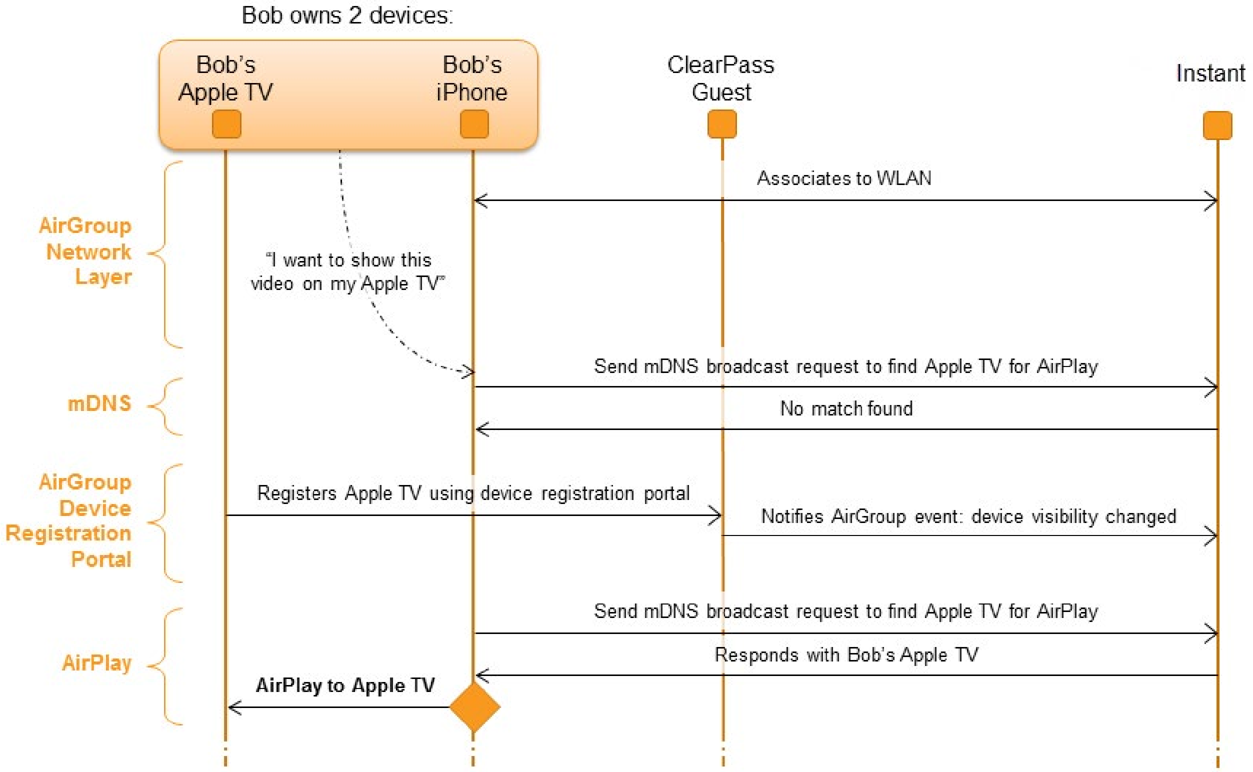

Bob owns 2 devices:
Bob's Apple TV
Bob's iPhone
ClearPass Guest
Instant
AirGroup Network Layer
Associates to WLAN
"I want to show this video on my Apple TV"
mDNS
Send mDNS broadcast request to find Apple TV for AirPlay
No match found
AirGroup Device Registration Portal
Registers Apple TV using device registration portal
Notifies AirGroup event: device visibility changed
AirPlay
Send mDNS broadcast request to find Apple TV for AirPlay
Responds with Bob's Apple TV
AirPlay to Apple TV

Figure 25-1 AirGroup Enables Personal Device Sharing

Note

AirGroup is not supported on 3G and PPPoE uplinks.

Note

For Apple TV mirroring to work, both Apple TV and users must be on either virtual controller-assigned VLANs or network-assigned VLANs. Otherwise, Apple TV mirroring will not work.

25.1.1 Multicast DNS and Bonjour® Services

Bonjour is the trade name for the zero configuration implementation introduced by Apple. It is supported by most of the Apple product lines, including the Mac OS X operating system, iPhone, iPod Touch, iPad, Apple TV, and AirPort Express. Apple AirPlay and AirPrint services are based on the Bonjour protocol and are essential services in campus Wi-Fi networks.

Bonjour can be installed on computers running Microsoft Windows® and is supported by the new network- capable printers. Bonjour is also included with popular software programs such as Apple iTunes, Safari, and iPhoto. Bonjour uses mDNS to locate devices and the services offered by these devices.

As shown in the following figure, the AP1 discovers AirPrint (P1) and AP3 discovers Apple TV (TV1). AP1 advertises information about its connected P1 device to the other APs that is AP2 and AP3. Similarly, AP3 advertises TV1 device to AP1 and AP2. This type of distributed architecture allows any AP to respond to its connected devices locally. In this example, the iPad connected to AP2 obtains direct response from the same AP about the other Bonjour-enabled services in the network.

For a list of supported Bonjour services, see AirGroup Services (Page 355).

25.1.2 DLNA UPnP Support

In addition to the mDNS protocol, APs now support UPnP, and DLNA enabled devices. DLNA is a network standard derived from UPnP, which enables devices to discover the services available in a network. DLNA also provides the ability to share data between the Windows or Android-based multimedia devices. All the features and policies applicable to mDNS are extended to DLNA to ensure full interoperability between compliant devices.

In a UPnP-based scenario, the following types of devices are available in a network:

- Controlled devices (servers)
- Control points (clients)

When a controlled device joins a network and acquires IP address, it multicasts a number of discovery messages for advertising itself, its embedded devices, and services. On the other hand, when a control point joins a network, it may multicast a search discovery message for finding interesting devices and services. The devices listening on the multicast address respond if they match the search criteria in the search message.

In a single AP network, the AP maintains a cache table containing the list of discovered services in the network. The AP also enforces native policies such as disallowing roles and VLANs and the policies defined on ClearPass Policy Manager to determine the devices or services that are allowed and can be discovered in the network. Whenever a search request comes, the AP looks up its cache table and filters the cached data, based on configured policies, then builds a search response, and unicasts it to the requesting device.

The following figure illustrates DLNA UPnP Services and AirGroup Architecture.

For a list of supported DLNA services, see AirGroup Services (Page 355).

25.1.3 AirGroup Features

AirGroup supports the following features:

- Sends unicast responses to mDNS or DLNA queries and reduces the traffic footprint.
- Ensures cross-VLAN visibility and availability of AirGroup devices and services.
- Allows or blocks AirGroup services for all users.
- Allows or blocks AirGroup services based on user roles.
- Allows or blocks AirGroup services based on VLANs.
- Matches devices to their closest services such as printers.

AirGroup also enables context awareness for services across the network:

- AirGroup is aware of personal and shared devices. For example, an Apple TV in a dorm room can be associated with the student who owns it or an Apple TV in a meeting room or a printer in a supply room that is available to certain users, such as the marketing department.
- AirGroup is aware of the location of services when ClearPass Policy Manager support is enabled. For example, depending on the proximity, a user would be presented with the closest printer instead of all the printers in the building.
- When configured, AirGroup enables a client to perform a location-based discovery. For example, when a client roams from one SCALANCE W cluster to another, it can discover devices available in the new cluster to which the client is currently connected
- The following figure shows an example of a higher-education environment with shared, local, and personal services available to mobile devices.

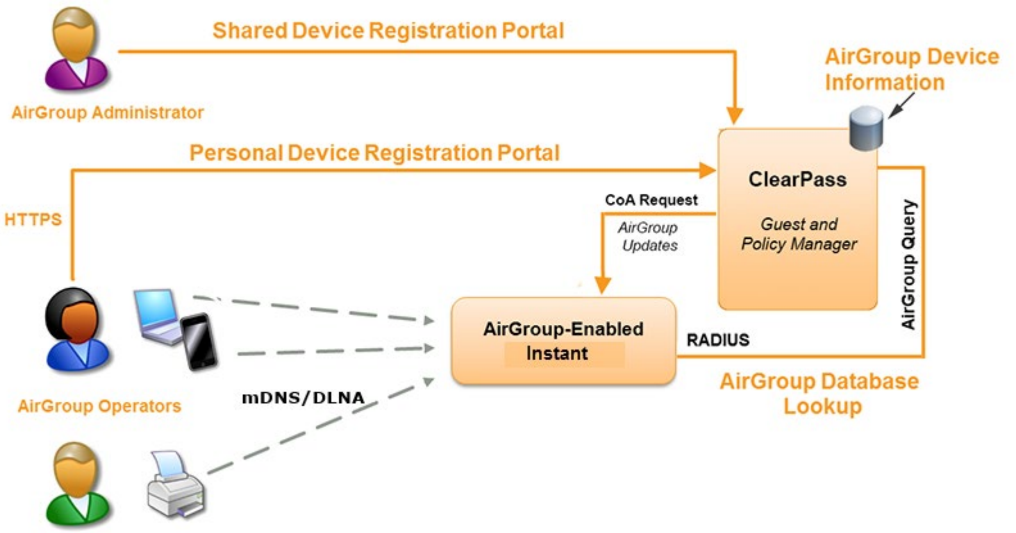


Figure 25-2 AirGroup in a Higher-Education Environment

Note

When AirGroup discovers a new device, it interacts with ClearPass Policy Manager to obtain the shared attributes such as shared location and role. However, the current versions of APs do not support the enforcement of shared location policy.

AirGroup Services

AirGroup supports zero configuration services. The services are preconfigured and are available as part of the factory default configuration. The administrator can also enable or disable any or all services by using the SCALANCE W UI or the CLI.

The following services are available for AP clients:

- AirPlay™—Apple® AirPlay allows wireless streaming of music, video, and slide shows from your iOS device to Apple TV® and other devices that support the AirPlay feature.
- AirPrint™—Apple AirPrint allows you to print from an iPad®, iPhone®, or iPod® Touch directly to any AirPrint-compatible printers.
- iTunes—The iTunes service is used by iTunes Wi-Fi sync and iTunes home-sharing applications across all Apple devices.
- RemoteMgmt—The RemoteMgmt service allows remote login, remote management, and FTP utilities on Apple devices.
- Sharing—The Sharing service allows applications such as disk sharing and file sharing among Apple devices.
- Chat—The iChat® (Instant Messenger) application on Apple devices uses this service.
- ChromeCast—The ChromeCast service allows you to use a ChromeCast device to play audio or video content on a high-definition television by streaming content through Wi-Fi from the Internet or local network.
- DLNA Media—Applications such as Windows Media Player use this service to browse and play media content on a remote device.
- DLNA Print—This service is used by printers that support DLNA.

Note

It is recommended to have a maximum of up to 80 AirGroup servers in the network.

For more information on configuring AirGroup services, see Configuring AirGroup and AirGroup Services on an AP (Page 358).

25.1.4 AirGroup Components

AirGroup leverages key elements of the Aruba solution portfolio including operating system software for SCALANCE W, ClearPass Policy Manager, and the VLAN-based or role-based filtering options offered by the AirGroup services. The components that make up the AirGroup solution include the AP, ClearPass Policy Manager, and ClearPass Guest.

Note

Starting from ClearPass Policy Manager version 6.0, the ClearPass Guest and the AirGroup Services plug-in are integrated into a single platform.

AirGroup maintains seamless connectivity between clients and services across VLANs and SSIDs. The following table summarizes the filtering options supported by SCALANCE W:

Table 25- 1 AirGroup Filtering Options

Features	SCALANCE W Deployment Models	
	Integrated with ClearPass Guest	Integrated with ClearPass Policy Manager
Allow mDNS and DLNA traffic to propagate across sub-nets/VLANs	Yes	Yes
Limit mDNS and DLNA traffic on the network	Yes	Yes
VLAN-based AirGroup service policy enforcement	Yes	Yes
User-role-based AirGroup service policy enforcement	Yes	Yes
Portal to self-register personal devices	No	Yes
Device-owner-based policy enforcement	No	Yes
Shared user-list-based policy enforcement	No	Yes
Shared role-list based-policy enforcement	No	Yes

ClearPass Policy Manager and ClearPass Guest Features

ClearPass Policy Manager and ClearPass Guest support the following features: n Registration portal for WLAN users to register their personal devices.

- Registration portal for WLAN administrators to register shared devices.
- Operator-defined *personal* AirGroup to specify a list of other users who can share devices with the operator.
- Administrator-defined username, user role, and location attributes for shared devices.

25.1.5 Configuring AirGroup and AirGroup Services on an AP

You can configure AirGroup services by using the SCALANCE W UI or the CLI.

In the SCALANCE W UI

To enable AirGroup and its services:

1. Click the **More > Services** link on the SCALANCE W main window.
2. Click the **Air Group** tab.
3. To enable support for Bonjour services, select the **Enable Bonjour** check box and select the AirGroup services related to Bonjour as required.
4. To enable DLNA support, select the **Enable DLNA** check box and select the DLNA services.
5. To allow the users to use Bonjour services enabled in a guest VLAN, select **Enable Guest Bonjour multicast**. When this check box is enabled, the Bonjour devices are visible only in the guest VLAN and AirGroup will not discover or enforce policies in guest VLAN.
6. Select the **Enable Air Group across mobility domains** check box to enable inter-cluster mobility. When enabled, the AP shares the mDNS database information with the other clusters. The DNS records in the virtual controller can be shared with all the virtual controller configured for L3 Mobility.

   By default, this feature is disabled. To define clusters, go to the **System > L3 Mobility** tab.
7. Ensure that the required AirGroup services are selected. To add any service, click **New** and add. To allow all services, select **allow all**. If a custom service is added, you can add a corresponding service ID by clicking **New** under **Service ID**.

   Note

   If an AP is upgraded to the current release with the **Bonjour** check box enabled, ensure that the corresponding Bonjour services are selected.

   Note

   SCALANCE W supports the use of up to 6 custom services.
8. Based on the services configured, you can block any user roles from accessing an AirGroup service and restrict the AirGroup servers connected to a specific set of VLANs from being discovered . The user roles and VLANs marked as disallowed are prevented from accessing the corresponding AirGroup service. You can create a list of disallowed

user roles and VLANs for all AirGroup services configured on the AP. For example, If the AirPlay service is selected, the **edit** links for the **airplay disallowed roles** and **airplay disallowed vlans** are displayed. Similarly, if sharing service is selected, the **edit** links for the **sharing disallowed roles** and **sharing disallowed vlans** are displayed.

- To block user roles from accessing an AirGroup service, click the corresponding **edit** link and select the user roles for which you want to restrict access. By default, an AirGroup service is accessible by all user roles configured in your AP cluster.
- To block VLANs from allowing access to an AirGroup service, click the corresponding **edit** link and select the VLANs to exclude. By default, the AirGroup services are accessible by users or devices in all VLANs configured in your AP cluster

9. **ClearPass Settings**—Use this section to configure the ClearPass Policy Manager server, CoA server, and enforce ClearPass registering.
   - **CPPM server 1**—Indicates the ClearPass Policy Manager server information for AirGroup policy.
   - **Enforce ClearPass registering** —When enabled, only devices registered with ClearPass Policy Manager will be discovered by Bonjour devices, based on the ClearPass Policy Manager policy.

In the CLI

To configure AirGroup:

```
(AP)(config)# airgroup
(AP)(airgroup)# enable [dlna-only | mdns-only]
(AP)(airgroup)# cppm enforce-registration
(AP)(airgroup)# cppm-server <server>
(AP)(airgroup)# cppm-query-interval <interval>
(AP)(airgroup)# disallow-vlan <vlan-ID>
(AP)(airgroup)# enable-guest-multicast
(AP)(airgroup)# multi-swarm
```

To enable DLNA support:

```
(AP)(config)# airgroup
(AP)(airgroup)# enable dlna-only
```

To configure AirGroup services:

```
(AP)(config)# airgroupservice <airgroup-service>
(AP)(airgroup-service)# id <airgroupservice-ID>
(AP)(airgroup-service)# description <text>
(AP)(airgroup-service)# disallow-role <role>
(AP)(airgroup-service)# disallow-vlan <vlan-ID>
```

To verify the AirGroup configuration status:

```
(AP)# show airgroup status
```

25.1.6 Configuring AirGroup and ClearPass Policy Manager Interface in SCALANCE W

Configure the SCALANCE W and ClearPass Policy Manager interface to allow an AirGroup AP and ClearPass Policy Manager to exchange information regarding device sharing, and location. The configuration options define the RADIUS server that is used by the AirGroup RADIUS client.

The AirGroup configuration with ClearPass Policy Manager involves the following steps:

1. Create a RADIUS Server
2. Assigning a Server to AirGroup
3. Configuring ClearPass Policy Manager to Enforce Registration
4. Configuring Change of Authorization (CoA)

Creating a RADIUS Server

You can create a RADIUS server in the **Air Group** window. Navigate to **Services > AirGroup > Clear Pass Settings > CPPM server 1 >** and select **New** from the drop-down list.

You can configure an external RADIUS Security window. For more information on configuring ClearPass Policy Manager server, see Configuring an External Server for Authentication (Page 188).

Assigning a Server to AirGroup

To associate the ClearPass Policy Manager server with AirGroup, select the ClearPass Policy Manager server from the **CPPM Server 1** drop-down list.

Note

If two ClearPass Policy Manager servers are configured, the CPPM server 1 acts as a primary server and the CPPM server 2 acts as a backup server.

After the configuration is complete, this particular server will be displayed in the CoA server option. To view this server go to **Services > AirGroup > ClearPass Settings > CoA server**.

Configuring ClearPass Policy Manager to Enforce Registration

When ClearPass Policy Manager registration is enforced, the devices registered with ClearPass Policy Manager will be discovered by Bonjour devices, based on the ClearPass Policy Manager policy.

Configuring CoA

When a RADIUS server is configured with CoA with the ClearPass Policy Manager server, the guest users are allowed to register their devices. For more information on configuring RADIUS server with CoA , see Configuring an External Server for Authentication (Page 188).

> **Note**
>
> You can also create a **CoA only server** in the **Services > AirGroup > Clear Pass Settings > CoA server** window.

25.2 Configuring an AP for RTLS Support

SCALANCE W supports the real-time tracking of devices when integrated with the AMP or a third-party RTLS server such as Aeroscout RTLS server. With the help of the RTLS, the devices can be monitored in real time or through history.

You can configure RTLS by using the SCALANCE W UI or the CLI.

In the SCALANCE W UI

To configure Aruba RTLS:

1. Click the **More > Services** link on the SCALANCE W main window.
2. In the **Services** section, click the **RTLS** tab.
3. Under **Aruba**, select the **RTLS** check box to integrate SCALANCE W with the AMP or Ekahau RTLS server.
4. Specify the IP address and port to which the location reports must be sent.
5. Specify the shared secret key in the **Passphrase** text box.
6. In the **Update** text box, specify the frequency at which the virtual controller can send updates to the server. You can specify a value within the range of 5-3600 seconds. The default value is 5 seconds.
7. Select the **Include unassociated stations** check box to send reports to the RTLS server about the stations that are not associated to any AP.
8. Click **OK**.

To configure third-party RTLS such as Aeroscout:

1. Select the **Aeroscout** check box to send the RFID tag information to an AeroScout RTLS.
2. Specify the IP address and port number of the AeroScout server to which location reports must be sent.
3. Select the **Include unassociated stations** check box to send reports on the stations that are not associated to any AP to the Aeroscout RTLS server.
4. Click **OK**

In the CLI

To configure AirWave RTLS:

```
(AP)(config)# airwave-rtls <IP-address> <port> <passphrase> <seconds> include-
unassoc- sta
```

To configure Aeroscout RTLS:

```
(AP)(config)# aeroscout-rtls <IP-address> <port> include-unassoc-sta
```

25.3 Configuring an AP for ALE Support

The ALE is designed to gather client information from the network, process it, and share it through a standard API. The client information gathered by ALE can be used for business purposes by analyzing a client’s Internet behavior such as shopping preferences.

ALE includes a location engine that calculates the associated and unassociated device location every 30 seconds by default. For every device on the network, ALE provides the following information through the Northbound API:

- Client username
- IP address
- MAC address
- Device type
- Application firewall data showing the destinations and applications used by associated devices
- Current location
- Historical location

ALE requires the AP placement data to be able to calculate location for the devices in a network.

ALE with SCALANCE W

The ALE server acts as a primary interface to all third-party applications and the AP sends client information and all status information to the ALE server.

To integrate AP with ALE, the ALE server address must be configured on an AP. If the ALE sever is configured with a host name, the virtual controller performs a mutual certificated-based authentication with the ALE server before sending any information.

Enabling ALE Support on an AP

You can configure an AP for ALE support by using the SCALANCE W UI or the CLI.

In the SCALANCE W UI

Configuring ALE support:

1. Click **More > Services**.
2. Click the **RTLS** tab.
3. Select the **Analytics & Location Engine** check box.
4. In the **Server** text box, specify the ALE server name or IP address.
5. In the **Report interval** text box, specify the reporting interval within the range of 6–60 seconds. The AP sends messages to the ALE server at the specified interval. The default interval is 30 seconds.
6. Click **OK**.

In the CLI

To enable AP integration with the ALE server:

```
(AP)(config)# ale-server <server-name | IP-address>
```

```
(AP)(config)# ale-report-interval <seconds>
```

Verifying ALE Configuration on an AP

To view the configuration details:

```
(AP)# show ale config
```

To verify the configuration status:

```
(AP)# show ale status
```

25.4 Managing BLE Beacons

The BLE devices can be connected to an AP and are monitored or managed by a cloud-based BMC. The BLE Beacon Management feature allows you to configure parameters for managing the BLE beacons and establishing secure communication with the BMC. You can also configure the BLE operation modes that determine the functions of the built-in BLE chip in the AP.

You can configure BLE operation modes and enable the BLE Beacon Management feature by using the SCALANCE W UI or the CLI.

In the SCALANCE W UI

Configuring BLE mode:

1. Click **More > Services**.
2. Click the **RTLS** tab. The tab details are displayed.
3. To manage the BLE devices using BMC, select **Manage BLE Beacons**.
4. Enter the authorization token. The authorization token is a text string of 1–255 characters used by the BLE devices in the HTTPS header when communicating with the BMC. This token is unique for each deployment.
5. In **Endpoint URL**, enter the URL of the server to which the BLE sends the monitoring data.
6. Select any of the following options from **Operation Mode** drop-down list:

Mode	Description
Beaconing	The built-in BLE chip of the AP functions as an iBeacon combined with the beacon management functionality.
Disabled	The built-in BLE chip of then AP is turned off. The BLE operation mode is set to **Disabled** by default.
Dynamic Console	The built-in BLE chip of the AP functions in the beaconing mode and dynamically enables access to AP console over BLE when the link to the LMS is lost.
Persistent Console	The built-in BLE chip of the AP provides access to the AP console over BLE and also operates in the **Beaconing** mode.

7. Click **OK**.

In the CLI

To enable BLE beacon management:

```
(AP)(config)# ble config <token> <url>
```

To configure a BLE operation mode:

```
(AP)(config)# ble mode <opmode>
```

To view the BLE configuration details:

```
(AP)# show ble-config
```

25.5 Clarity Live

AP provides support for Inline Monitoring support using Clarity Live to identify client connectivity issues and sends user debug data to AirWave. The client connectivity issues can be a problem with the client, Radius Authentication, DHCP, DNS, or it can be delay in the network. Clarity Live is used to identify the root cause of the problem, this feature can be used.

Inline Monitoring

his functionality of Clarity Live helps diagnose client connectivity issues. It provides the network administrator or engineers with more information regarding the exact stage at which the client connectivity fails or provides data where the dhcp or radius server is slow.

The AP collects all information related to user transitions like association, authentication, and dhcp. Then, the AP sends these records to a management server like AirWave. The management server analyzes the data and concludes which dhcp or radius server was not working efficiently causing user connectivity issues. This enhancement allows the management server to isolate WLAN issues caused by external servers such as dhcp or radius.

HTTPS is the data transport protocol used to communicate basic statistics or state changes to AirWave. Inline Monitoring makes use of HTTPS to send the statistics to AirWave too.

The following events are used by AP to send inline monitoring (Clarity Live) updates to AirWave:

- Authentication Failure Events—The statistics or updates shared as part of this event are related to the management frame. These frames are processed by STM and are collected in the user space.
- DHCP Failure Events—In scenarios where the DHCP Server does not respond, information about the failure of the event can be collected by the AP with the help of Clarity Live and sent to AirWave. This functionality receives client DHCP transactions from the control plane.
- DNS Failure Events—The AP measures the responsiveness of each DNS server with the help of Clarity Live. The monitoring includes minimum, maximum, and average response time of each DNS server. A maximum of 16 DNS servers can be monitored at a time and a maximum of 16 DNS server entries are made in the DNS table. If there are no queries from a particular DNS server for a long period of time, the DNS server entry can be removed and replaced with a new DNS server entry. The statistical data collected for the DNS server will be pushed to AirWave before the entry is replaced by a new DNS entry.
- STA Failure Events—The station passive monitor statistic is generated when enabled on the AP. The AP generate the data periodically for every 60 seconds and sends it to AirWave.

Note

All of the above clarity configurations must be enabled or disabled at the same time whether if it is by the SCALANCE W UI or the CLI. AirWave will drop the message even if one of the four stats is disabled.

You can configure an AP to generate inline monitoring statistics by using the SCALANCE W UI or the CLI.

In the SCALANCE W UI

To enable Clarity Live for generating inline monitoring statistics:

1. Click **More > Services**.
2. Click **Clarity**. The configuration options for the Clarity group are displayed.
3. Select the **Inline Auth stats** checkbox to enable the AP to generate statistics and update messages for Authentication Failure Events.
4. Select the **Inline DHCP stats** checkbox to enable the AP to generate statistics and update messages for DHCP Failure Events.
5. Select the **Inline DNS stats** checkbox to enable the AP to generate statistics and update messages for DNS Failure Events.
6. Select the **Inline STA stats** checkbox to enable the AP to generate statistics and update messages for STA Failure Events.
7. Click **OK.**

In the SCALANCE W CLI

To configure inline monitoring statistics using the CLI:

```
(AP)(config)# clarity

(AP)(clarity)# inline-auth-stats

(AP)(clarity)# inline-dhcp-stats

(AP)(clarity)# inline-dns-stats

(AP)(clarity)# inline-sta-stats
```

Verify Clarity Configuration on AP

The following command is used to view the status of the Inline Monitoring events:

```
(AP)# show clarity config
```

The following command is used to view the history of the authentication events:

```
(AP)# show clarity history auth
```

The following command is used to view the history of the DHCP events:

```
(AP)# show clarity history dhcp
```

The following command is used to view the history of the DNS events:

```
(AP)# show clarity history dns
```

25.6 Configuring OpenDNS Credentials

When configured, the OpenDNS credentials are used by SCALANCE W to access OpenDNS to provide enterprise level content filtering. You can configure OpenDNS credentials by using the SCALANCE W UI or the CLI.

In the SCALANCE W UI

To configure OpenDNS credentials:

1. Click **More > Services > OpenDNS**.
2. Enter the **Username** and **Password** to enable access to OpenDNS.
3. Click **OK** to apply the changes.

In the CLI

To configure OpenDNS credentials:

```
(AP)(config)# opendns <username> <password>
```

25.7 Integrating an AP with Palo Alto Networks Firewall

Palo Alto Networks next-generation firewall offers contextual security for all users for safe enabling of applications. A simple firewall beyond basic IP address or TCP port numbers only provides a subset of the enhanced security required for enterprises to secure their networks. In the context of businesses using social networking sites, legacy firewalls are not able to differentiate valid authorized users from casual social networking users.

The Palo Alto next-generation firewall is based on user ID, which provides many methods for connecting the users to sources of identity information and associating them with firewall policy rules. For example, it provides an option to gather user information from Active Directory or LDAP server.

Integration with SCALANCE W

The functionality provided by the Palo Alto Networks firewall based on user ID requires the collection of information from the network. AP maintains the network (such as mapping IP address) and user information for its clients in the network and can provide the required information for the user ID on Palo Alto Networks firewall. Before sending the user-ID mapping information to the Palo Alto Networks firewall, the AP must retrieve an API key that will be used for authentication for all APIs.

AP provides the User ID mapping information to the Palo Alto Networks firewall for integration. The client user id for authentication will not be sent to the Palo Alto Networks firewall unless it has a domain prefix. The AP checks for the domain information in the client username for all login and logout requests sent to the Palo Alto Networks firewall. If the user id already has a domain prefix, AP forwards the request to the Palo Alto Networks firewall. Otherwise, the static client domain configured in the Palo Alto Networks firewall profile will be prefixed to the user id and then sent to the Palo Alto Networks firewall.

AP and Palo Alto Networks firewall integration can be seamless with the XML-API that is available with Palo Alto Networks-OS 5.0 or later.

To integrate an AP with Palo Alto Networks user ID, a global profile is added. This profile can be configured on an AP with Palo Alto Networks firewall information such as IP address, port, username, password, firewall-enabled or firewall-disabled status.

The AP sends messages to Palo Alto Networks based on the type of authentication and client status:

- After a client completes the authentication and is assigned an IP address, AP sends the **login** message.
- After a client is disconnected or dissociated from the AP, the AP sends a **logout** message.

Configuring an AP for PAN integration

You can configure an AP for Palo Alto Networks firewall integration by using the SCALANCE W UI or the CLI.

In the SCALANCE W UI

To configure Palo Alto Networks firewall integration in an AP:

1. Click **More > Services**.
2. Click **Network Integration**. The Palo Alto Networks firewall configuration options are displayed.
3. Select the **Enable** check box to enable Palo Alto Networks firewall.
4. Provide the user credentials of the Palo Alto Networks firewall administrator in the **Username** and **Password** text boxes.
5. Enter the Palo Alto Networks firewall IP address.
6. Enter the port number within the range of 1–65,535. The default port is 443.
7. Specify the static **Client Domain** to be mapped to the client User IDs that do not have a domain name of its own.
8. Click **OK**.

In the CLI

To enable Palo Alto Networks firewall integration with the AP:

```
(AP)(config)# firewall-external-enforcement pan

(AP)(firewall-external-enforcement pan)# enable

(AP)(firewall-external-enforcement pan)# domain-name <name>

(AP)(firewall-external-enforcement pan)# ip <ip-address>

(AP)(firewall-external-enforcement pan)# port <port>

(AP)(firewall-external-enforcement pan)# user <name> <password>
```

25.8 Integrating an AP with an XML API Interface

The XML API interface provides options to create and execute user management operations seamlessly on behalf of the clients or users.

Integration with SCALANCE W

The XML API interface allows you to send specific XML commands to an AP from an external server. These XML commands can be used to customize AP client entries. You can use the XML API interface to add, delete, authenticate, query, or blacklist a user or a client.

Note

The user authentication is supported only for users authenticated by captive portal authentication and not for the dot1x-authentication users.

Note

The user add operation performed by the XML API interface is only used to modify the role of an existing user and not to create a new user.

You can now use HTTP or HTTPS to post commands to AP. The communication process using the XML API Interface is as follows:

An API command is issued in XML format from the server to the virtual controller.

The virtual controller processes the XML request and identifies where the client is and sends the command to the correct slave AP.

Once the operation is completed, the virtual controller sends the XML response to the XML server.

Users can use the response and take appropriate action to suit their requirements. The response from the virtual controller is returned using the predefined formats.

Configuring an AP for XML API integration

You can configure an AP for XML API integration by using the SCALANCE W UI or the CLI. AP supports the configuration of up to 8 XML API server entries.

In the SCALANCE W UI

Enabling XML API server entries:

1. Click **More > Services**.
2. Click **Network Integration**. The XML API Server configuration parameters are displayed.
3. Enter a name for the XML API Server in the **Name** text box.
4. Enter the subnet of the XML API Server in the **Subnet** text box.
5. Enter the subnet mask of the XML API Server in the **Mask** text box.
6. Enter a passcode in the **Passphrase** text box, to enable authorized access to the XML API Server.

7. Re-enter the passcode in the **Retype** box.
8. To add multiple entries, repeat the procedure
9. Click **OK.**
10. To edit or delete the server entries, use the **Edit** and **Delete** buttons, respectively.

In the CLI

To enable XML API integration with the SCALANCE WAP:

```
(AP)(config)# xml-api-server <xml_api_server_profile>

(AP)(xml-api-server <profile-name>)# ip <subnet> [mask <mask>]

(AP)(xml-api-server)# key <key>
```

Creating an XML API Request

You can now create an XML request with an appropriate authentication command and send it to the virtual controller through HTTPS post. The format of the URL to send the XML request is:

```
https://<virtualcontroller-ip/auth/command.xml>
```

- **virtualcontroller-ip**: The IP address of the virtual controller that will receive the XML API request
- **command.xml** : The XML request that contains the XML API command. The format of the XML API request is:
- `xml=<scalance command="<XML API command>">`

```
<options>Value</options>

...

<options>Value</options>

</ scalance>
```

You can specify any of the following commands in the XML request:

Table 25- 2 XML API Command

Parameter	**Description**
user_add	If the user entry is already present in the user table, the command will modify the entry with the values defined in the XML request. For an existing user, this command will update any value that is supplied, with an exception of IP and MAC address. Session time-out is only applicable to captive portal users.
user_delete	This command deletes an existing user from the user table of the virtual controller. **NOTE**: Do not use the user_delete command if the intention is to clear the association from the virtual controller user table. If the client is dual-stack, it re-inherits the authentication state from the IPv6 address. If not dual-stack, the client reverts to the initial role
user_authenticate	This command authenticates against the server group defined in the captive portal profile. This is only applicable to captive portal users.

Parameter	Description
user_blacklist	This command blacklists a user from connecting to your network. This command uses the default blacklist timeout of 3600 seconds. There is no corresponding clear command.
user_query	This command fetches the status and details of a user connected to your network. A dual- stack client can be queried by any of its IPv4 or IPv6 addresses, but only the queried IP address is displayed in the output.

Each XML API command requires certain mandatory options to successfully execute the task. The list of all available options are:

Table 25- 3 XML API Command Options

Parameter	Description	Range / Defaults
ipaddr	IP address of the user in IPv4 or IPv6 format.	—
macaddr	MAC address of the user in aa:bb:cc:dd:ee:ff format.	Enter MAC address with colon.
user	Name of the user.	64-character string
role	This option is used to change the role of an existing user. This option applies to user_add and user_delete commands only.	64-character string
password	The password of the user for authentication.	—
session_timeout	The role will be changed to a pre-auto role after session timeout.	—
authentication	Authentication method used to authenticate the message and the sender. You can use any of MD5, SHA-1 or clear text methods of authentication. This option is ignored if shared secret is not configured. It is, however, mandatory if it is configured.	
key	This is the encoded MD5 or SHA-1 hash of shared secret or plain text shared secret. This option is ignored if shared secret is not configured on the switch. The actual MD5 or SHA-1 hash is 16/20 bytes and consists of binary data. It must be encoded as an ASCII-based HEX string before sending. It must be present when the virtual controller is configured with an xml API key for the server. Encoded hash length is 32/40 bytes for MD5 or SHA-1.	
version	The version of the XML API interface available in the virtual controller. This is mandatory in all XML API requests.	Current version is XML API 1.0

25.9 CALEA Integration and Lawful Intercept Compliance

LI allows the Law Enforcement Agencies to perform an authorized electronic surveillance. Depending on the country of operation, the service providers are required to support LI in their respective networks.

In the United States, service providers are required to ensure LI compliance based on CALEA specifications.

SCALANCE W supports CALEA integration in a hierarchical and flat topology, mesh AP network, the wired and wireless networks.

Note

Enable this feature only if lawful interception is authorized by a law enforcement agency.

CALEA Server Integration

To support CALEA integration and ensure LI compliance, you can configure the APs to replicate a specific or selected client traffic and send it to a remote CALEA server.

Traffic Flow from AP to CALEA Server

You can configure an AP to send GRE-encapsulated packets to the CALEA server and replicate client traffic within the GRE tunnel. Each AP sends GRE encapsulated packets only for its associated or connected clients. The following figure illustrates the traffic flow from the AP to the CALEA server.

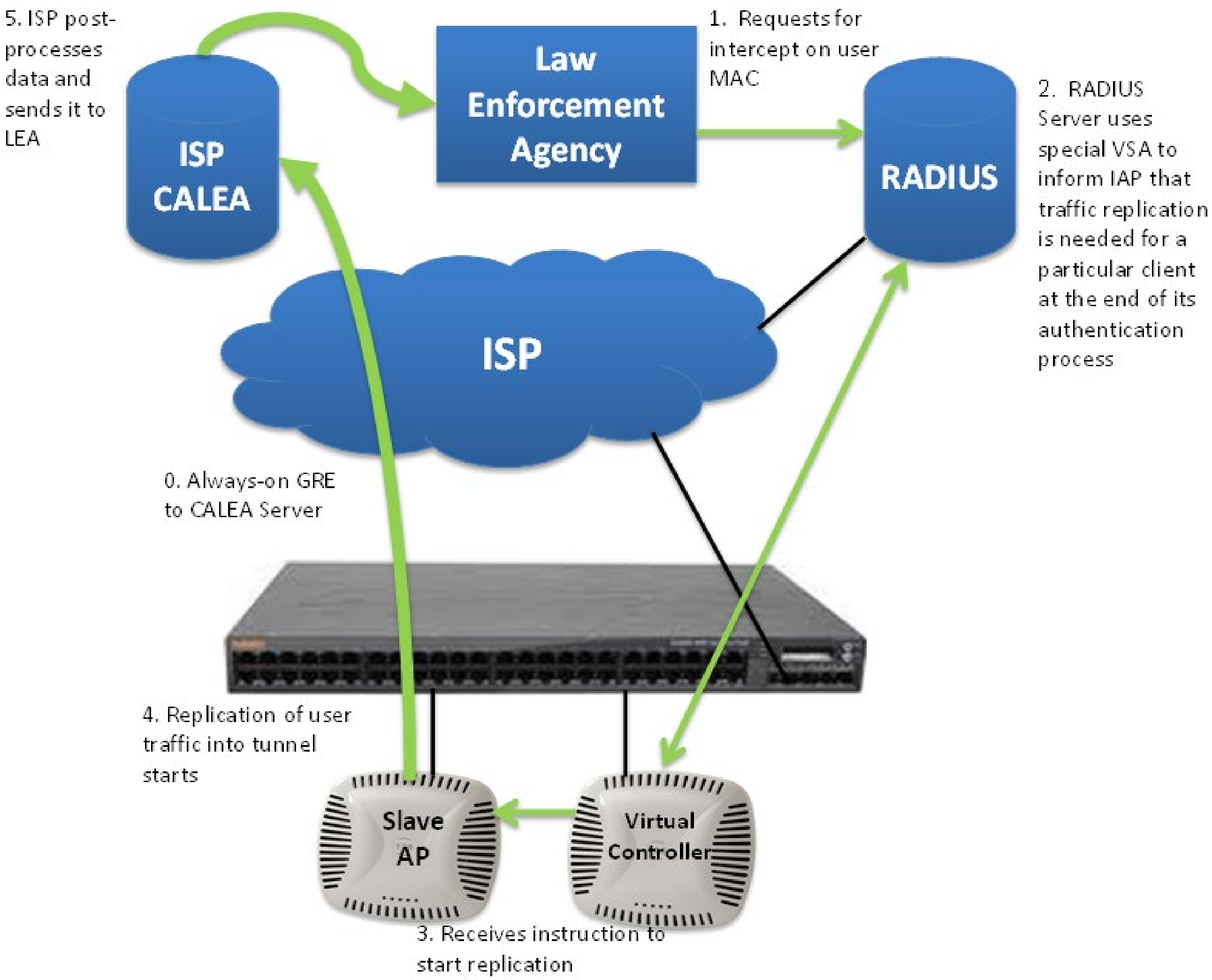

5. ISP post-processes data and sends it to LEA
Law Enforcement Agency
1. Requests for intercept on user MAC
ISP CALEA
RADIUS
2. RADIUS Server uses special VSA to inform IAP that traffic replication is needed for a particular client at the end of its authentication process
ISP
0. Always-on GRE to CALEA Server
4. Replication of user traffic into tunnel starts
Slave AP
Virtual Controller
3. Receives instruction to start replication

Figure 25-3 AP to CALEA Server

Traffic Flow from AP to CALEA Server through VPN

You can also deploy the CALEA server with the controller and configure an additional IPsec tunnel for corporate access. When CALEA server is configured with the controller, the client traffic is replicated by the slave AP and client data is encapsulated by GRE on slave, and routed to the master AP. The master AP sends the IPsec client traffic to the controller. The controller handles the IPsec client traffic while GRE data is routed to the CALEA server. The following figure illustrates the traffic flow from AP to the CALEA server through VPN

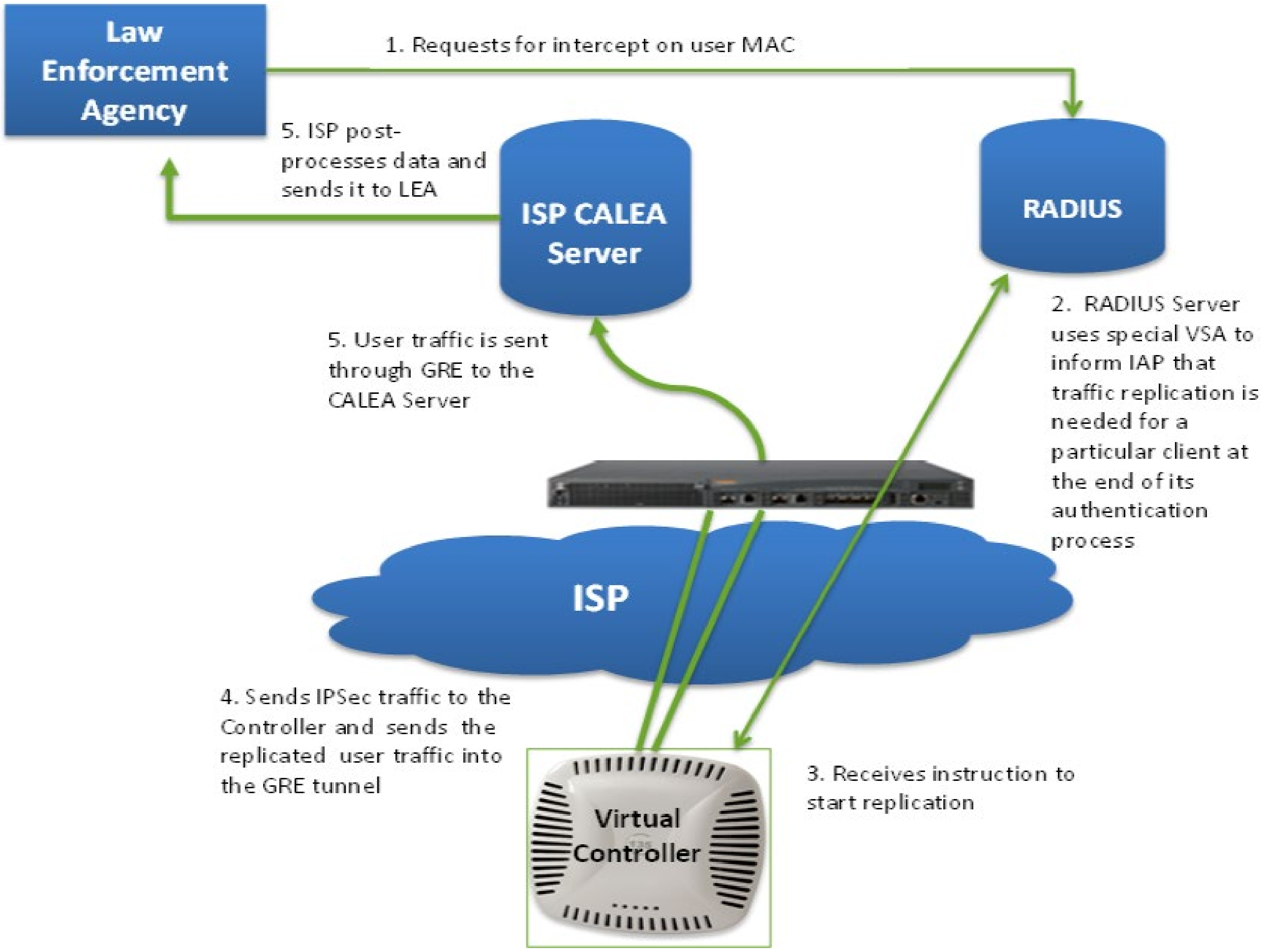

Law Enforcement Agency
1. Requests for intercept on user MAC
5. ISP post-processes data and sends it to LEA
ISP CALEA Server
RADIUS
5. User traffic is sent through GRE to the CALEA Server
2. RADIUS Server uses special VSA to inform IAP that traffic replication is needed for a particular client at the end of its authentication process
ISP
4. Sends IPSec traffic to the Controller and sends the replicated user traffic into the GRE tunnel
Virtual Controller
3. Receives instruction to start replication

Figure 25-4 AP to CALEA Server through VPN

Client Traffic Replication

Client traffic is replicated in the following ways:

- Through RADIUS VSA—In this method, the client traffic is replicated by using the RADIUS VSA to assign clients to a CALEA-related user role. To enable role assignment to clients, you need to create a user role and a CALEA access rule, and then assign the CALEA rule to the user role. Whenever a client that is configured to use a CALEA rule connects, a replication role is assigned.

- Through CoA—In this method, a user session can start without replication. When the network administrator triggers a CoA from the RADIUS server, the user session is replicated. The replication is stopped when the user disconnects or by sending a CoA to change the replication role.

As the client information is shared between multiple APs in a cluster, the replication rules persist when clients roam within the cluster.

Configuring an AP for CALEA Integration

To enable CALEA server integration, perform the following steps:

1. Create a CALEA profile.
2. If a replication role must be assigned through the RADIUS VSA, create an access rule and assign the access rule to a WLAN SSID or wired profile.
3. Verify the configuration.

Creating a CALEA Profile

You can create a CALEA profile by using the SCALANCE W UI or the CLI.

In the SCALANCE W UI

1. Click **More > Services** link on the SCALANCE W main window.
2. In the Services section, click **CALEA**. The **CALEA** tab details are displayed.
3. Specify the following parameters:
   – **IP address**—Specify the IP address of the CALEA server.
   – **Encapsulation type**—Select the encapsulation type. The current release of SCALANCE W supports GRE only.
   – **GRE type**—Specify the GRE type.
   – **MTU** —Specify a size for the MTU within the range of 68–1500. After GRE encapsulation, if packet length exceeds the configured MTU, IP fragmentation occurs. The default MTU size is 1500.
4. Click **OK**.

In the CLI

To create a CALEA profile:

```
(AP)(config)# calea

(AP)(calea)# ip <IP-address>

(AP)(calea)# ip mtu <size>

(AP)(calea)# encapsulation-type <gre>

(AP)(calea)# gre-type <type>
```

Creating an Access Rule for CALEA

You can create an access rule for CALEA by using the SCALANCE W UI or the CLI.

In the SCALANCE W UI

1. To add the CALEA access rule to an existing profile:
   - Select an existing wireless (**Network > edit**) or,
   - Select a Wired (**More > Wired > Edit**) profile.
2. To add the access rule to a new profile:
   - Click **New** under the **Network** tab and create a WLAN profile or,
   - Click **More > Wired > New** and create a wired port profile.
3. On the **Access** tab, select the role for which you want create the access rule.
4. Under **Access Rules**, click **New**.
5. In the **New Rule** window that is displayed, select **CALEA**.
6. Click **OK**.
7. Create a role assignment rule if required.
8. Click **Finish**.

In the CLI

To create a CALEA access rule:

```
(AP)(config)# wlan access-rule <name>
```

```
(AP)(Access Rule <name>)# calea
```

To assign the CALEA rule to a user role:

```
(AP)(config)# wlan ssid-profile <name>
```

```
(AP)(SSID Profile <name>)# set-role <attribute>{{equals | not-equals | starts-with|
ends-with | contains}<operator><role> | value-of}
```

To associate the access rule with a wired profile:

```
(AP)(config)# wired-port-profile <name>
```

```
(AP)(Wired ap profile <name>)# access-rule-name <name>
```

Verifying the configuration

To verify the CALEA configuration:

```
(AP)# show calea config
```

To view the tunnel encapsulation statistics:

```
(AP)# show calea statistics
```

Example

To enable CALEA integration:

```
(AP)(config)# calea
```

To enable a CALE access rule:

```
(AP)(config)# wlan access-rule ProfileCalea
(AP)(Access Rule "ProfileCalea")# calea
```

To assign the CALEA rule to user role:

```
(AP)(config)# wlan ssid-profile Calea-Test
(AP)(SSID Profile"Calea-Test")# enable
(AP)(SSID Profile"Calea-Test")# index 0
(AP)(SSID Profile"Calea-Test")# type employee
(AP)(SSID Profile"Calea-Test")# essid QA-Calea-Test
(AP)(SSID Profile"Calea-Test")# opmode wpa2-aes
(AP)(SSID Profile"Calea-Test")# max-authentication-failures 0
(AP)(SSID Profile"Calea-Test")# auth-server server1
(AP)(SSID Profile"Calea-Test")# set-role Filter-Id equals 123456 calea-test
(AP)(SSID Profile"Calea-Test")# rf-band 5.0
(AP)(SSID Profile"Calea-Test")# captive-portal disable
(AP)(SSID Profile"Calea-Test")# dtim-period 1
(AP)(SSID Profile"Calea-Test")# inactivity-timeout 1000
(AP)(SSID Profile"Calea-Test")# broadcast-filter none
(AP)(SSID Profile"Calea-Test")# dmo-channel-utilization-threshold 90
(AP)(SSID Profile"Calea-Test")# local-probe-req-thresh 0
(AP)(SSID Profile"Calea-Test")# max-clients-threshold 64
```

To verify the configuration:

```
(AP)# show calea config
calea-ip :10.0.0.5
encapsulation-type :gre
gre-type :25944
ip mtu : 150
```

To view the tunnel encapsulation statistics:

```
(AP)# show calea statistics

Rt resolve fail : 0

Dst resolve fail: 0

Alloc failure : 0

Fragged packets : 0

Jumbo packets : 263

Total Tx fail : 0

Total Tx ok : 263
```

SDN 26

26.1 Overview

SDN is an architecture that uses OpenFlow. It enables software programs to manipulate the flow of packets in a network, and manages the traffic to suit the requirements of an application. OpenFlow enables an SDN controller by allowing dynamic manipulation of a forwarding plane of controllers and routers. In an SCALANCE W deployment scenario, OpenFlow runs on every master and slave AP. The APs can connect and communicate with the OpenFlow controller over a TCP channel. However encryption between the OpenFlow agent and OpenFlow controller takes place through TLS.

Functionalities of SDN

Interoperability

With SDN and OpenFlow, it is possible to interoperate with, control, and manage third party devices in the network.

Customization or Programmability

SDN enables network programmability. This flexibility enables customers to build applications that can control and manage network traffic to suit their needs.

26.2 Openflow for WLAN

Every AP interacts directly with an OpenFlow controller. An AP makes wireless clients connected to the OpenFlow enabled port appear on the OpenFlow controller. When the AP learns about a client connected to the port, the AP sends a gratuitous ARP packet (enclosed in an OpenFlow protocol message) to the OpenFlow controller. Prior to this, the AP exposes all WLAN ports and OpenFlow SSIDs as a logical port to the Openflow controller. This way, OpenFlow controller learns about the hosts on some ports of the AP. When an OpenFlow controller pushes the flow of clients to an AP, it can find out the right AP to which the flow needs to be pushed.

Heuristics and RTPA Support

When OpenFlow agent is enabled, APs can send heuristics and RTP analysis data to the OpenFlow controller. The controller runs as Service Controller.

Note

OpenFlow is not supported on Layer-3 mobility profiles and wired profiles.

You can enable OpenFlow configuration by using the SCALANCE W UI or the CLI:

In the SCALANCE W UI:

To enable OpenFlow SSID:

1. On the **Network** tab of the SCALANCE W main window, click the **New** link. The **New WLAN** window is displayed.
2. Enter a name that uniquely identifies a WLAN network in the **Name** text box.
3. Select the **Openflow** checkbox.

To enable OpenFlow TLS authentication:

1. Click the **Services** link under **More** on the SCALANCE W main window. The **Services** window is displayed.
2. Click the **Openflow** tab.
3. Update the controller IP address in the **OFC IP/FQDN** textbox.
4. Update the port address in the **Port** text box.
5. Select the **TLS** checkbox.
6. Click **OK**.

In the CLI:

To configure an OpenFlow enabled SSID in a WLAN profile:

```
(AP)(config)# wlan ssid-profile <name>
```

```
(AP)(SSID Profile <name>)# openflow-enable
```

To enable OpenFlow through TCP and TLS channels:

```
openflow-server {host <addr> tcp-port <port> | tls-enable}
```

Cluster Security 27

27.1 Overview

Cluster security is a communication protocol that secures control plane messages between SCALANCE W access points. Control plane messages such as configuration, cluster join, and other messages distributed between the devices in a cluster are secured using this protocol. Cluster security operates on the UDP port 4434 and uses DTLS protocol to secure messages.

Cluster Security Using DTLS

Cluster security provides secure communication using DTLS. A DTLS connection is established between the APs communicating with each other in the cluster.

Following are some of the advantages of using DTLS for cluster security:

- Mutual authentication is done between the APs in a cluster using device certificate.
- Peer MAC address validation against **AP whitelist** can be enabled in the configuration.
- Control plane messages between cluster members are transmitted securely using the DTLS connection established.

Note

If auto-join is enabled, backward compatibility and recovery of APs is allowed on UDP port 8211. Messages required for image synchronization and cluster security DTLS state synchronization are the only messages allowed.

Note

If auto-join is disabled, the MAC address of a peer AP is verified against the **AP whitelist** during device certificate validation.

Locked Mode Slave AP

A slave AP with non-factory default configuration and DTLS enabled in that configuration is considered to be in locked mode of operation. These slave APs will not be able to join the existing non-DTLS cluster as backward compatibility and recovery is not allowed. This is done for security reasons.

To recover the slave APs in locked mode:

- Execute the **disable-cluster-security-dtls** action command on the slave AP , or
- Factory reset the slave AP.

Auto-Join Disabled Mode

A cluster with DTLS enabled and auto-join disabled is the most secure mode of operation. In this mode, the cluster communicates only using DTLS, and backward compatibility and recovery are denied. This is done for security reasons.

In this mode, a new slave AP with DTLS disabled or running a software version prior to SCALANCE W 6.5.1.0- 4.3.1.0 will not be able to join the cluster even if the MAC address of the slave AP is added to the allowed AP whitelist.

To recover the slave AP:

- Enable Auto join mode.
- Wait for the new slave AP to join the cluster. The MAC address of the AP is automatically added to the allowed AP whitelist.
- Disable Auto join mode.

27.2 Enabling Cluster Security

You can enable cluster security using the SCALANCE W UI or the CLI. Ensure that the following pre-requisites are satisfied:

Pre-requisites

1. NTP server must be reachable—If internet is reachable, pool.ntp.org will be used by default, otherwise a static NTP server needs to be configured.
2. UDP port 4434 should be permitted.

In the SCALANCE W UI:

To enable cluster security:

1. Navigate to **System > General** .
2. Select **Enabled** from the **Cluster security** drop-down list.
3. Click **OK**.

Note

Reboot all the APs in the swarm for the configuration to take effect.

In the CLI:

To enable cluster security:

```
(AP)(config)# cluster-security
```

```
(AP)(cluster-security)# dtls
```

To disable cluster security DTLS:

```
(AP)(config)# cluster-security
```

```
(AP)(cluster-security)# no dtls
```

To change per module logging level of cluster security:

```
(AP)# cluster-security logging module <module_name> log-level <level>
```

To set individual log level for each module:

```
(AP)# cluster-security logging module <module_name> log-level-individual <level>
```

Note

After enabling or disabling the cluster security option, ensure that the Config Sync Status is TRUE in the output of the show summary command, before rebooting the cluster.

Note

Cluster security is not supported for L3 mobility.

27.3 Cluster Security Debugging Logs

Cluster security logging is organized into modules based on functionality. The following are the core modules which are useful and should be used for debugging:

peer—The peer module is used to log connection initiation, renegotiation, collision and active connection updates. The log-level should be set to **debug** level while debugging any issues.

conn—The connection module is used to log connection creation, establishment, data transfer and maintenance updates. The log-level should be set to **debug** level for debugging DTLS connection issues.

mcap—The module capture module is used to log messages sent and received to the socket. Set log-level to **debug** to log only control messages. Set log-level to **debug1** to log control and data messages.

The following command can be used to set per module logging level:

```
(AP)# cluster-security logging module <module_name> log-level <level>
```

Once the log-level is set, logs can be viewed using:

```
(AP)# show log papi-handler
```

27.4 Verifying the Configuration

The following show commands can be used to view the cluster security configuration:

To view current cluster security Configuration and running state

```
(AP)# show cluster-security
```

To view the cluster security statistics:

```
(AP)# show cluster-security stats
```

To view the cluster security connection table:

```
(AP)# show cluster-security connections
```

To view the cluster security peers:

```
(AP)# show cluster-security peers
```

To view the message handler process logs:

```
(AP) # show log papi-handler <count>
```

AP Management and Monitoring 28

28.1 Managing an AP from AirWave

AirWave is a powerful platform and easy-to-use network operations system that manages Aruba wireless, wired, and remote access networks, as well as wired and wireless infrastructures from a wide range of third- party manufacturers. With its easy-to-use interface, AirWave provides real-time monitoring, proactive alerts, historical reporting, as well as fast and efficient troubleshooting. It also offers tools that manage RF coverage, strengthen wireless security, and demonstrate regulatory compliance.

AirWave can be used to provision, manage, and monitor a multi-site deployment of SCALANCE W networks. For example, if you have 100 retail offices that require SCALANCE W to provide WLAN connectivity at each office, AirWave can be used to provision all the 100 offices from a central site. AirWave also provides the administrator with the ability to monitor these geographically dispersed SCALANCE W networks using an AirWave server depending on the scalability recommendations for AirWave.

The APs communicate with AirWave using the HTTPS, XML, or Websocket protocol. This allows an AirWave server to be deployed in the cloud across a NAT device, such as a router.

The AirWave features available in the SCALANCE W network are described in the following sections:

Image Management

AirWave allows you to manage firmware updates on WLAN devices by defining a minimum acceptable firmware version for each make and model of a device. It remotely distributes the firmware image to the WLAN devices that require updates, and it schedules the firmware updates such that updating is completed without requiring you to manually monitor the devices.

The following models can be used to upgrade the firmware:

- Automatic—In this model, the virtual controller periodically checks for newer updates from a configured URL and automatically initiates upgrade of the network.
- Manual—In this model, the user can manually start a firmware upgrade for each virtual controller or set the desired firmware preference per group of devices.

Resetting an AP

A virtual controller is added to the AirWave database either on management mode or monitor mode based on the AirWave configuration.

An AP device can be reset through AirWave in the **Managed** mode:

1. In the **Modify Devices** section, select the AP devices you want to reset to factory-default by selecting the check box beside it.
2. From the **Change Device Group Folder** drop-down list, select **Factory Reset selected devices**.
3. Click the **Factory Reset** tab.

Note

On resetting the AP device from AirWave, all the configuration values will be set to default except for the **per- ap-settings** and **VC Key** value.

AP and Client Monitoring

AirWave allows you to find any AP or client on the wireless network and to see real-time monitoring views. These monitoring views can be used to aggregate critical information and high-end monitoring information.

In the AirWave UI, you can select either **Manage Read/Write** or **Monitor-only+Firmware Upgrades** as management modes. When the AirWave Management level is set to **Manage Read/Write**, the SCALANCE W UI is in read-only mode. When the AirWave Management level is set to **Monitor-only+Firmware Upgrades**, the SCALANCE W UI changes to the read-write mode.

With the latest version of AirWave, a new option in the AMP is available to put the AP in config-only mode. In this mode, the AP will receive the firmware upgrades and configurations, but will not send any statistics for monitoring. The load is reduced on AP and AirWave and this assists in scaling AirWave effectively.

Template-Based Configuration

AirWave automatically creates a configuration template based on any of the existing APs, and it applies that template across the network as shown in the following figure. It audits every device on an ongoing basis to ensure that configurations never vary from the enterprise policies. It alerts you whenever a violation is detected and automatically repairs the incorrectly configured devices.

Trending Reports

AirWave saves up to 14 months of actionable information, including network performance data and user roaming patterns, so you can analyze how network usage and performance trends have changed over time. It also provides detailed capacity reports with which you can plan the capacity and appropriate strategies for your organization.

IDS

AirWave provides advanced, rules-based rogue classification. It automatically detects rogue APs irrespective of their location in the network and prevents authorized APs from being detected as rogue APs. It tracks and correlates the IDS events to provide a complete picture of network security.

WIDS Event Reporting to AirWave

AirWave supports WIDS Event Reporting, which is provided by SCALANCE W. This includes WIDS classification integration with the RAPIDS module. RAPIDS is a powerful and easy-to-use tool for automatic detection of unauthorized wireless devices. It supports multiple methods of rogue detection and uses authorized wireless APs to report other devices within range.

The WIDS report cites the number of IDS events for devices that have experienced the most instances in the prior 24 hours and provides links to support additional analysis or configuration in response.

RF Visualization Support for SCALANCE W

AirWave supports RF visualization for SCALANCE W. The VRF module provides a real-time picture of the actual radio environment of your wireless network and the ability to plan the wireless coverage of new sites. VRF uses sophisticated RF fingerprinting to accurately display coverage patterns and calculate the location of every SCALANCE W device in range. VRF provides graphical access to floor plans, client location, and RF visualization for floors, buildings, and campuses that host your network.

PSK-Based and Certificate-Based Authentication

The PSK-Based and Certificate-Based Authentication are determined by the AMP configuration field.

For a PSK-based authentication, the AMS-IP and PSK must be configured in the AP. The virtual controller attempts to use the login message to initiate a connection.

For a Certificate-based authentication, the AMS-IP and the PSK or just the AMS hostname must be configured in the AP. The AP sends a login message to the AMP. The AMP responds with a randomly generated string. The AP signs the string with its private key and certificate, and sends it back to the AMP. The AMP verifies if the certificate and signature are valid.

A virtual controller is approved based on the status of the Whitelist database:

- When Whitelist is enabled, the AMP verifies if the MAC address and serial number in the login message of the virtual controller and the whitelist database match. If they match, a virtual controller is created and approved. If they do not match, no virtual controller is created.
- When Whitelist is disabled, the virtual controller is created based on the following conditions:
  - Presence of other virtual controller with the same organization string and PSK in the AMP.
  - Approval of at least one of the virtual controller in the AMP.

Configurable Port for AP and AirWave Management Server Communication

You can now customize the port number of the AMP server through the **server_host:server_port** format, for example, **amp.siemens.com:4343**.

The following example shows how to configure the port number of the AMP server:

```
24:de:c6:cf:63:60 (config) # ams-ip 10.65.182.15:65535
```

28.2 Configuring Organization String

The Organization string is a set of colon-separated strings created by the AirWave administrator to accurately represent the deployment of each AP. This string is defined by the installation personnel on the site.

You can use any of the following strings:

- AMP Role—"Org Admin" (initially disabled)
- AMP User—"Org Admin" (assigned to the role "Org Admin")
- Folder—"Org" (under the Top folder in AMP)
- Configuration Group—"Org"

You can also assign additional strings to create a hierarchy of subfolders under the folder named "Org". For example:

- subfolder1 for a folder under the "Org" folder
- subfolder2 for a folder under subfolder

Shared Key

The Shared Secret key is an optional key used by the administrator to manually authorize the first virtual controller for an organization. Any string is acceptable.

The AirWave administrator can use a shared key to manually authorize the first virtual controller for an organization. Any string is acceptable, but this string must be the same for all devices in your organization.

The AirWave administrator sends the shared secret key, Organization String and the AirWave IP address to the on-site installer setting up the virtual controller and other SCALANCE W devices on the network. The AirWave administrator then manually authorizes the virtual controller shared secret key when it appears in the **APs/Devices** > **New list**. After the virtual controller has been validated, other SCALANCE W devices using that shared key will automatically be sent to the AirWave server, and appear in the **APs/Devices** > **New list**.

Configuring AirWave Information

You can configure AirWave information by using the SCALANCE W UI or the CLI.

In the SCALANCE W UI

To configure AirWave information:

1. Click the AirWave **Set Up Now** link of the main window. The **System** window is displayed with the AirWave parameters on the **Admin** tab.
2. Enter the name of your organization in the **Organization name** text box. The name defined for the organization is displayed under the **Groups** tab in the AirWave UI.
3. Enter the IP address or domain name of the AirWave server in the **AirWave server** text box.

4. Enter the IP address or domain name of a backup AirWave server in the **AirWave backup server** text box. The backup server provides connectivity when the primary server is down. If the AP cannot send data to the primary server, the virtual controller switches to the backup server automatically.
5. Enter the shared key in the **Shared key** text box and reconfirm. This shared key is used for configuring the first AP in the SCALANCE W network.
6. Click **OK**.

In the CLI

To configure AirWave information:

```
(AP)(config)# organization <name>

(AP)(config)# ams-ip <IP-address or domain name>

(AP)(config)# ams-backup-ip <IP-address or domain name>

(AP)(config)# ams-key <key>
```

Configuring for AirWave Discovery Through DHCP

AirWave can be discovered through the DHCP server. You can configure this only if AirWave was not configured earlier or if you have deleted the precedent configuration.

On the DHCP server, the format for option 60 is “**SCALANCE WAP**“, and the two formats for option 43 are “**<organization>,<ams-ip>,<ams-key>**” and “**<organization>,<ams-domain>**” .

If you use the **<organization>,<ams-ip>,<ams-key>** format, the PSK-based authentication is used to access the AMP server.

If you use the **<organization>,<ams-domain>** format, the AP resolves the domain name into two IP addresses—AirWave Primary and AirWave Backup.

Note

For option 43, when you choose to enter the domain name, the IP address and key are not available.

Enabling DNS-Based Discovery of the Provisioning AMP Server

APs can now automatically discover the provisioning AMP server if the DHCP option 43 and Activate cannot perform ZTP and transfer the AirWave configuration to the AP.

When a domain option **xxx** is included in the DHCP configuration, the AP will search the DNS server records for **airwave.xxx**. When there is no domain option, the AP will search only the server records for **airwave**.

Note

To enable APs to automatically discover the AMP server, create a DNS record for **airwave.xxx** or **airwave** in the DNS server. To use this feature on the AirWave side, enable certificate-based login. For information on how to enable certificate-based login, see PSK-Based and Certificate-Based Authentication (see Page 385).

Standard DHCP Options 60 and 43 on Windows Server 2008

In networks that are not using DHCP options 60 and 43, it is easy to use the standard DHCP options 60 and 43 for an AP or AP. For APs, these options can be used to indicate the master controller or the local controller. For APs, these options can be used to define the AirWave IP, group, password, and domain name.

1. From a server running Windows Server 2008, navigate to **Server Manager > Roles > DHCP sever > domain > DHCP Server > IPv4**.
2. Right-click **IPv4** and select **Set Predefined Options**
3. Select **DHCP Standard Options** in the **Option class** drop-down list and then click **Add**.
4. Enter the following information:
   - Name— SCALANCE W
   - Data Type—String
   - Code—60
   - Description—AP
5. Navigate to **Server Manager** and select **Server Options** in the **IPv4** window. This sets the value globally. Use options on a per-scope basis to override the global options.
6. Right-click **Server Options** and select the configuration options
7. Select **060 Aruba AP** in the **Server Options** window and enter **SCALANCEWAP** in the **String value** text box.
8. Select **043 Vendor Specific Info** and enter a value for either of the following in the ASCII text box:
   - **airwave-orgn, airwave-ip, airwave-key**; for example:Siemens,192.0.2.20, 12344567
   - **airwave-orgn, airwave-domain**; for example:Siemens, support.industry.siemens.com

This creates DHCP options 60 and 43 on a global basis. You can do the same on a per-scope basis. The per- scope option overrides the global option.

28.3 Alternate Method for Defining Vendor Specific DHCP Options

This section describes how to add vendor-specific DHCP options for APs in a network that already uses DHCP options 60 and 43 for other services. Some networks use DHCP standard options 60 and 43 to provide the DHCP clients information about certain services such as PXE. In such an environment, the standard DHCP options 60 and 43 cannot be used for APs.

This method describes how to set up a DHCP server to send option 43 with AirWave information to the AP. This section assumes that option 43 is sent per scope, because option 60 is being shared by other devices as well.

Note

The DHCP scope must be specific to SCALANCE W, and the PXE devices that use options 60 and 43 must not connect to the subnet defined by this scope. This is because you can specify only one option 43 for a scope, and if other devices that use option 43 connect to this subnet, they are presented with the information specific to the AP.

1. In Windows Server 2008, navigate to **Server Manager > Roles > DHCP Server > Domain DHCP Server**
2. Select a scope [subnet]. Scope [10.169.145.0]145 is selected in the example shown in the figure below.
3. Right-click and select **Advanced,** and then specify the following options:
   – Vendor class — DHCP Standard Options
   – User class — Default User Class
   – Available options — Select 043 Vendor-Specific Info
   – String Value —SCALANCE W AP, tme-store4, 10.169.240.8, Siemens123 (which is the AP description, organization string, AirWave IP address or domain name, Pre-shared key, for AirWave)

Upon completion, the AP shows up as a new device in AirWave, and a new group called **tme-store4** is created. Navigate to **APs/Devices > New > Group** to view this group.

28.4 Web Socket Connection

WebSocket is a protocol based on which the virtual controllers and the slave APs can establish and maintain a connection with the AirWave servers. A WebSocket support is more efficient because the server does not depend on a client request to respond to an AP. When a WebSocket connection is established, all the access points including virtual controllers and slaves can communicate with the server at any time. Virtual controllers can communicate with the AirWave management server. Slave APs can communicate with application level components.

A new WebSocket capable AP connects to a server through the HTTPS post. If a server supports WebSocket, it will send an HTTP redirect message to the AP. The AP closes the existing HTTPS connection and connects to the server through WebSocket. If the server does not support WebSocket, it will ignore the header and APs will continue using HTTPS and XML to communicate with the server.

In the CLI:

To view the websocket status between APs and AirWave:

```
(AP)# show ap debug airwave
```

Uplink Configuration 29

29.1 Uplink Interfaces

SCALANCE W network supports Ethernet, 3G and 4G USB modems, and the Wi-Fi uplink to provide access to the corporate SCALANCE W network. The 3G/4G USB modems and the Wi-Fi uplink can be used to extend the connectivity to places where an Ethernet uplink cannot be configured. It also provides a reliable backup link for the Ethernet-based SCALANCE W network.

The following types of uplinks are supported on SCALANCE W:

- Ethernet Uplink (Page 396)
- Cellular Uplink (Page 398)
- Wi-Fi Uplink (Page 400)

29.2 Ethernet Uplink

The Eth0 port on an AP is enabled as an uplink port by default. You can view the type of uplink and the status of uplink of an AP in the **Info** tab on selecting a client.

Ethernet uplink supports the following types of configuration:

- Pepo
- DHCP
- Static IP

You can use PPPoE for your uplink connectivity in both AP and AP-VPN deployments. PPPoE is supported only in a single AP deployment.

Note

Uplink redundancy with the PPPoE link is not supported.

When the Ethernet link is up, it is used as a PPPoE or DHCP uplink. After the PPPoE settings are configured, PPPoE has the highest priority for the uplink connections. The AP can establish a PPPoE session with a PPPoE server at the ISP and get authenticated using PAP or CHAP. Depending upon the request from the PPPoE server, either the PAP or the CHAP credentials are used for authentication. After configuring PPPoE, reboot the AP for the configuration to take effect. The PPPoE connection is dialed after the AP comes up. The PPPoE configuration is checked during AP boot and if the configuration is correct, Ethernet is used for the uplink connection.

Note

When PPPoE is used, do not configure Dynamic RADIUS Proxy and IP address of the virtual controller. An SSID created with default VLAN is not supported with PPPoE uplink.

You can also configure an alternate Ethernet uplink to enable uplink failover when an Ethernet port fails.

Configuring PPPoE Uplink Profile

You can configure PPPoE settings from the SCALANCE W UI or the CLI.

In the SCALANCE W UI

Configuring PPPoE settings:

1. Click the **System** link on the SCALANCE W main window.
2. In the **System** section, click the **Show advanced options** link.

3. Perform the following steps in the **PPPoE** section in the **Uplink** tab:
   – Enter the PPPoE service name provided by your service provider in the **Service name** text box.
   – Enter the secret key used for CHAP authentication in the **CHAP secret** and **Retype** text boxes. You can use a maximum of 34 characters for the CHAP secret key.
   – Enter the username for the PPPoE connection in the **User** text box.
   – Enter a password for the PPPoE connection and confirm the password in the **Password** and **Retype text boxes.**
4. Select a value from the **Local interface** drop-down list to set a local interface for the PPPoE uplink connections. The selected DHCP scope will be used as a local interface on the PPPoE interface and the Local, L3 DHCP gateway IP address as its local IP address. When configured, the local interface acts as an unnumbered PPPoE interface and allows the entire Local, L3 DHCP subnet to be allocated to clients.

Note

The options in the **Local interface** drop-down list are displayed only if a Local, L3 DHCP scope is configured on the AP.

5. Click **OK**.
6. Reboot the AP for the configuration to take effect.

In the CLI

To configure a PPPoE uplink connection:

```
(AP)(config) # pppoe-uplink-profile

(AP)(pppoe-uplink-profile)# pppoe-svcname <service-name>

(AP)(pppoe-uplink-profile)# pppoe-username <username>

(AP)(pppoe-uplink-profile)# pppoe-passwd <password>

(AP)(pppoe-uplink-profile)# pppoe-chapsecret <password>

(AP)(pppoe-uplink-profile)# pppoe-unnumbered-local-l3-dhcp-profile <dhcp-profile>
```

To view the PPPoE configuration:

```
(AP)# show pppoe config
PPPoE Configuration
-------------------
Type Value
---- -----
User testUser
Password 3c28ec1b82d3eef0e65371da2f39c4d49803e5b2bc88be0c
Service name internet03
CHAP secret 8e87644deda9364100719e017f88ebce
Unnumbered dhcp profile dhcpProfile1
```

To view the PPPoE status:

```
(AP)# show pppoe status

pppoe uplink state:Suppressed.
```

29.3 Cellular Uplink

SCALANCE W supports the use of 3G and 4G USB modems to provide the Internet backhaul to an SCALANCE W network. The 3G or 4G USB modems can be used to extend client connectivity to places where an Ethernet uplink cannot be configured. This enables the APs to automatically choose the available network in a specific region.

Note

RAP-155/155P devices do not support the high-speed option (HSO) module.

Note

When UML290 runs in auto-detect mode, the modem can switch from 4G network to 3G network or vice-versa based on the signal strength. To configure the UML290 for the 3G network only, manually set the USB type to **pantech-3g**.

To configure the UML290 for the 4G network only, manually set the 4G USB type to **pantech-lte**.

Configuring Cellular Uplink Profiles

You can configure 3G or 4G uplinks by using the SCALANCE W UI or the CLI.

In the SCALANCE W UI

To configure 3G/4G uplinks:

1. Click the **System** link on the SCALANCE W main window.
2. In the **System** window, click the **show advanced settings** link.
3. Click the **Uplink** tab.
4. To configure a 3G or 4G uplink, select the **Country** and **ISP**.
5. Click **OK**.
6. Reboot the AP for changes to take effect.

In the CLI

To configure 3G/4G uplink manually:

```
(AP)(config) # cellular-uplink-profile

(AP)(cellular-uplink-profile)# usb-type <3G-usb-type>

(AP)(cellular-uplink-profile)# 4g-usb-type <4g-usb>

(AP)(cellular-uplink-profile)# modem-country <country>

(AP)(cellular-uplink-profile)# modem-isp <service-provider-name>

(AP)(cellular-uplink-profile)# usb-auth-type <usb-authentication_type>

(AP)(cellular-uplink-profile)# usb-user <username>

(AP)(cellular-uplink-profile)# usb-passwd <password>

(AP)(cellular-uplink-profile)# usb-dev <device-ID>
```

```
(AP)(cellular-uplink-profile)# usb-tty <tty-port>
```

```
(AP)(cellular-uplink-profile)# usb-init <Initialization-parameter>
```

```
(AP)(cellular-uplink-profile)# usb-dial <dial-parameter>
```

```
(AP)(cellular-uplink-profile)# usb-modeswitch <usb-modem>
```

To switch a modem from the storage mode to modem mode:

```
(AP)(cellular-uplink-profile)# usb-modeswitch <usb-modem>
```

To view the cellular configuration:

```
(AP)# show cellular config
```

Managing Cellular SIM PIN

APs now support the SIM PIN management functions such as locking, unlocking, and renewing the SIM PIN of the 3G/4G modems. In the current release, these functions can be configured only through the AP CLI.

To prevent any fraudulent use of 3G/4G modems connected to an AP, you can enable locking of the SIM PIN of the modems. When enabled, if an incorrect PIN code is provided in the three consecutive attempts, the SIM PIN is locked. To unlock the PIN, the users must use the Personal Unblocking Code code provided by your ISP.

Note

After enabling SIM PIN lock, reboot the AP to apply the SIM PIN lock configuration changes.

To enable SIM PIN lock:

```
(AP)# pin-enable <pin_current_used>
```

To disable SIM PIN locking:

```
(AP)# no pin-enable <pin_current_used>
```

To unlock a PIN with the PUK code provided by the operator:

```
(AP)# pin-puk <pin_puk> <pin_new>
```

To renew the PIN:

```
(AP)# pin-renew <pin_current> <pin_new>
```

29.4 Wi-Fi Uplink

Generally only the master AP uses this Wi-Fi. The Wi-Fi allows uplink to open, PSK-CCMP, and PSK-TKIP SSIDs.

- For single-radio APs, the radio serves wireless clients and the Wi-Fi uplink.
- For dual-radio APs, both radios can be used to serve clients but only one of them can be used for the Wi-Fi uplink.

Note

When the Wi-Fi uplink is in use, the client IP is assigned by the internal DHCP server.

Configuring a Wi-Fi Uplink Profile

The following configuration conditions apply to the Wi-Fi uplink:

- To bind or unbind the Wi-Fi uplink on the 5 GHz band, reboot the AP.
- If the Wi-Fi uplink is used on the 5 GHz band, mesh is disabled. The two links are mutually exclusive.

In the SCALANCE W UI

To provision an AP with the Wi-Fi uplink:

1. If you are configuring a Wi-Fi uplink after restoring factory settings on an AP, connect the AP to an Ethernet cable to allow the AP to get the IP address. Otherwise, go to step 2.
2. Click the **System** link on the SCALANCE W main window.
3. In the **System** section, click the **Show advanced options** link. The advanced options are displayed.
4. Click the **Uplink** tab.
5. Under **Wi-Fi**, enter the name of the wireless network that is used for the Wi-Fi uplink in the **Name (SSID)** text box.
6. Select the type of key for uplink encryption and authentication from the **Key management** drop-down list. If the uplink wireless router uses mixed encryption, WPA-2 is recommended for the Wi-Fi uplink.
7. Select the band in which the virtual controller currently operates, from the **band** drop-down list. The following options are available:
   - 2.4 GHz (default)
   - 5 GHz

8. Select a passphrase format from the **Passphrase format** drop-down list. The following options are available:
   - 8–63 alphanumeric characters
   - 64 hexadecimal characters

Note

Ensure that the hexadecimal password string is exactly 64 digits in length.

9. Enter a PSK passphrase in the **Passphrase** text box and click **OK.**
10. Navigate to **System > General > Show Advanced Options** view and set the **Extended SSID** parameter to **Disabled**.
11. Reboot the AP to apply the changes. After the AP reboot, the Wi-Fi and mesh links are automatically enabled.

In the CLI

To configure Wi-Fi uplink on an AP:

```
(AP)(config) # wlan sta-profile

(AP)(sta uplink)# cipher-suite<clear | wpa-tkip-psk | wpa2-ccmp-psk>

(AP)(sta uplink)# essid <essid>

(AP)(sta uplink)# uplink-band <band>

(AP)(sta uplink)# wpa-passphrase <key>
```

To view the W-Fi uplink status in the CLI:

```
(AP)# show wifi-uplink status

configured :NO
```

To view the configuration status in the CLI:

```
(AP)# show wifi-uplink config

ESSID :

Cipher Suite :

Passphrase :

Band :

(AP)# show wifi-uplink auth log

----------------------------------------------------------------------

wifi uplink auth configuration:

----------------------------------------------------------------------

----------------------------------------------------------------------

wifi uplink auth log:

----------------------------------------------------------------------

[1116]2000-01-01 00:00:45.625: Global control interface '/tmp/supp_gbl'
```

29.5 Uplink Preferences and Switching

29.5.1 Enforcing Uplinks

The following configuration conditions apply to the uplink enforcement:

- When an uplink is enforced, the AP uses the specified uplink as the primary uplink regardless of uplink preemption configuration and the current uplink status.
- When an uplink is enforced and multiple Ethernet ports are configured ,and if the uplink is enabled on the wired profiles, the AP tries to find an alternate Ethernet link based on the priority configured.
- When no uplink is enforced and preemption is not enabled, and if the current uplink fails, the AP tries to find an available uplink based on the priority configured. The uplink with the highest priority is used as the primary uplink. For example, if Wi-Fi-sta has the highest priority, it is used as the primary uplink.
- When no uplink is enforced and preemption is enabled, and if the current uplink fails, the AP tries to find an available uplink based on the priority configured. If current uplink is active, the AP periodically tries to use a higher-priority uplink and switches to the higher-priority uplink even if the current uplink is active.

You can enforce a specific uplink on an AP by using the SCALANCE W UI or the CLI.

In the SCALANCE W UI

To enforce an uplink:

1. Click the **System > show advanced settings > Uplink**. The **Uplink** tab contents are displayed.
2. Under **Management**, select the type of uplink from the **Enforce Uplink** drop-down list. If Ethernet uplink is selected, the **Port** text box is displayed.
3. Specify the Ethernet interface port number.
4. Click **OK**. The selected uplink is enforced on the AP.

In the CLI

To enforce an uplink:

```
(AP)(config)# uplink

(AP)(uplink)# enforce {cellular|ethernet | wifi | none}
```

29.5.2 Setting an Uplink Priority

You can set an uplink priority by using the SCALANCE W UI or the CLI.

In the SCALANCE W UI

Setting an uplink priority:

1. Click **System > show advanced settings > Uplink** .
2. Under **Uplink Priority List**, select the uplink, and click the icons in the **Uplink Priority List** section, to increase or decrease the priority. By default, the Eth0 uplink is set as a high-priority uplink.
3. Click **OK**. The selected uplink is prioritized over other uplinks.

In the CLI

Setting an uplink priority:

```
(AP)(config)# uplink
```

```
(AP)(uplink)# uplink-priority {cellular <priority> | ethernet <priority> | [port
<Interface-number> <priority>] | wifi <priority>}
```

Setting an Ethernet uplink priority :

```
(AP)(uplink)# uplink-priority ethernet port 0 1
```

29.5.3 Enabling Uplink Preemption

The following configuration conditions apply to uplink preemption:

- Preemption can be enabled only when no uplink is enforced.
- When preemption is disabled and the current uplink goes down, the AP tries to find an available uplink based on the uplink priority configuration.
- When preemption is enabled and if the current uplink is active, the AP periodically tries to use a higher-priority uplink, and switches to a higher-priority uplink even if the current uplink is active.

You can enable uplink preemption by using SCALANCE W UI or the CLI.

In the SCALANCE W UI

To enable uplink preemption:

1. Click **System > show advanced settings > Uplink**. The **Uplink** tab contents are displayed.
2. Under **Management**, ensure that the **Enforce Uplink** is set to none.
3. Select **Enabled** from the **Pre-emption** drop-down list.
4. Click **OK**.

In the CLI

To configure uplink preemption:

```
(AP)(config)# uplink
```

```
(AP)(uplink)# preemption
```

29.5.4 Switching Uplinks Based on VPN and Internet Availability

The default priority for uplink switchover is Ethernet and then 3G/4G. The AP can switch to the lower- priority uplink if the current uplink is down.

Switching Uplinks Based on VPN Status

SCALANCE W supports switching uplinks based on the VPN status when deploying multiple uplinks (Ethernet, 3G/4G, and Wi-Fi). When VPN is used with multiple backhaul options, the AP switches to an uplink connection based on the VPN connection status, instead of only using the Ethernet or the physical backhaul link.

The following configuration conditions apply to uplink switching:

- If the current uplink is Ethernet and the VPN connection is down, the AP tries to reconnect to VPN. The retry time depends on the fast failover configuration and the primary or backup VPN tunnel. If this fails, the AP waits for the VPN failover timeout and selects a different uplink such as 3G/4G or Wi-Fi.
- If the current uplink is 3G or Wi-Fi, and Ethernet has a physical link, the AP periodically suspends user traffic to try and connect to the VPN on the Ethernet. If the AP succeeds, the AP switches to Ethernet. If the AP does not succeed, it restores the VPN connection to the current uplink.

Uplink switching based on VPN status is automatically enabled if VPN is configured on the AP. However, you can specify the duration in the **VPN failover timeout** text box to wait for an uplink switch. By default, this duration is set to 180 seconds. The AP monitors the VPN status and when the VPN connection is not available for 3 minutes, the uplink switches to another available connection (if a low-priority uplink is detected and the uplink preference is set to none). When **VPN failover timeout** is set to 0, uplink does not switch over.

When uplink switching based on the Internet availability is enabled, the uplink switching based on VPN failover is automatically disabled.

Switching Uplinks Based on Internet Availability

You can configure SCALANCE W to switch uplinks based on Internet availability.

When the uplink switchover based on Internet availability is enabled, the AP continuously sends Internet Control Management Protocol packets to some well-known Internet servers. If the request is timed out due to a bad uplink connection or uplink interface failure, and the public Internet is not reachable from the current uplink, the AP switches to a different connection.

You can set preferences for uplink switching by using the SCALANCE W UI and the CLI.

In the SCALANCE W UI

To configure uplink switching:

1. Click **System > show advanced settings > Uplink**. The **Uplink** tab contents are displayed.
2. Under **Management**, configure the following parameters:

   VPN failover timeout — To configure uplink switching based on VPN status, specify the duration to wait for an uplink switch. The default duration is set to 180 seconds.

   Internet failover — To configure uplink switching based on Internet availability, perform the following steps:

   – Select **Enabled** from the **Internet failover** drop-down list.

   – Specify the required values for the following parameters:
   Max allowed test packet loss
   The maximum number of ICMP test packets that are allowed to be lost to determine if the AP must switch to a different uplink connection. You can specify a value within the range of 1 – 1000.
   Secs between test packets
   The frequency at which ICMP test packets are sent. You can specify a value within the range of 1 – 3600 seconds.
   Internet check timeout
   Internet check timeout is the duration for the test packet timeout. You can specify a value within the range of 0–3600 seconds and the default value is 10 seconds.

   – **Internet failover IP** — To configure an IP address to which the AP must send AP packets and verify if the Internet is reachable when the uplink is down. By default, the master AP sends the ICMP packets to 8.8.8.8 IP address only if the out-of-service operation based on Internet availability (internet-down state) is configured on the SSID.
3. Click **OK**.

Note

When **Internet failover** is enabled, the AP ignores the VPN status, although uplink switching based on VPN status is enabled.

In the CLI

To enable uplink switching based on VPN status:

```
(AP)(config)# uplink

(AP)(uplink)# failover-vpn-timeout <seconds>
```

To enable uplink switching based on Internet availability:

```
(AP)(config)# uplink

(AP)(uplink)# failover-internet

(AP)(uplink)# failover-internet-ip <ip>

(AP)(uplink)# failover-internet-pkt-lost-cnt <count>

(AP)(uplink)# failover-internet-pkt-send-freq <frequency>
```

29.5.5 Viewing Uplink Status and Configuration

To view the uplink status:

```
(AP)# show uplink status

Uplink preemption :enable

Uplink preemption interval 600

Uplink enforce :none

Ethernet uplink eth0 :DHCP

Uplink Table

Type State Priority In Use

---- ----- -------- ------

eth0 UP 2 Yes

Wifi-sta INIT 1 No

3G/4G INIT 3 No

Internet failover :enable

Internet failover IP :192.2.0.1

Max allowed test packet loss :10

Secs between test packets 30

VPN failover timeout (secs) 180

Internet check timeout (secs) 10

ICMP pkt sent 1

ICMP pkt lost 1

Continuous pkt lost 1

VPN down time 0

AP1X type :NONE

Certification type :NONE

Validate server :NONE
```

To view the uplink configuration in the CLI:

```
(AP)# show uplink config
Uplink preemption :enable
Uplink preemption interval 600
Uplink enforce :none
Ethernet uplink eth0 :DHCP
Internet failover :disable
Max allowed test packet loss 10
Secs between test packets 30
VPN failover timeout (secs) 180
Internet check timeout (secs) 10
Secs between test packets 30
```

Intrusion Detection 30

The IDS is a feature that monitors the network for the presence of unauthorized APs and clients. It also logs information about the unauthorized APs and clients, and generates reports based on the logged information.

The IDS feature in the network enables you to detect rogue APs, interfering APs, and other devices that can potentially disrupt network operations.

- Detecting and Classifying Rogue APs
- OS Fingerprinting
- Configuring Wireless Intrusion Protection and Detection Levels
- Configuring IDS

30.1 Detecting and Classifying Rouge APs

A rogue AP is an unauthorized AP plugged into the wired side of the network.

An interfering AP is an AP seen in the RF environment but it is not connected to the wired network. While the interfering AP can potentially cause RF interference, it is not considered a direct security threat, because it is not connected to the wired network. However, an interfering AP may be reclassified as a rogue AP.

To detect the rogue APs, click the **IDS** link in the SCALANCE W main window. The built-in IDS scans for access points that are not controlled by the virtual controller. These are listed and classified as either Interfering or Rogue, depending on whether they are on a foreign network or your network.

30.2 OS Fingerprinting

The OS Fingerprinting feature gathers information about the client that is connected to the SCALANCE W network to find the operating system that the client is running on. The following is a list of advantages of this feature:

- Identifying rogue clients—Helps to identify clients that are running on forbidden operating systems.
- Identifying outdated operating systems—Helps to locate outdated and unexpected OS in the company network.
- Locating and patching vulnerable operating systems—Assists in locating and patching specific operating system versions on the network that have known vulnerabilities, thereby securing the company network.

OS Fingerprinting is enabled in the SCALANCE W network by default. The following operating systems are identified by SCALANCE W:

- Windows 7
- Windows Vista n Windows Server n Windows XP
- Windows ME
- OS-X
- iPhone
- iOS
- Android
- Blackberry
- Linux

30.3 Configuring Wireless Intrusion Protection and Detection Levels

WIP offers a wide selection of intrusion detection and protection features to protect the network against wireless threats.

Like most other security-related features of the SCALANCE W network, the WIP can be configured on the AP. You can configure the following options:

- **Infrastructure Detection Policies**—Specifies the policy for detecting wireless attacks on access points.
- **Client Detection Policies**—Specifies the policy for detecting wireless attacks on clients.
- **Infrastructure Protection Policies**—Specifies the policy for protecting access points from wireless attacks.
- **Client Protection Policies**—Specifies the policy for protecting clients from wireless attacks.
- **Containment Methods**—Prevents unauthorized stations from connecting to your SCALANCE W network.

Each of these options contains several default levels that enable different sets of policies. An administrator can customize, enable, or disable these options accordingly.

The detection levels can be configured using the **IDS** window. To view the IDS window, click **More > IDS** link on the SCALANCE W main window.

The following levels of detection can be configured in the WIP Detection page:

- Off
- Low
- Medium
- High

The following table describes the detection policies enabled in the Infrastructure Detection **Custom settings** text box:

Table 30- 1 Infrastructure Detection Policies

Detection Level	Detection Policy
Off	Rogue Classification
Low	• Detect AP Spoofing • Detect Windows Bridge • IDS Signature — Deauthentication Broadcast • IDS Signature — Deassociation Broadcast

Detection Level	Detection Policy
Medium	• Detect ad hoc networks using VALID SSID — Valid SSID list is autoconfigured based on SCALANCE W AP configuration • Detect Malformed Frame — Large Duration
High	• Detect AP Impersonation • Detect ad hoc Networks • Detect Valid SSID Misuse • Detect Wireless Bridge • Detect 802.11 40 MHz intolerance settings • Detect Active 802.11n Greenfield Mode • Detect AP Flood Attack • Detect Client Flood Attack • Detect Bad WEP • Detect CTS Rate Anomaly • Detect RTS Rate Anomaly • Detect Invalid Address Combination • Detect Malformed Frame — HT IE • Detect Malformed Frame — Association Request • Detect Malformed Frame — Auth • Detect Overflow IE • Detect Overflow EAPOL Key • Detect Beacon Wrong Channel • Detect devices with invalid MAC OUI

The following table describes the detection policies enabled in the Client Detection **Custom settings** text box.

Table 30- 2 Client Detection Policies

Detection Level	Detection Policy
Off	All detection policies are disabled.
Low	• Detect Valid Station Misassociation
Medium	• Detect Disconnect Station Attack • Detect Omerta Attack • Detect FATA-Jack Attack • Detect Block ACK DOS • Detect Hotspotter Attack • Detect unencrypted Valid Client • Detect Power Save DOS Attack
High	• Detect EAP Rate Anomaly • Detect Rate Anomaly • Detect Chop Chop Attack • Detect TKIP Replay Attack • IDS Signature — Air Jack • IDS Signature — ASLEAP

The following levels of detection can be configured in the WIP Protection page:

- Off
- Low
- High

The following table describes the protection policies that are enabled in the Infrastructure Protection **Custom settings** text box:

Table 30- 3 Infrastructure Protection Policies

Protection Level	Protection Policy
Off	All protection policies are disabled
Low	• Protect SSID—Valid SSID list should be auto- derived from SCALANCE W configuration • Rogue Containment
High	• Protect from ad hoc Networks • Protect AP Impersonation

The following table describes the detection policies that are enabled in the Client Protection **Custom settings** text box:

Table 30- 4 Client Protection Policies

Protection Level	**Protection Policy**
Off	All protection policies are disabled
Low	Protect Valid Station
High	Protect Windows Bridge

Containment Methods

You can enable wired and wireless containments to prevent unauthorized stations from connecting to your SCALANCE W network.

SCALANCE W supports the following types of containment mechanisms:

- Wired containment—When enabled, APs generate ARP packets on the wired network to contain wireless attacks.
  - wired-containment-ap-adj-mac—Enables a wired containment to Rogue APs whose wired interface MAC address is offset by one from its BSSID.
  - wired-containment-susp-l3-rogue—Enables the users to identify and contain an AP with a preset MAC address that is different from the BSSID of the AP, if the MAC address that the AP provides is offset by one character from its wired MAC address.

Note

Enable the **wired-containment-susp-l3-rogue** parameter only when a specific containment is required, to avoid a false alarm.

- Wireless containment—When enabled, the system attempts to disconnect all clients that are connected or attempting to connect to the identified Access Point.
  - None—Disables all the containment mechanisms.
  - Deauthenticate only—With deauthentication containment, the Access Point or client is contained by disrupting the client association on the wireless interface.
  - Tarpit containment—With Tarpit containment, the Access Point is contained by luring clients that are attempting to associate with it to a tarpit. The tarpit can be on the same channel or a different channel as the Access Point being contained

30.4 Configuring IDS

The IDS policy for APs can be created using the CLI.

To configure IDS using CLI:

```
(AP)(config)# ids

(AP)(IDS)# infrastructure-detection-level <type>

(AP)(IDS)# client-detection-level <type>

(AP)(IDS)# infrastructure-protection-level <type>

(AP)(IDS)# client-protection-level <type>

(AP)(IDS)# wireless-containment <type>

(AP)(IDS)# wired-containment

(AP)(IDS)# wired-containment-ap-adj-mac

(AP)(IDS)# wired-containment-susp-l3-rogue

(AP)(IDS)# detect-ap-spoofing

(AP)(IDS)# detect-windows-bridge

(AP)(IDS)# signature-deauth-broadcast

(AP)(IDS)# signature-deassociation-broadcast

(AP)(IDS)# detect-adhoc-using-valid-ssid

(AP)(IDS)# detect-malformed-large-duration

(AP)(IDS)# detect-ap-impersonation

(AP)(IDS)# detect-adhoc-network

(AP)(IDS)# detect-valid-ssid-misuse

(AP)(IDS)# detect-wireless-bridge

(AP)(IDS)# detect-ht-40mhz-intolerance

(AP)(IDS)# detect-ht-greenfield

(AP)(IDS)# detect-ap-flood

(AP)(IDS)# detect-client-flood

(AP)(IDS)# detect-bad-wep

(AP)(IDS)# detect-cts-rate-anomaly

(AP)(IDS)# detect-rts-rate-anomaly

(AP)(IDS)# detect-invalid-addresscombination

(AP)(IDS)# detect-malformed-htie

(AP)(IDS)# detect-malformed-assoc-req

(AP)(IDS)# detect-malformed-frame-auth

(AP)(IDS)# detect-overflow-ie

(AP)(IDS)# detect-overflow-eapol-key
```

```
(AP)(IDS)# detect-beacon-wrong-channel

(AP)(IDS)# detect-invalid-mac-oui

(AP)(IDS)# detect-valid-clientmisassociation

(AP)(IDS)# detect-disconnect-sta

(AP)(IDS)# detect-omerta-attack

(AP)(IDS)# detect-fatajack

(AP)(IDS)# detect-block-ack-attack

(AP)(IDS)# detect-hotspotter-attack

(AP)(IDS)# detect-unencrypted-valid

(AP)(IDS)# detect-power-save-dos-attack

(AP)(IDS)# detect-eap-rate-anomaly

(AP)(IDS)# detect-rate-anomalies

(AP)(IDS)# detect-chopchop-attack

(AP)(IDS)# detect-tkip-replay-attack

(AP)(IDS)# signature-airjack

(AP)(IDS)# signature-asleap

(AP)(IDS)# protect-ssid

(AP)(IDS)# rogue-containment

(AP)(IDS)# protect-adhoc-network

(AP)(IDS)# protect-ap-impersonation

(AP)(IDS)# protect-valid-sta

(AP)(IDS)# protect-windows-bridge
```

Mesh AP Configuration 31

31.1 Mesh Network Overview

The SCALANCE W secure enterprise mesh solution is an effective way to expand network coverage for outdoor and indoor enterprise environments without any wires. As traffic traverses across mesh APs, the mesh network automatically reconfigures around broken or blocked paths. This self-healing feature provides increased reliability and redundancy and allows the network to continue operation even when an AP stops functioning or if a connection fails.

Mesh APs

Mesh network requires at least one valid uplink (wired or 3G) connection. Any provisioned AP that has a valid uplink (wired or 3G) functions as a mesh portal, and the AP without an Ethernet link functions as a mesh point. The mesh portal can also act as a virtual controller. Mesh portals and mesh points are also known as mesh nodes, a generic term used to describe APs configured for mesh.

If two APs have valid uplink connections, there is redundancy in the mesh network, and most mesh points try to mesh directly with one of the two portals. However, depending on the actual deployment and RF environment, some mesh points may mesh through other intermediate mesh points.

In an SCALANCE W mesh network, the maximum hop count is two nodes (point > point > portal) and the maximum number of mesh points per mesh portal is eight.

Mesh APs detect the environment when they boot up, locate and associate with their nearest neighbor, to determine the best path to the mesh portal.

SCALANCE W mesh functionality is supported only on dual-radio APs. On dual-radio APs, the 2.4 GHz radio is always used for client traffic, while the 5 GHz radio is always used for both mesh-backhaul and client traffic.

Note

Mesh service is automatically enabled on 802.11a band for dual-radio AP only, and this is not configurable.

For AP-RW variants, the mesh network must be provisioned for the first time by plugging into the wired network. After that, mesh works on AP-RWs like any other regulatory domain.

Mesh Portals

A mesh portal is a gateway between the wireless mesh network and the enterprise wired LAN. The mesh roles are automatically assigned based on the AP configuration. A mesh network could have multiple mesh portals to support redundant mesh paths (mesh links between neighboring mesh points that establish the best path to the mesh portal) from the wireless mesh network to the wired LAN.

The mesh portal broadcasts a mesh services set identifier or mesh cluster name to advertise the mesh network service to other mesh points in that SCALANCE W network. This is not configurable and is transparent to the user.

The mesh points authenticate to the mesh portal and establish a link that is secured using AES encryption.

Note

The mesh portal reboots after 5 minutes when it loses its uplink connectivity to a wired network.

Mesh Points

The mesh point establishes an all-wireless path to the mesh portal. The mesh point provides traditional WLAN services such as client connectivity, IDS capabilities, user role association, and QoS for LAN-to-mesh communication to clients and performs mesh backhaul or network connectivity.

Note

A mesh point also supports LAN bridging. You can connect any wired device to the downlink port of the mesh point. In the case of single Ethernet port platforms such as AP-105, you can convert the Eth0 uplink port to a downlink port by enabling **Eth0 Bridging**. For additional information, see Configuring Wired Bridging on Ethernet 0 for Mesh Point (Page 420).

31.2 Setting up SCALANCE W Mesh Network

Starting from SCALANCE W 6.4.0.2-4.1.0.0 release, mesh functionality is disabled by default, because of which over- the-air provisioning of mesh APs is not supported.

To provision APs as mesh APs:

1. Connect the APs to a wired switch.
2. Ensure that the virtual controller key is synchronized and the country code is configured.
3. Ensure that a valid SSID is configured on the AP.
4. If the AP has a factory default SSID (SCALANCE W SSID), delete the SSID.
5. If an ESSID is enabled on the virtual controller, disable it and reboot the AP cluster.
6. Disconnect the APs that you want to deploy as mesh points from the switch, and place the APs at a remote location. The APs come up without any wired uplink connection and function as mesh points. The APs with valid uplink connections function as mesh portals.

Note

SCALANCE W does not support the topology in which the APs are connected to the downlink Ethernet port of a mesh point.

31.3 Configuring Wired Bridging on Ethernet 0 for Mesh Point

SCALANCE W supports wired bridging on the Ethernet 0 port of an AP. If AP is configured to function as a mesh point, you can configure wired bridging.

Note

Enabling wired bridging on this port of an AP makes the port available as a downlink wired bridge and allows client access through the port

Note

When using 3G uplink, the wired port will be used as downlink.

You can configure support for wired bridging on the Ethernet 0 port of an AP by using the SCALANCE W UI or the CLI.

In the SCALANCE W UI

To configure Ethernet bridging:

1. On the **Access Points** tab, click the AP to modify.
2. Click the **edit** link.
3. Click the **Uplink** tab.
4. Select **Enable** from the **Eth0 Bridging** drop-down list.
5. Click **OK**.
6. Reboot the AP.

In the CLI

To configure Ethernet bridging:

```
(AP)# enet0-bridging
```

Note

Make the necessary changes to the wired-profile when eth0 is used as the downlink port. For more information, see Configuring a Wired Profile.

Mobility and Client Management 32

32.1 Layer-3 Mobility Overview

APs form a single SCALANCE W network when they are in the same Layer-2 domain. As the number of clients increase, multiple subnets are required to avoid broadcast overhead. In such a scenario, a client must be allowed to roam away from the SCALANCE W network to which it first connected (home network) to another network supporting the same WLAN access parameters (foreign network) and continue its existing sessions.

Layer-3 mobility allows a client to roam without losing its IP address and sessions. If WLAN access parameters are the same across these networks, clients connected to APs in a given SCALANCE W network can roam to APs in a foreign SCALANCE W network and continue their existing sessions. Clients roaming across these networks are able to continue using their IP addresses after roaming. You can configure a list of virtual controller IP addresses across which Layer-3 mobility is supported.

The SCALANCE W Layer-3 mobility solution defines a Mobility Domain as a set of SCALANCE W networks, with the same WLAN access parameters, across which client roaming is supported. The SCALANCE W network to which the client first connects is called its home network. When the client roams to a foreign network, an AP in the home network (home AP) anchors all traffic to or from this client. The AP to which the client is connected in the foreign network (foreign AP) tunnels all client traffic to or from the home AP through a GRE tunnel.

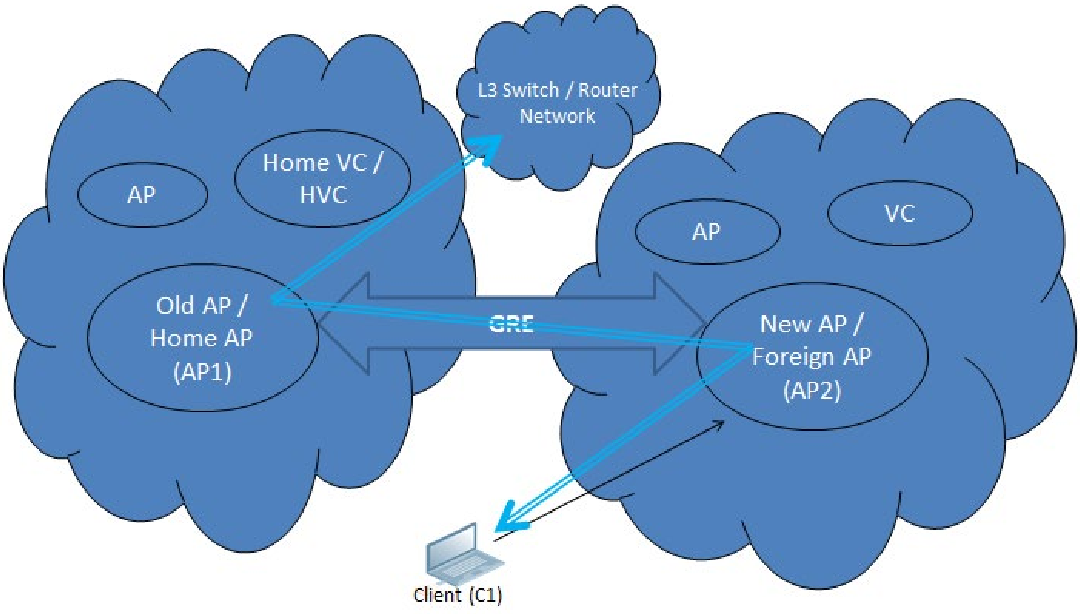


Figure 32-1 Routing of traffic when the client is away from its home network

When a client first connects to an SCALANCE W network, a message is sent to all configured virtual controller IP addresses to see if this is an Layer-3 roamed client. On receiving an acknowledgment from any of the configured virtual controller IP addresses, the client is identified as an Layer-3 roamed client. If the AP has no GRE tunnel to this home network, a new tunnel is formed to an AP (home AP) from the client's home network.

Each foreign AP has only one home AP per SCALANCE W network to avoid duplication of broadcast traffic. Separate GRE tunnels are created for each foreign AP-home AP pair. If a peer AP is a foreign AP for one client and a home AP for another, two separate GRE tunnels are used to handle Layer-3 roaming traffic between these APs.

If client subnet discovery fails on association due to some reason, the foreign AP identifies its subnet when it sends out the first Layer-3 packet. If the subnet is not a local subnet and belongs to another SCALANCE W network, the client is treated as an Layer-3 roamed client and all its traffic is forwarded to the home network through a GRE tunnel.

32.2 Configuring L3-Mobility

To configure a mobility domain, you have to specify the list of all SCALANCE W networks that form the mobility domain. To allow clients to roam seamlessly among all the APs, specify the virtual controller IP for each foreign subnet. You may include the local SCALANCE W or virtual controller IP address, so that the same configuration can be used across all SCALANCE W networks in the mobility domain.

It is recommended that you configure all client subnets in the mobility domain. When the client subnets are configured, note the following scenarios:

- If a client is from a local subnet, it is identified as a local client. When a local client starts using the IP address, Layer-3 roaming is terminated.
- If the client is from a foreign subnet, it is identified as a foreign client. When a foreign client starts using the IP address, Layer-3 roaming is set up.

Home Agent Load Balancing

Home Agent Load Balancing is required in large networks where multiple tunnels might terminate on a single border or lobby AP and overload it. When load balancing is enabled, the virtual controller assigns the home AP for roamed clients by applying a *round robin* policy. With this policy, the load for the APs acting as Home Agents for roamed clients is uniformly distributed across the AP cluster.

Configuring a Mobility Domain for SCALANCE W

You can configure Layer-3 mobility domain by using the SCALANCE W UI or the CLI.

In the SCALANCE W UI

To configure a mobility domain:

1. Click the **System** link on the SCALANCE W main window.
2. In the **Services** section, click the **Show advanced options** link.
3. Click **L3 Mobility**.

4. Select **Enabled** from the **Home agent load balancing** drop-down list. By default, home agent load balancing is disabled.
5. Click **New** in the **Virtual Controller IP Addresses** section, add the IP address of a virtual controller that is part of the mobility domain, and click **OK**.
6. Repeat Steps 2 to 5, to add the IP addresses of all virtual controller that form the Layer-3 mobility domain.
7. Click **New** in the **Subnets** section and specify the following:
   – Enter the client subnet in the **IP address** text box.
   – Enter the mask in the **Subnet mask** text box.
   – Enter the VLAN ID of the home network in the **VLAN ID** text box.
   – Enter the home virtual controller IP address for this subnet in the **Virtual controller IP** text box.
8. Click **OK**.

In the CLI

To configure a mobility domain:

```
(AP)(config)# l3-mobility

(AP)(L3-mobility)# home-agent-load-balancing

(AP)(L3-mobility)# virtual-controller <IP-address>

(AP)(L3-mobility)# subnet <IP-address> <subnet-mask> <VLAN-ID> <virtual-controller-
IP- address>
```

Spectrum Monitor 33

33.1 Understanding Spectrum Data

Wireless networks operate in environments with electrical and RF devices that can interfere with network communications. Microwave ovens, cordless phones, and even adjacent Wi-Fi networks are all potential sources of continuous or intermittent interference. The spectrum monitor software modules on APs can examine the RF environment in which the Wi-Fi network is operating, identify interference, and classify its sources. An analysis of the results can then be used to quickly isolate issues associated with packet transmission, channel quality, and traffic congestion caused by contention with other devices operating in the same band or channel.

Spectrum monitors are AP radios that gather spectrum data but do not service clients. Each SM scans and analyzes the spectrum band used by the SM's radio (2.4 GHz or 5 GHz). An AP radio in hybrid AP mode continues to serve clients as an access point while it analyzes spectrum analysis data for the channel the radio uses to serve clients. You can record data for both types of spectrum monitor devices.

However, the recorded spectrum is not reported to the virtual controller. A spectrum alert is sent to the virtual controller when a non-Wi-Fi interference device is detected.

The spectrum monitor is fully supported on all APs or Remote APs with a few exceptions:

- RAP-155 does not support Spectrum from SCALANCE W 6.3.1.1-4.0.0.0 release.
- AP-105 supports the dedicated Spectrum mode, but not the Hybrid Spectrum mode.
- Remote AP3 do not support Spectrum display in the SCALANCE W UI.

The spectrum data is collected by each AP spectrum monitor and hybrid AP. The spectrum data is not reported to the virtual controller. The **Spectrum** link is visible in the SCALANCE W UI (Access Point view) only if you have enabled the Spectrum Monitoring feature.

You can view the following spectrum data in the UI:

- Device List
- Non-Wi-Fi Interferers
- Channel Metrics
- Channel Details
- Spectrum Alerts

Device List

The device list consists of a device summary table and channel information for active non-Wi-Fi devices currently seen by a spectrum monitor or hybrid AP radio. To view the device list, click **Spectrum** in the dashboard

The following table shows the device details that are displayed.

Table 33- 1 Device Summary and Channel Information

Column	Description
Type	Device type. This parameter can be any of the following: • Audio FF (fixed frequency) • Bluetooth • Cordless base FH (frequency hopper) • Cordless phone FF (fixed frequency) • Cordless network FH (frequency hopper) • Generic FF (fixed frequency) • Generic FH (frequency hopper) • Generic interferer • Microwave • Microwave inverter • Video • Xbox **NOTE:** For additional details about non-Wi-Fi device types shown in this table, see Non-Wi-Fi Interferer Types.
ID	ID number assigned to the device by the spectrum monitor or hybrid AP radio. Spectrum monitors and hybrid APs assign a unique spectrum ID per device type.
Cfreq	Center frequency of the signal sent from the device.
Bandwidth	Channel bandwidth used by the device.
Channels-affected	Radio channels affected by the wireless device.
Signal-strength	Strength of the signal sent from the device, represented in dBm.
Duty-cycle	Device duty cycle. This value represents the percent of time the device broadcasts a signal.
Add-time	Time at which the device was first detected.
Update-time	Time at which the device’s status was updated.

Non-Wi-Fi Interferers

The following table describes each type of non-Wi-Fi interferer detected by the Spectrum Monitor feature:

Table 33- 2 Non-Wi-Fi Interferer Types

Non Wi-Fi Interferer	Description
Bluetooth	Any device that uses the Bluetooth protocol to communicate in the 2.4 GHz band is classified as a *Bluetooth* device. Bluetooth uses a frequency hopping protocol.
Fixed Frequency (Audio)	Some audio devices such as wireless speakers and microphones also use fixed frequency to continuously transmit audio. These devices are classified as *Fixed Frequency (Audio)*.
Fixed Frequency (Cordless Phones)	Some cordless phones use a fixed frequency to transmit data (much like the fixed frequency video devices). These devices are classified as *Fixed Frequency (Cordless Phones)*.
Fixed Frequency (Video)	Video transmitters that continuously transmit video on a single frequency are classified as *Fixed Frequency (Video)*. These devices typically have close to a 100% duty cycle. These types of devices may be used for video surveillance, TV or other video distribution, and similar applications.
Fixed Frequency (Other)	All other fixed frequency devices that do not fall into any of the above categories are classified as *Fixed Frequency (Other)*. Note that the RF signatures of the fixed frequency audio, video, and cordless phone devices are very similar and that some of these devices may be occasionally classified as *Fixed Frequency (Other)*.
Frequency Hopper (Cordless Base)	Frequency hopping cordless phone base units transmit periodic beacon-like frames at all times. When the handsets are not transmitting (that is, when there are no active phone calls), the cordless base is classified as *Frequency Hopper (Cordless Base)*.
Frequency Hopper (Cordless Network)	When there is an active phone call and one or more handsets are part of the phone conversation, the device is classified as *Frequency Hopper (Cordless Network)*. Cordless phones may operate in 2.4 GHz or 5 GHz bands. Some phones use both 2.4 GHz and 5 GHz bands (for example, 5 GHz for Base-to-handset and 2.4 GHz for Handset-to-base). These phones may be classified as unique Frequency Hopper devices on both bands.
Frequency Hopper (Xbox)	The Microsoft Xbox device uses a frequency hopping protocol in the 2.4 GHz band. These devices are classified as *Frequency Hopper (Xbox)*.
Frequency Hopper (Other)	When the classifier detects a frequency hopper that does not fall into any of the prior categories, it is classified as *Frequency Hopper (Other)*. Some examples include IEEE 802.11 FHSS devices, game consoles, and cordless/hands-free devices that do not use one of the known cordless phone protocols.
Microwave	Common residential microwave ovens with a single magnetron are classified as a *Microwave*. These types of microwave ovens may be used in cafeterias, break rooms, dormitories, and similar environments. Some industrial, healthcare, or manufacturing environments may also have other equipment that functions like a microwave and may also be classified as a Microwave device.

Non Wi-Fi Interferer	Description
Microwave (Inverter)	Some newer-model microwave ovens have the inverter technology to control the power output and these microwave ovens may have a duty cycle close to 100%. These microwave ovens are classified as *Microwave (Inverter)*. Dual-magnetron industrial microwave ovens with higher duty cycle may also be classified as *Microwave (Inverter)*. There may be other equipment that functions like inverter microwaves in some industrial, healthcare, or manufacturing environments. Those devices may also be classified as *Microwave (Inverter)*.
Generic Interferer	Any non-frequency hopping device that does not fall into any of the prior categories described in this table is classified as a *Generic Interferer*. For example, a Microwave-like device that does not operate in the known operating frequencies used by the Microwave ovens may be classified as a *Generic Interferer*. Similarly wide-band interfering devices may be classified as *Generic Interferers*.

Channel Details

When you move the mouse over a channel, the channel details or the summary of the 2.4 GHz and 5 GHz channels as detected by a spectrum monitor are displayed. You can view the aggregate data for each channel seen by the spectrum monitor radio, including the maximum AP power, interference, and the SNIR. The SNIR is the ratio of signal strength to the combined levels of interference and noise on that channel. Spectrum monitors display spectrum data of all channels in the selected band, and hybrid APs display data for the channel they are monitoring.

Channel Details Information shows the information that you can view in the Channel Details graph.

Table 33- 3 Channel Details Information

Column	Description
Channel	An 802.11a or 802.11g radio channel.
Quality(%)	Current relative quality of the channel.
Utilization(%)	The percentage of the channel being used.
Wi-Fi (%)	The percentage of the channel currently being used by Wi-Fi devices.
Type	Device type.
Total nonwifi (%)	The percentage of the channel currently being used by non-Wi-Fi devices.
Known APs	Number of valid APs identified on the radio channel.
UnKnown APs	Number of invalid or rogue APs identified on the radio channel.
Channel Util (%)	Percentage of the channel currently in use.
Max AP Signal (dBm)	Signal strength of the AP that has the maximum signal strength on a channel.
Max Interference (dBm)	Signal strength of the non-Wi-Fi device that has the highest signal strength.
SNIR (dB)	The ratio of signal strength to the combined levels of interference and noise on that channel. This value is calculated by determining the maximum noise-floor and interference-signal levels, and then calculating how strong the desired signal is above this maximum.

Channel Metrics

The channel metrics graph displays channel quality, availability, and utilization metrics as seen by a spectrum monitor or hybrid AP. You can view the channel utilization data based on 2 GHz and 5 GHz radio channels. The percentage of each channel that is currently being used by Wi-Fi devices, and the percentage of each channel being used by non-Wi-Fi devices and 802.11 ACI. The graph shows the channel availability, the percentage of each channel that is available for use, and the current relative quality of selected channels in the

2.4 GHz or 5 GHz radio bands. To view the graphs, click **2.4 GHz** or **5 GHz** in the **Spectrum** section of the dashboard. While spectrum monitors can display data for all channels in their selected band, hybrid APs display data for a single monitored channel.

Channel Metrics shows the information displayed in the **Channel Metrics** graph.

Column	Description
Channel	A 2.4 GHz or 5 GHz radio channel.
Quality(%)	Current relative quality of selected channels in the 2.4 GHz or 5 GHz radio bands, as determined by the percentage of packet retries, the current noise floor, and the duty cycle for non-Wi-Fi devices on that channel.
Availability(%)	The percentage of the channel currently available for use.
Utilization(%)	The percentage of the channel being used.
WiFi Util(%)	The percentage of the channel currently being used by Wi-Fi devices.
Interference Util(%)	The percentage of the channel currently being used by non-Wi-Fi interference plus Wi-Fi ACI.

Spectrum Alerts

When a new non-Wi-Fi device is found, an alert is reported to the virtual controller. The spectrum alert messages include the device ID, device type, IP address of the spectrum monitor or hybrid AP, and the timestamp. The virtual controller reports the detailed device information to AMP.

33.2 Configuring Spectrum Monitors and Hybrid APs

An AP can be provisioned to function as a spectrum monitor or as a hybrid AP. The radios on groups of APs can be converted to dedicated spectrum monitors or hybrid APs through the AP group's 802.11a and 802.11g radio profiles.

Converting an AP to a Hybrid AP

You can convert all APs in an SCALANCE W network into hybrid APs by selecting the

Background Spectrum Monitoring option in the 802.11a and 802.11g radio profiles of an AP. APs in **Access** mode continue to provide normal access service to clients, while providing the additional function of monitoring RF interference. If any AP in the SCALANCE W network does not support the Spectrum Monitoring feature, that AP continues to function as a standard AP, rather than a hybrid AP. By default, the background spectrum monitoring option is disabled.

In the hybrid mode, spectrum monitoring is performed only on the home channel. In other words, if the AP-channel width is 80 MHz, spectrum monitoring is performed for 80 MHz. If the channel width is 40, spectrum monitoring is performed for 40 MHz channel. In a dedicated Air Monitor mode, APs perform spectrum monitoring on all channels.

You can convert APs in an SCALANCE W network to hybrid mode by using the SCALANCE W UI or the CLI.

In the SCALANCE W UI

To convert an AP to a hybrid AP:

1. Click the **RF** link on the SCALANCE W main window.
2. In the **RF** section, click **Show advanced options** to view the **Radio** tab.
3. To enable a spectrum monitor on the 802.11g radio band, in the 2.4 GHz radio profile, select **Enabled** from the **Background Spectrum Monitoring** drop-down list.
4. To enable a spectrum monitor on the 802.11a radio band, in the 5 GHz radio profile, select **Enabled** from the **Background Spectrum Monitoring** drop-down list.
5. Click **OK**.

In the CLI

To configure 2.4 GHz radio settings:

```
(AP)(config)# rf dot11g-radio-profile
```

```
(AP)(RF dot11g Radio Profile)# spectrum-monitor
```

To configure 5 GHz radio settings:

```
(AP)(config)# rf dot11a-radio-profile
```

```
(AP)(RF dot11a Radio Profile)# spectrum-monitor
```

Converting an AP to a Spectrum Monitor

In spectrum mode, spectrum monitoring is performed on entire bands and the AP functions as a dedicated full-spectrum RF monitor, scanning all channels to detect interference, whether from the neighboring APs or from non-Wi-Fi devices such as microwaves and cordless phones.

By default, spectrum monitoring is performed on a higher band of the 5 GHz radio.

You can configure an AP to function as a stand-alone spectrum monitor by using the SCALANCE W UI or the CLI.

In the SCALANCE W UI

To convert an AP to a spectrum monitor:

1. In the **Access Points** tab, click the AP that you want to convert to a spectrum monitor.
2. Click the **edit** link.
3. Click the **Radio** tab.
4. From the **Access Mode** drop-down list, select **Spectrum Monitor**.
5. Click **OK**.
6. Reboot the AP for the changes to take effect.
7. To enable spectrum monitoring for any other band for the 5 GHz radio:
   - Click the **RF** link on the SCALANCE W main window.
   - In the **RF** section, click **Show advanced options** to view the **Radio** tab.
   - For the 5 GHz radio, specify the spectrum band you want that radio to monitor by selecting **Lower**, **Middle**, or **Higher** from the **Standalone spectrum band** drop-down list.
   - Click **OK**.

In the CLI

To convert an AP to a spectrum monitor:

```
(AP)# wifi0-mode {<access> | <monitor> | <spectrum-monitor>}
```

```
(AP)# wifi1-mode {<access> | <monitor> | <spectrum-monitor>}
```

To enable spectrum monitoring for any other band for the 5 GHz radio:

```
(AP)(config)# rf dot11a-radio-profile
```

```
(AP)(RF dot11a Radio Profile)# spectrum-band <type>
```

To view the radio configuration:

```
(AP)# show radio config

2.4 GHz:

Legacy Mode:disable

Beacon Interval: 100

802.11d/802.11h: disable

Interference Immunity Level: 2

Channel Switch Announcement Count: 0

Channel Reuse Type: disable

Channel Reuse Threshold: 0

Background Spectrum Monitor: disable


5.0 GHz:

Legacy Mode: disable

Beacon Interval: 100

802.11d/802.11h: disable

Interference Immunity Level: 2

Channel Switch Announcement Count: 0

Channel Reuse Type: disable

Channel Reuse Threshold: 0

Background Spectrum Monitor: disable

Standalone Spectrum Band: 5ghz-upper
```

AP Maintenance 34

34.1 Backing up and Restoring AP Configuration Data

You can back up the AP configuration data and restore the configuration when required.

Viewing Current Configuration

To view the current configuration on the AP:

- In the SCALANCE W UI, navigate to **Maintenance > Configuration > Current Configuration.**
- In the CLI, enter the following command at the command prompt:

```
(AP)# show running-config
```

Backing up Configuration Data

To back up the AP configuration data:

1. Navigate to the **Maintenance > Configuration** page.
2. Click **Backup Configuration**.
3. Click **Continue** to confirm the backup. The *backup.cfg* containing the AP configuration data is saved in your local file system.
4. To view the configuration that is backed up by the AP, enter the following command at the command prompt::

```
(AP)# show backup-config
```

Restoring Configuration

To restore configuration:

1. Navigate to the **Maintenance > Configuration** page.
2. Click **Restore Configuration**.
3. Click **Browse** to browse your local system and select the configuration file.
4. Click **Restore Now**.
5. Click **Restore Configuration** to confirm restoration. The configuration is restored and the AP reboots to load the new configuration.

```
(AP)(config)# copy config tftp://x.x.x.x/confgi.cfg
```

34.2 Converting an AP to a Remote AP and Campus AP

Regulatory Domain Restrictions for AP to RAP or CAP Conversion

You can provision an AP as a Campus AP or a Remote AP in a controller-based network. Before converting an AP, ensure that there is a regulatory domain match between the AP and the controller.

Converting an AP to a Remote AP

For converting an AP to a Remote AP, the virtual controller sends the Remote AP convert command to all the other APs. The virtual controller, along with the slave APs, sets a VPN tunnel to the remote controller, and downloads the firmware through FTP. The virtual controller uses IPsec to communicate to the Mobility Controller over the Internet.

- If the AP obtains AirWave information through DHCP (Option 43 and Option 60), it establishes an HTTPS connection to the AirWave server, downloads the configuration, and operates in the AP mode.

Note

A mesh point cannot be converted to Remote AP, because mesh access points do not support VPN connection.

The following table describes the supported AP platforms and minimal SCALANCE W version required for the Campus AP or Remote AP conversion.

Table 34- 1 AP Platforms and Minimum SCALANCE W Versions for AP-to-Remote AP Conversion

AP Platform	ArubaOS Release	SCALANCE W Release
W1750D	ArubaOS 6.5.0.0 or later versions	6.5.1.0-4.3.1or later versions

To convert an AP to a Remote AP:

1. Click **Maintenance** in the SCALANCE W main window.
2. Click the **Convert** tab.
3. Select **Remote APs managed by a Mobility Controller** from the drop-down list.
4. Enter the host name or the IP address of the controller in the **Hostname or IP Address of Mobility Controller** text box. Contact your local network administrator to obtain the IP address.

   Note

   Ensure that the Mobility Controller IP address is reachable by the APs.

5. Click **Convert Now** to complete the conversion. The AP reboots and begins operating in the Remote AP mode.
6. After conversion, the AP is managed by the mobility controller.

Note

For APs to function as Remote APs, configure the AP in the Remote AP whitelist and enable the FTP service on the controller.

Note

If the VPN setup fails and an error message is displayed, click **OK**, copy the error logs, and share them with your local administrator.

Converting an AP to a Campus AP

To convert an AP to a Campus AP:

1. Click **Maintenance** in the SCALANCE W main window.
2. Click the **Convert** tab.
3. Select **Campus APs managed by a Mobility Controller** from the drop-down list.
4. Enter the host name, FQDN, or the IP address of the controller in the **Hostname or IP Address of Mobility Controller** text box. Contact your local administrator to obtain these details.
5. Click **Convert Now** to complete the conversion.

Converting an AP to Stand-Alone Mode

This feature allows you to deploy an AP as an autonomous AP, which is a separate entity from the existing virtual controller cluster in the Layer 2 domain.

When an AP is converted to function in stand-alone mode, it cannot join a cluster of APs even if the AP is in the same VLAN. If the AP is in the cluster mode, it can form a cluster with other virtual controller APs in the same VLAN.

To deploy an AP as a stand-alone or autonomous AP:

1. Click **Maintenance** in the SCALANCE W main window.
2. Click the **Convert** tab.
3. Select **Standalone AP** from the drop-down list.
4. Select the Access Point from the **Access Point to Convert** drop-down list.
5. Click **Convert Now** to complete the conversion. The AP now operates in the stand-alone mode.

Converting an AP using CLI

To convert an AP to a Remote AP or Campus AP:

```
(AP)# convert-aos-ap <mode> <controller-IP-address>
```

To convert an AP to a stand-alone AP or to provision an AP in the cluster mode:

```
(AP)# swarm-mode <mode>
```

34.3 Resetting a Remote AP or Campus AP to an AP

The reset knob located on the rear of an AP can be used to reset the AP to factory default settings.

To reset an AP, perform the following steps:

1. Turn off the AP.
2. Press and hold the reset knob using a small and narrow object such as a paperclip.
3. Turn on the AP without releasing the reset knob. The power LED flashes within 5 seconds indicating that the reset is completed.
4. Release the reset knob. The AP reboots with the factory default settings.

34.4 Rebooting the AP

If you encounter any problem with the APs, you can reboot all APs or a selected AP in a network using the SCALANCE W UI. To reboot an AP:

1. Click **Maintenance** in the SCALANCE W main window.
2. Click the **Reboot** tab.
3. In the AP list, select the AP that you want to reboot and click **Reboot selected Access Point.** To reboot all the APs in the network, click **Reboot All.**
4. The **Confirm Reboot for AP** message is displayed. Click **Reboot Now** to proceed.

   The **Reboot in Progress** message is displayed indicating that the reboot is in progress. The **Reboot Successful** message is displayed after the process is complete. If the system fails to boot, the **Unable to contact Access Points after reboot was initiated** message is displayed.
5. Click **OK.**

34.5 DRT Upgrade

The DRT upgrade feature installs and upgrades the DRT file for an AP. When new certifications are available for APs, the subsequent releases will automatically receive support for these certs. Only the newer version of the DRT file is used for an upgrade.

The DRT file is installed under the following scenarios:

AP Boot Up

The DRT information is stored at two locations, one in the image file, and another in the flash memory. Every time an AP boots up, it compares the DRT version at both the locations and uses the newer version of DRT in the flash.

Install DRT File In a Cluster

When all the APs in a cluster finish downloading the DRT table, the master AP communicates to the slave APs to upgrade the DRT file. After the slave APs upgrade the DRT file, the master AP proceeds with DRT upgrade. There is a timeout mechanism set during the download and upgrade process. When a slave AP has finished DRT downloading from the master AP, but has not received an upgrade command within 5 minutes, the slave AP will attempt to upgrade the DRT file without waiting. Similarly, if the slave AP has not finished downloading within 5 minutes, the master AP will not wait for these slaves. It will continue with the rest of the upgrade process.

The DRT version can be upgraded by using the SCALANCE W UI or CLI.

In the SCALANCE W UI:

1. Navigate to the **Maintenance** > **DRT** page.
2. To upgrade by using a DRT file, select the **DRT file** radio button.
3. To upgrade the DRT by using a web URL, select the **DRT URL** radio button.
4. Click **Upgrade Now**.

Note

If a new version of DRT is displayed in the **Automatic** section, upgrade it by clicking **Upgrade Now**.

In the CLI:

To upgrade an AP cluster with the new DRT version:

```
upgrade-drt <url>
```

To reset the DRT version on an AP:

```
reset drt
```

To view the status of DRT version on an AP:

```
show drt state
```

Monitoring Devices and Logs 35

35.1 Configuring SNMP

SNMP Parameters for AP

SCALANCE W supports SNMPv1, SNMPv2, and SNMPv3 for reporting purposes only. An AP cannot use SNMP to set values in an Aruba system.

You can configure the following parameters for an AP:

Table 35- 1 SNMP Parameters for AP

Parameter	Description
Community Strings for SNMPV1 and SNMPV2	An SNMP community string is a text string that acts as a password, and is used to authenticate messages sent between the virtual controller and the SNMP agent.
If you are using SNMPv3 to obtain values from the AP, you can configure the following parameters:	
Name	A string representing the name of the user.
Authentication Protocol	An indication of whether messages sent on behalf of this user can be authenticated, and if so, the type of authentication protocol used. This can take one of the two values: • MD5—HMAC-MD5-96 Digest Authentication Protocol • SHA—HMAC-SHA-96 Digest Authentication Protocol
Authentication protocol password	If messages sent on behalf of this user can be authenticated, a (private) authentication key is used with the authentication protocol. This is a string password for MD5 or SHA based on the conditions mentioned above.
Privacy protocol	An indication of whether messages sent on behalf of this user can be protected from disclosure, and if so, the type of privacy protocol that is used. This takes the value CBC-DES Symmetric Encryption.
Privacy protocol password	If messages sent on behalf of this user can be encrypted or decrypted with DES, the (private) privacy key with the privacy protocol is used.

Configuring SNMP

This section describes the procedure for configuring SNMPv1, SNMPv2, and SNMPv3 community strings by using the SCALANCE W UI or the CLI.

Creating Community Strings for SNMPv1 and SNMPv2 Using SCALANCE W UI

To create community strings for SNMPv1 and SNMPv2:

1. Click the **System** link on the SCALANCE W main window.
2. Click **New** under the **Community Strings for SNMPv1 and SNMPv2** box.
3. Enter the string in the **New Community String** text box.
4. Click **OK.**
5. To delete a community string, select the string, and click **Delete**.

Creating Community Strings for SNMPv3 Using SCALANCE W UI

To create community strings for SNMPv3:

1. Click the **System** link on the SCALANCE W main window.
2. In the **System** window that is displayed, click the **Monitoring** tab.
3. Click **New** under the **Users for SNMPV3** box.
4. Enter the name of the user in the **Name** text box.
5. Select the type of authentication protocol from the **Auth protocol** drop-down list.
6. Enter the authentication password in the **Password** text box and retype the password in the **Retype** text box.
7. Select the type of privacy protocol from the **Privacy protocol** drop-down list.
8. Enter the privacy protocol password in the **Password** text box and retype the password in the **Retype** text box.
9. Click **OK.**
10. To edit the details for a particular user, select the user and click **Edit**.
11. To delete a particular user, select the user and click **Delete**.

Configuring SNMP Community Strings in the CLI

To configure an SNMP engine ID and host:

```
(AP)(config)# snmp-server engine-id <engine-ID>
```

```
(AP)(config)# host <ipaddr> version {1 <name> udp-port <port>}|{2c|3 <name> [inform]
[udp-port <port>]}
```

To configure SNMPv1 and SNMPv2 community strings:

```
(AP)(config)# snmp-server community <password>
```

To configure SNMPv3 community strings:

```
(AP)(config)# snmp-server user <name> <auth-protocol> <password> <privacy-
protocol><password>
```

To view SNMP configuration:

```
(AP)# show snmp-configuration
Engine ID:D8C7C8C44298
Community Strings
-----------------
Name
----
SNMPv3 Users
------------
Name Authentication Type Encryption Type
---- ------------------- ---------------
SNMP Trap Hosts
---------------
IP Address Version Name Port Inform
-- ------- ------- ---- ---- ------
```

Configuring SNMP Traps

SCALANCE W supports the configuration of external trap receivers. Only the AP acting as the virtual controller generates traps. The traps for AP cluster are generated with virtual controller IP as the source IP, if virtual controller IP is configured. The OID of the traps is 1.3.6.1.4.1.14823.2.3.3.1.200.2.X.

You can configure SNMP traps by using the SCALANCE W UI or the CLI.

In the SCALANCE W UI

To configure an SNMP trap receiver:

1. Navigate to **System > Show advanced options > Monitoring**.
2. Under **SNMP Traps**, enter a name in the **SNMP Engine ID** text box. It indicates the name of the SNMP agent on the AP. The SNMPv3 agent has an engine ID that uniquely identifies the agent in the device and is unique to that internal network.
3. Click **New** and update the following information:
   - **IP Address**—Enter the **IP Address** of the new SNMP Trap receiver.
   - **Version**—Select the SNMP version— **v1, v2c, v3** from the drop-down list. The version specifies the format of traps generated by the access point.
   - **Community/Username**—Specify the community string for SNMPv1 and SNMPv2c traps and a username for SNMPv3 traps.
   - **Port**—Enter the port to which the traps are sent. The default value is 162.
   - **Inform**—When enabled, traps are sent as SNMP INFORM messages. It is applicable to SNMPv3 only. The default value is **Yes**.
4. Click **OK** to view the trap receiver information in the **SNMP Trap Receivers** window.

In the CLI

To configure SNMP traps:

```
(AP)(config)# snmp-server host <IP-address> {version 1 | version 2 | version 3}
<name> udp-port <port> inform
```

```
(AP)(config)# end (AP)# commit apply
```

35.2 Configuring a Syslog Server

You can specify a syslog server for sending syslog messages to the external servers by using the SCALANCE W UI or the CLI.

In the SCALANCE W UI

To configure a Syslog server and Syslog facility levels:

1. In the SCALANCE W main window, click the **System** link.
2. Click **Show advanced options** to display the advanced options.
3. Click the **Monitoring** tab.
4. In the **Syslog server** text box, enter the IP address of the server to which you want to send system logs.

   Note

   The syslog source address is sent individually by the APs in the cluster and never the virtual controller IP. Even the master AP sends the syslog source address from its actual IP address.

5. Select the required values to configure syslog facility levels. Syslog Facility is an information field associated with a syslog message. It is an application or operating system component that generates a log message. The following seven facilities are supported by Syslog:
   - **AP-Debug**—Detailed log about the AP device.
   - **Network**—Log about change of network; for example, when a new AP is added to a network.
   - **Security**—Log about network security; for example, when a client connects using wrong password.
   - **System**—Log about configuration and system status.
   - **User**—Important logs about client.
   - **User-Debug**—Detailed logs about client debugging.
   - **Wireless**—Log about radio.

The following table describes the logging levels in order of severity, from the most to the least severe.

Logging Level	Description
Emergency	Panic conditions that occur when the system becomes unusable.
Alert	Any condition requiring immediate attention and correction.
Critical	Any critical conditions such as a hard drive error.
Errors	Error conditions.
Warning	Warning messages.
Notice	Significant events of a noncritical and normal nature. The default value for all Syslog facilities.
Informational	Messages of general interest to system users.
Debug	Messages containing information useful for debugging.

6. Click **OK**.

In the CLI

To configure a syslog server:

```
(AP)(config)# syslog-server <IP-address>
```

To configure syslog facility levels:

```
(AP)(config)# syslog-level <logging-level>[ap-debug |network |security |system |user
| user-debug | wireless]
```

To view syslog logging levels:

```
(AP)# show syslog-level Logging Level

-------------

Facility Level

-------- -----

ap-debug warn

network warn

security warn

system warn

user warn user-debug warn wireless error
```

35.3 Configuring TFTP Dump Server

You can configure a TFTP server for storing core dump files by using the SCALANCE W UI or the CLI.

In the SCALANCE W UI

To configure a TFTP server:

1. In the SCALANCE W main window, click the **System** link.
2. Click **Show advanced options** to display the advanced options.
3. Click the **Monitoring** tab.
4. Enter the IP address of the TFTP server in the **TFTP Dump Server** text box.
5. Click **OK**.

In the CLI

To configure a TFTP server:

```
(AP)(config)# tftp-dump-server <IP-address>
```

35.4 Running Debug Commands

To run the debugging commands from the UI:

1. Navigate to **More > Support** on the SCALANCE W main window.
2. Select the required option from the **Command** drop-down list.
3. Select **All Access Points** or **SCALANCE W Access Point(VC)** from the **Target** drop-down list.
4. Click **Run**. When you run debug commands and click **Save**, the output of all the selected commands is displayed in a single page.

The **Support** window allows you to run commands for each access point and virtual controller in a cluster. For a complete list of commands supported in a particular release train, execute the **show support-commands** command at the AP CLI. The output of this command displays the list of support commands that you can run through the UI and the corresponding CLI commands. For more information on these commands, refer to the respective command page in the *SCALANCE W CLI Function Manual*.

```
(AP) # show support-commands

Support Commands
----------------
Description                               Command Name
-----------                               ------------
AP Tech Support Dump                      show tech-support
AP Tech Support Dump Supplemental         show tech-support supplemental
AP Provisioning Status                    show activate status
AP 3G/4G Status                           show cellular status
AP 802.1X Statistics                      show ap debug dot1x-statistics
AP Access Rule Table                      show access-rule-all
AP Inbound Firewall Rules                 show inbound-firewall-rules
AP Active                                 show aps
AP AirGroup Cache                         show airgroup cache entries
AP AirGroup CPPM Entries                  show airgroup cppm entries
AP AirGroup CPPM Servers                  show airgroup cppm server
AP AirGroup Debug Statistics              show airgroup debug statistics
AP AirGroup Servers                       show airgroup servers verbose
AP AirGroup User                          show airgroup users verbose
AP ALE Configuration                      show ale config
AP ALE Status                             show ale status
AP Allowed Channels                       show ap allowed-channels
AP Allowed MAX-EIRP                       show ap allowed-max-EIRP
AP All Supported Timezones                show clock timezone all
AP ARM Bandwidth Management               show ap arm bandwidth-management
AP ARM Channels                           show arm-channels
AP ARM Configuration                      show arm config
AP ARM History                            show ap arm history
AP ARM Neighbors                          show ap arm neighbors
AP ARM RF Summary                         show ap arm rf-summary
AP ARM Scan Times                         show ap arm scan-times
AP ARP Table                              show arp
AP Association Table                      show ap association
AP Authentication Frames                  show ap debug auth-trace-buf
AP Auth-Survivability Cache               show auth-survivability cached-info
AP Auth-Survivability Debug Log           show auth-survivability debug-log
AP BSSID Table                            show ap bss-table
AP Captive Portal Domains                 show captive-portal-domains
AP Captive Portal Auto White List         show captive-portal auto-white-list
AP Client Match Status                    show ap debug client-match
AP Client Match History                   show ap client-match-history
```

AP Client Match Action	show ap client-match-actions
AP Client Match Live	show ap client-match-live
AP Client Match Triggers	show ap client-match-triggers
AP Client Table	show ap debug client-table
AP Client View	show ap client-view
AP Country Codes	show country-codes
AP CPU Details	show cpu details
AP CPU Utilization	show cpu
AP Crash Info	show ap debug crash-info
AP Current Time	show clock
AP Current Timezone	show clock timezone
AP Datapath ACL Table Allocation	show datapath acl-allocation
AP Datapath ACL Tables	show datapath acl-all
AP Datapath Bridge Table	show datapath bridge
AP Datapath DMO session	show datapath dmo-session
AP Datapath DMO station	show datapath dmo-station
AP Datapath Dns Id MAP	show datapath dns-id-map
AP Datapath Multicast Table	show datapath mcast
AP Datapath Nat Pool	show datapath nat-pool
AP Datapath Route Table	show datapath route
AP Datapath Session Table	show datapath session
AP Datapath DPI Session Table	show datapath session dpi
AP Datapath DPI Session Table Verbose	show datapath session dpi verbose
AP Datapath Statistics	show datapath statistics
AP Datapath User Table	show datapath user
AP Datapath VLAN Table	show datapath vlan
AP DPI Debug statistics	show dpi debug statistics
AP Daylight Saving Time	show clock summer-time
AP Derivation Rules	show derivation-rules
AP Driver Configuration	show ap debug driver-config
AP Election Statistics	show election statistics
AP External Captive Portal Status	show external-captive-portal
AP Environment Variable	show ap-env
AP ESSID Table	show network
AP Flash Configuration	show ap flash-config
AP IGMP Group Table	show ip igmp
AP Interface Counters	show interface counters
AP Interface Status	show port status
AP Internal DHCP Status	show dhcp-allocation
AP IP Interface	show ip interface brief
AP IP Route Table	show ip route
AP L3 Mobility Datapath	show l3-mobility datapath
AP L3 Mobility Events log	show log l3-mobility
AP L3 Mobility Status	show l3-mobility status
AP LACP Status	show lacp status
AP Log All	show log debug
AP Log AP-Debug	show log ap-debug
AP Log Conversion	show log convert
AP Log Driver	show log driver
AP Log Kernel	show log kernel
AP Log Network	show log network
AP Log PPPd	show log pppd
AP Log Rapper	show log rapper
AP Log Rapper Counter	show log rapper-counter
AP Log Rapper Brief	show log rapper-brief
AP Log Sapd	show log sapd
AP Log Security	show log security
AP Log System	show log system
AP Log Tunnel Status Management	show log apifmgr
AP Log Upgrade	show log upgrade
AP Log User-Debug	show log user-debug
AP Log User	show log user
AP Log VPN Tunnel	show log vpn-tunnel
AP Log Wireless	show log wireless
AP Management Frames	show ap debug mgmt-frames
AP Memory Allocation State Dumps	show malloc-state-dumps
AP Memory Utilization	show memory

```
AP Mesh Counters                          show ap mesh counters
AP Mesh Link                              show ap mesh link
AP Mesh Neighbors                         show ap mesh neighbours
AP Monitor Active Laser Beams             show ap monitor active-laser-beams
AP Monitor AP Table                       show ap monitor ap-list
AP Monitor ARP Cache                      show ap monitor ARP Cache
AP Monitor Client Table                   show ap monitor sta-list
AP Monitor Containment Information        show ap monitor containment-info
AP Monitor Potential AP Table             show ap monitor pot-ap-list
AP Monitor Potential Client Table         show ap monitor pot-sta-list
AP Monitor Router                         show ap monitor routers
AP Monitor Scan Information               show ap monitor scan-info
AP Monitor Status                         show ap monitor status
AP Persistent Clients                     show ap debug persistent-clients
AP PMK Cache                              show ap pmkcache
AP PPPoE uplink debug                     show pppoe debug-logs
AP PPPoE uplink status                    show pppoe status
AP Processes                              show process
AP Radio 0 Client Probe Report            show ap client-probe-report 0
AP Radio 0 Stats                          show ap debug radio-stats 0
AP Radio 0 info                           show ap debug radio-info 0
AP Radio 1 Client Probe Report            show ap client-probe-report 1
AP Radio 1 Stats                          show ap debug radio-stats 1
AP Radio 1 info                           show ap debug radio-info 1
AP RADIUS Statistics                      show ap debug radius-statistics
AP Termination RADIUS Statistics          show ap debug radius-statistics termination
AP Shaping Table                          show ap debug shaping-table
AP Sockets                                show socket
AP STM Configuration                      show ap debug stm-config
AP Swarm State                            show swarm state
AP System Status                          show ap debug system-status
AP System Summary                         show summary support
AP Uplink Status                          show uplink status
AP User Table                             show clients
AP Valid Channels                         show valid-channels
AP Version                                show version
AP Virtual Beacon Report                  show ap virtual-beacon-report
AP VPN Config                             show vpn config
AP VPN Status                             show vpn status
AP AP-VPN Retry Counters                  show vpn tunnels
AP Wired Port Settings                    show wired-port-settings
AP Wired User Table                       show clients wired
AP Checksum                               show ap checksum
AP Spectrum AP table                      show ap spectrum ap-list
AP Spectrum channel table                 show ap spectrum channel-details
AP Spectrum channel metrics               show ap spectrum channel-metrics
AP Spectrum channel summary               show ap spectrum channel-summary
AP Spectrum client table                  show ap spectrum client-list
AP Spectrum device duty cycle             show ap spectrum device-duty-cycle
AP Spectrum non-wifi device history       show ap spectrum device-history
AP Spectrum non-wifi device table         show ap spectrum device-list
AP Spectrum non-wifi device log           show ap spectrum device-log
AP Spectrum number of device              show ap spectrum device-summary
AP Spectrum interference-power table      show ap spectrum interference-power
AP Spectrum status                        show ap spectrum status
VC 802.1x Certificate                     show 1xcert
VC All Certificates                       show cert all
VC radsec Certificates                    show radseccert
VC Captive Portal domains                 show captive-portal-domains
VC About                                  show about
VC Active Configuration                   show running-config
VC AirGroup Service                       show airgroupservice
VC AirGroup Status                        show airgroup status
VC Allowed AP Table                       show allowed-aps
VC AMP Status                             show ap debug airwave
VC AMP Current State Data                 show ap debug airwave-state
VC AMP Current Stats Data                 show ap debug airwave-stats
VC AMP Data Sent                          show ap debug airwave-data-sent
VC AMP Events Pending                     show ap debug airwave-events-pending
VC AMP Last Configuration Received        show ap debug airwave-config-received
VC AMP Single Sign-on Key                 show ap debug airwave-signon-key
VC AMP Configuration Restore Status       show ap debug airwave-restore-status
VC Central Current State Data             show ap debug cloud-state
VC Central Current Stats Data             show ap debug cloud-stats
VC Central Data Sent                      show ap debug cloud-data-sent
VC Central Events Pending                 show ap debug cloud-events-pending
VC Central Last Configuration Received    show ap debug cloud-config-received
VC Central Single Sign-on Key             show ap debug cloud-signon-key
VC Central Configuration Restore Status   show ap debug cloud-restore-status
VC Application Services                   show app-services
VC Cloud Server Status                    show ap debug cloud-server
VC DHCP Option 43 Received                show dhcpc-opts
VC Global Alerts                          show alert global
VC Global Statistics                      show stats global
VC IDS AP List                            show ids aps
VC IDS Client List                        show ids clients
VC Internal DHCP Server Configuration     show ip dhcp database
VC Local User Database                    show users
VC OpenDNS Configuration and Status       show opendns support
VC Provisioning Log                       show log provision
VC Radius Attributes                      show radius-attributes
VC Radius Servers                         show radius-servers support
AP Radius Status                          show radius status
VC Saved Configuration                    show configuration
VC Scanning Stats                         show aps scanning
VC show SBR Table                         show datapath sbr
VC SNMP Configuration                     show snmp-configuration
VC Uplink 3G/4G Configuration             show cellular config
VC Uplink Management Configuration        show uplink config
VC WISPr Configuration                    show wispr config
VC XML API Server Information             show xml-api-server
VC rfc3576-radius statistics              show ap debug rfc3576-radius-statistics
```

Note

Use the support commands under the supervision of Siemens technical support.

35.5 Uplink Bandwidth Monitoring

An AP uses Iperf3 as a TCP or UDP client to run a speed test and measure the bandwidth on an uplink. The results from the speed test are collated by the AP and published to ALE. Speed tests can be run only on master APs. They cannot be run on slave APs.

You may choose to configure and execute a speed test profile during boot time and additionally at specific time intervals using the configuration mode or execute the speed test at any preferred time using the privileged EXEC mode in the CLI.

To configure and automatically run speed tests at specific time intervals:

```
(AP)(config)# speed-test
(AP)(speed-test)# include-reverse
(AP)(speed-test)# server-ip <server>
(AP)(speed-test)# server-port <port>
(AP)(speed-test)# protocol <tcp/udp>
(AP)(speed-test)# on-boot
(AP)(speed-test)# time-interval <interval>
(AP)(speed-test)# bandwidth <bandwidth>
(AP)(speed-test)# sec-to-measure <secs>
```

To configure and execute a speed test at any point in time:

```
(AP)# speed-test <server> <protocol> [<bandwidth>|<include-reverse>|<sec-to-
measure>|<server-port>]
```

To view the speed test results:

```
(AP)# show speed-test data
```

The following command shows the number of times the uplink bandwidth report was sent to the ALE server. To display the uplink bandwidth counter:

```
(AP)# show ale stats
ALE Stats
---------
Type Value
---- -----
VC package 0
RSSI package 0
APPRF package 0
URLv package 0
STATE package 0
STAT package 0 UPLINK BW package 0 Total 0
```

35.6 WAN Link Health Monitoring

Starting from SCALANCE W 8.3.0.0, APs support the WAN Link Health Monitoring feature for the Service Assurance application. The Service Assurance application helps run various tests to determine the network performance and reachability of hosts that are configured by the customer.

WAN Link Health Monitoring supports Aruba Central WAN Health Monitoring feature. It helps Aruba Central customers get periodic statistics on reachability, connectivity, and AP performance.

Note

WAN Link Health Monitoring supports only IPv4 addresses. It does not support IPv6 addresses in this release.

From Central, customers can send request (using the **Clarity > Health Checks** page or API interface) to run the following performance and reachability test suites:

- Reachability

  Ping/ICMP test for reachability

  - Supports up to five host names/IP addresses.
  - Response information for the Ping test containing the number of transmitted and received packets, and response time are sent.

- Connectivity

  TCP Connect test for connectivity to hosts

  Supports maximum of five host name/IP address and port combinations. Only IPv4 addresses are supported.

- Performance

  Iperf (UDP/TCP) test for WAN speed/performance

  - Supports maximum of five host IPs as input.
  - Response contains the important parameters parsed from iperf3 response.

  wget (webpage load) tests for AP performance o Supports up to five valid URLs.

  - Supports up to five valid URLs.
  - Download rate and download bytes are sent back in response along with the

  The execution time for each test can be up to 36 seconds. Central customers can configure any of these tests that can be run on demand or at scheduled intervals for any branch or site.

Note

APs support a maximum of four test suites with five hosts each. On-demand policies are prioritized against periodic policies.

On-Demand Policies

An on-demand policy is executed once when a request is received. It is not stored on the AP. For example, when a network admin finds a problem and wants to troubleshoot it, the admin user can send an on-demand policy to run some tests and check the results to troubleshoot the problem.

1. Each AP can handle one on-demand policy at a time. If there is an on-demand policy in progress and another on-demand policy request is received by an AP, Central receives a NACK response.
2. If an AP is executing a periodic policy and an on-demand policy request is received, then the on- demand policy is executed after executing the periodic policy.

Periodic Policies

Periodic policies are run periodically based on a schedule and periodicity. Up to 4 periodic policies can be added for an AP. The schedule is defined at policy level and periodicity is defined test suite level. They can be used to monitor a given branch or site for various parameters, and get the required statistics.

Points to Note:

- Central customers must have an API Gateway or Clarity Health Check license.
- The user from the customer’s branch or site must have admin access to AP and Central.
- This feature is supported only on APs.
- IPv6 address is not supported.
- Central customers can set thresholds so that the application can trigger notifications when set thresholds are reached.

Central customers can monitor the network performance data.

- The policy entries are cleared when Central connection goes DOWN.
- If a device restarts or Central connection goes DOWN and then restores, then Central takes care to resend the policies to the same device or a different device.
- When a policy request is received and no test is running at that time, all the tests in the request are run sequentially. The order in which tests are executed (if configured) is reachability, connectivity, and then performance tests.
- When a test is already running and a new policy request is seen, NACK response is sent to Aruba Central and the policy is rejected.

Aruba Central sends the customer-configured tests and the associated data to AP devices as protocol buffer messages. The APs parse the protocol buffer messages and converts them into a policy. APs then run these tests sequentially, collate the test results, and send them as protocol buffer messages to Central.

Verification of WAN Link Health Monitoring Status

Execute the following command to get the WAN Link Health Monitoring status:

```
(AP) #show lhm status
```

Execute the following command to get the Health Checks sent from Central to AP:

```
(AP) #show lhm policy
```

Troubleshooting WAN Link Health Monitoring

Use the following commands to view trace logs of WAN Link Health Monitoring process:

```
(AP) #trace component LHM sub-component ALL
```

```
(AP) #trace level DEBUG LHM
```

```
(AP) #show trace log lhm <no_of_lines>
```

Note

These commands are for troubleshooting purpose only and must be disabled after that.

Hotspot Profiles 36

Note

In the current release, SCALANCE W supports the hotspot profile configuration only through the CLI.

36.1 Understanding Hotspot Profiles

Hotspot 2.0 R1 is a WFA specification based on the 802.11u protocol, which allows wireless clients to discover hotspots using management frames (such as beacon, association request, and association response), connect to networks, and roam between networks without additional authentication.

Hotspot 2.0 provides the following services:

- Network discovery and selection—Allows the clients to discover suitable and available networks by advertising the access network type, roaming consortium, and venue information through the management frames. For network discovery and selection, GAS and ANQP are used.
- QOS Mapping—Provides a mapping between the network-layer QoS packet marking and over- the-air QoS frame marking based on user priority.

This release supports the following new features:

- Online Sign-Up—Mobile devices use Online Sign-Up (OSU) for registration and credential provisioning to obtain secure network access using the service provider's OSU server.
- WNM Subscription Remediation—Subscription remediation is a process that Home Service Providers use to correct, update, and resolve subscription issues. WNM(11v) is used for Subscription Remediation.

When a hotspot is configured in a network:

- The clients search for available hotspots using the beacon management frame.
- When a hotspot is found, the client sends queries to obtain information about the type of network authentication and IP address, and IP address availability using the GAS action frames.
- Based on the response of the advertisement server (response to the GAS Action Frames), the relevant hotspot is selected and the client attempts to associate with it.
- Based on the authentication mode used for mobility clients, the client authenticates to access the network.

GAS

GAS is a request-response protocol, that provides L2 transport mechanism between a wireless client and a server in the network prior to authentication. It helps to determine an 802.11 infrastructure before associating clients and allows clients to send queries to multiple 802.11 networks in parallel.

An AP can include its SP Organization Identifier indicating the identity of the SP in beacons and probe responses to clients. When a client recognizes an AP's OI, it attempts to associate to that AP using the security credentials corresponding to that SP. If the client does not recognize the AP’s OI, the client sends a GAS query to the AP to request more information about the network before associating. A client transmits a GAS Query using a GAS Initial Request frame and the AP provides the query response or information on how to receive the query response in a GAS Initial Response frame. To transmit a GAS query for any advertisement protocol, the advertisement protocol ID must include the advertisement protocol information element with details of the advertisement protocol and its corresponding advertisement control.

ANQP

ANQP provides a range of information, such as IP address type and availability, roaming partners accessible through a hotspot, and the EAP method supported for authentication, for a query and response protocol. The ANQP Information Elements provide additional data that can be sent from an AP to the client to identify the AP's network and service provider. If a client requests this information through a GAS query, the hotspot AP sends the ANQP capability list in the GAS Initial Response frame indicating support for the following IEs:

- Venue Name
- Domain Name
- Network Authentication Type
- Roaming Consortium List
- Network Access Identifier Realm
- 3GPP Cellular Network Data
- IP Address Availability

H2QP

The H2QP profiles provide a range of information on Hotspot 2.0 elements such as hotspot protocol and port, operating-class, operator names, WAN status, OSU provider list, and uplink and downlink metrics.

Information Elements and Management Frames

The Hotspot 2.0 configuration supports the following IEs:

- Interworking IE—Provides information about the Interworking service capabilities such as the Internet availability in a specific service provider network.
- Advertisement Protocol IE—Provides information about the advertisement protocol that a client can use for communication with the advertisement servers in a network.
- Roaming Consortium IE—Provides information about the service provider network for roaming clients, which can be used to authenticate with the AP.

The IEs are included in the following Management Frames when 802.11u is enabled:

- Beacon Frame
- Probe Request Frame
- Probe Response frame
- Association Request
- Re-Association request

Network Access Identifier Realm List

A Network Access Identifier Realm profile identifies and describes a NAI realm to which the clients can connect. The NAI realm settings on an AP act as an advertisement profile to determine the NAI realm elements that must be included as part of a GAS Response frame.

36.2 Configuring Hotspot Profiles

To configure a hotspot profile, perform the following steps:

1. Create the required ANQP and H2QP advertisement profiles.
2. Create a hotspot profile.
3. Associate the required ANQP and H2QP advertisement profiles created in step 1 to the hotspot profile created in step 2.
4. Create an SSID Profile with enterprise security and WPA-2 encryption settings and then associate the SSID with the hotspot profile created in step 2.

36.2.1 Creating Advertisement Profiles for Hotspot Configuration

A hotspot profile contains one or sever advertisement profiles. The following advertisement profiles can be configured through the SCALANCE W CLI:

ANQP advertisement profiles

- NAI Realm profile
- Venue Name Profile
- Network Authentication Profile
- Roaming Consortium Profile
- 3GPP Profile
- IP Address availability Profile
- Domain Name Profile

H2QP advertisement profiles

- Operator Friendly Name Profile
- Connection Capability Profile
- Operating-Class Profile
- WAN-Metrics Profile
- OSU Provider Profile

Configuring an NAI Realm Profile

You can configure a Network Access Identifier Realm profile to define the NAI realm information, which can be sent as an ANQP IE in a GAS query response.

To configure a NAI profile:

```
(AP)(config)# hotspot anqp-nai-realm-profile <name>

(AP)(nai-realm <name>)# nai-realm-name <name>

(AP)(nai-realm <name>)# nai-realm-encoding {<utf8>|<rfc4282>}

(AP)(nai-realm <name>)# nai-realm-eap-method <eap-method>

(AP)(nai-realm <name>)# nai-realm-auth-id-1 <authentication-ID>

(AP)(nai-realm <name>)# nai-realm-auth-id-2 <authentication-ID>

(AP)(nai-realm <name>)# nai-realm-auth-value-1 <authentication-value>

(AP)(nai-realm <name>)# nai-realm-auth-value-2 <authentication-value>

(AP)(nai-realm <name>)# nai-home-realm
```

You can specify any of the following EAP methods for the **nai-realm-eap-method <eap-method>** command:

- **identity** - To use EAP Identity type. The associated numeric value is 1.
- **notification** - To allow the hotspot realm to use EAP Notification messages for authentication. The associated numeric value is 2.
- **one-time-password** - To use Authentication with a single-use password. The associated numeric value is 5.
- **generic-token-card** - To use EAP Generic Token Card (EAP-GTC). The associated numeric value is 6.
- **eap-tls** - To use EAP-Transport Layer Security. The associated numeric value is 13.
- **eap-sim** - To use EAP for Global System for Mobile Communication (GSM) Subscriber Identity Modules (SIM). The associated numeric value is 18.
- **eap-ttls** - To use EAP-Tunneled Transport Layer Security. The associated numeric value is 21.
- **peap** - To use protected Extensible Authentication Protocol. The associated numeric value is 25.
- **crypto-card** - To use crypto card authentication. The associated numeric value is 28.
- **peapmschapv2** - To use PEAP with Microsoft Challenge Handshake Authentication Protocol version 2 (MSCHAPv2). The associated numeric value is 29.
- **eap-aka** - To use EAP for Universal Mobile Telecommunications System (UMTS) Authentication and Key Agreement (AKA). The associated numeric value is 50.

The following table lists the possible authentication IDs and their respective values:

Table 36- 1 NAI Realm Profile Configuration Parameters

Authentication ID	Authentication Value
reserved • Uses the reserved authentication method. • The associated numeric value is **0**.	-
expanded-eap • Uses the expanded EAP authentication method. • The associated numeric value is **1**.	Use expanded-eap as the authentication value.
non-eap-inner-auth • Uses non-EAP inner authentication type. • The associated numeric value is **2**.	The following authentication values apply: • **reserved** - The associated numeric value is **0**. • **pap** - The associated numeric value is **1**. • **chap** - The associated numeric value is **2**. • **mschap** - The associated numeric value is **3**. • **mschapv2** - The associated numeric value is **4**.
eap-inner-auth • Uses EAP inner authentication type. • The associated numeric value is **3**.	The following authentication values apply: • **reserved** - The associated numeric value is **0**. • **pap** - The associated numeric value is **1**. • **chap** - The associated numeric value is **2**. • **mschap** - The associated numeric value is **3**. • **mschapv2** - The associated numeric value is **4**.
exp-inner-eap • Uses the expanded inner EAP authentication method. • The associated numeric value is **4**.	Use the exp-inner-eap authentication value.
credential • Uses credential authentication. • The associated numeric value is **5**.	The following authentication values apply: • **sim** - The associated numeric value is **1**. • **usim** - The associated numeric value is **2**. • **nfc-secure** - The associated numeric value is **3**. • **hw-token** - The associated numeric value is **4**. • **softoken** - The associated numeric value is **5**. • **certificate** - The associated numeric value is **6**. • **uname-passward** - The associated numeric value is **7**. • **none** - The associated numeric value is **8**. • **reserved** - The associated numeric value is **9**. • **vendor-specific** - The associated numeric value is **10**.

Configuring a Venue Name Profile

You can configure a venue name profile to send the venue information as an ANQP IE in a GAS query response. To configure a venue name profile:

```
(AP)(config)# hotspot anqp-venue-name-profile <name>

(AP)(venue-name <name>)# venue-name <name>

(AP)(venue-name <name>)# venue-group <group-name>

(AP)(venue-name <name>)# venue-type <type>

(AP)(venue-name <name>)# venue-lang-code <language>
```

You can specify any of the following venue groups and the corresponding venue types:

Table 36- 2 Venue Types

Authentication ID	Authentication Value
unspecified The associated numeric value is **0**.	—
assembly The associated numeric value is **1**.	• unspecified—The associated numeric value is **0**. • arena—The associated numeric value is **1**. • stadium—The associated numeric value is **2**. • passenger-terminal—The associated numeric value is **3**. • amphitheater—The associated numeric value is **4**. • amusement-park—The associated numeric value is **5**. • place-of-worship—The associated numeric value is **6**. • convention-center—The associated numeric value is **7**. • library—The associated numeric value is **8**. • museum—The associated numeric value is **9**. • restaurant—The associated numeric value is **10**. • theater—The associated numeric value is **11**. • bar—The associated numeric value is **12**. • coffee-shop—The associated numeric value is **13**. • zoo-or-aquarium—The associated numeric value is **14**. • emergency-cord-center—The associated numeric value is **15**.

Authentication ID	Authentication Value
business The associated numeric value is **2**.	- unspecified—The associated numeric value is **0**. - doctor—The associated numeric value is **1**. - bank—The associated numeric value is **2**. - fire-station—The associated numeric value is **3**. - police-station—The associated numeric value is **4**. - post-office—The associated numeric value is **6**. - professional-office—The associated numeric value is **7**. - research-and-dev-facility—The associated numeric value is **8**. - attorney-office—The associated numeric value is **9**.
educational The associated numeric value is **3**.	- unspecified—The associated numeric value is **0**. - school-primary—The associated numeric value is **1**. - school-secondary—The associated numeric value is **2**. - univ-or-college—The associated numeric value is **3**.
factory-and-industrial The associated numeric value is **4**.	- unspecified—The associated numeric value is **0**. - factory—The associated numeric value is **1**.
institutional The associated numeric value is **5**	- unspecified—The associated numeric value is **0**. - hospital—The associated numeric value is **1**. - ong-term-care—The associated numeric value is **2**. - alc-drug-rehab—The associated numeric value is **3**. - group-home—The associated numeric value is **4**. - prison-or-jail—The associated numeric value is .
mercantile The associated numeric value is **6**.	- unspecified—The associated numeric value is **0**. - retail-store—The associated numeric value is **1**. - Grocery-market—The associated numeric value is **2**. - auto-service-station—The associated numeric value is **3**. - shopping-mall—The associated numeric value is **4**. - gas-station—The associated numeric value is **5**
residential The associated numeric value is **7**.	- unspecified—The associated numeric value is **0**. - private-residence—The associated numeric value is **1**. - hotel—The associated numeric value is **2**. - dormitory—The associated numeric value is **3**. - boarding-house—The associated numeric value is **4**.
storage The associated numeric value is **8**.	- unspecified—The associated numeric value is **0**.
utility-misc The associated numeric value is **9**.	- unspecified—The associated numeric value is **0**.

Authentication ID	Authentication Value
vehicular The associated numeric value is **10**.	• unspecified—The associated numeric value is **0**. • automobile-or-truck—The associated numeric value is **1**. • airplane—The associated numeric value is **2**. • bus—The associated numeric value is **3**. • ferry—The associated numeric value is **4**. • ship—The associated numeric value is **5**. • train—The associated numeric value is **6**. • motor-bike—The associated numeric value is **7**.
outdoor The associated numeric value is **11**.	• unspecified—The associated numeric value is **0** • muni-mesh-network—The associated numeric value is **1**. • city-park—The associated numeric value is **2**. • rest-area—The associated numeric value is **3**. • traffic-control—The associated numeric value is **4**. • bus-stop—The associated numeric value is **5**. • kiosk—The associated numeric value is **6**.

Configuring a Network Authentication Profile

You can configure a network authentication profile to define the authentication type used by the hotspot network.

To configure a network authentication profile:

```
(AP)(config)# hotspot anqp-nwk-auth-profile <name>

(AP)(network-auth <name>)# nwk-auth-type <type>

(AP)(network-auth <name>)# url <URL>
```

You can specify any of the following network authentication type for the **nwk-auth-type <type>** command:

- **accept-term-and-cond**—When configured, the network requires the user to accept terms and conditions.

  This option requires you to specify a redirection URL string as an IP address, FQDN or URL.
- **online-enrollment**—When configured, the network supports the online enrollment.
- **http-redirect**—When configured, additional information on the network is provided through HTTP/HTTPS redirection.
- **dns-redirect**—When configured, additional information on the network is provided through DNS redirection. This option requires you to specify a redirection URL string as an IP address, FQDN, or URL.

Configuring a Roaming Consortium Profile

You can configure a roaming consortium profile to send the roaming consortium information as an ANQP IE in a GAS query response.

To configure a roaming consortium profile:

```
(AP)(config)# hotspot anqp-roam-cons-profile <name>

(AP)(roaming-consortium <name>)# roam-cons-oi <roam-cons-oi>

(AP)(roaming-consortium <name>)# roam-cons-oi-len <roam-cons-oi-len>

(AP)(roaming-consortium <name>)# enable

(AP)(roaming-consortium <name>)# end (AP)# commit apply
```

Specify a hexadecimal string of 3–5 octets for **roam-cons-oi <roam-cons-oi>**.

Based on the Organization Identifier (OI) specified, you can specify the following parameters for the length of OI in **roam-cons-oi-len <roam-cons-oi-len>**.

- For 0: 0 Octets in the OI (Null)
- For 3: OI length is 24-bits (3 Octets)
- For 5: OI length is 36-bits (5 Octets)

Configuring a 3GPP Profile

You can configure a 3rd Generation Partnership Project (3GPP) profile to define information for the 3G Cellular Network for hotspots.

To configure a 3GPP profile:

```
(AP)(config)# hotspot anqp-3gpp-profile <name>

(AP)(3gpp <name>)# 3gpp-plmn1 <plmn-ID>

(AP)(3gpp <name>)# enable
```

The Public Land Mobile Network (PLMN) ID is a combination of the mobile country code and network code. You can specify up to 6 PLMN IDs for a 3GPP profile.

Configuring an IP Address Availability Profile

You can configure an available IP address types to send information on IP address availability as an ANQP IE in a GAS query response.

To configure an IP address availability profile:

```
(AP)(config)# hotspot anqp-ip-addr-avail-profile <name>

(AP)(IP-addr-avail <name>)# ipv4-addr-avail

(AP)(IP-addr-avail <name>)# ipv6-addr-avail

(AP)(IP-addr-avail <name>)# enable
```

Configuring an Operator-Friendly Profile

You can configure an operator-friendly name profile to define the identify the operator. To configure an H2QP operator-friendly name profile:

```
(AP)(config)# hotspot h2qp-oper-name-profile <name>

(AP)(operator-friendly-name <name>)# op-fr-name <op-fr-name>

(AP)(operator-friendly-name <name>)# op-lang-code <op-lang-code>

(AP)(operator-friendly-name <name>)# enable

(AP)(operator-friendly-name <name>)# end

(AP)# commit apply
```

Configuring a Domain Profile

You can configure a domain profile to send the domain names as an ANQP IE in a GAS query response.

To configure a domain name profile, execute the following commands:

```
(AP)(config)# hotspot anqp-domain-name-profile <name>

(AP)(domain-name <name>)# domain-name <domain-name>

(AP)(domain-name <name>)# enable
```

Configuring an Operator-Friendly Profile

You can configure an operator-friendly name profile to define the identify the operator.

To configure an H2QP operator-friendly name profile:

```
(AP)(config)# hotspot h2qp-oper-name-profile <name>

(AP)(operator-friendly-name <name>)# op-fr-name <op-fr-name>

(AP)(operator-friendly-name <name>)# op-lang-code <op-lang-code>

(AP)(operator-friendly-name <name>)# enable
```

Configuring a Connection Capability Profile

You can configure a connection capability profile to define information such as the hotspot IP protocols and associated port numbers that are available for communication.

To configure an H2QP connection capability profile:

```
(AP)(config) # hotspot h2qp-conn-cap-profile <name>
(AP)(connection-capabilities <name>)# esp-port
(AP)(connection-capabilities <name>)# icmp
(AP)(connection-capabilities <name>)# tcp-ftp
(AP)(connection-capabilities <name>)# tcp-http
(AP)(connection-capabilities <name>)# tcp-pptp-vpn
(AP)(connection-capabilities <name>)# tcp-ssh
(AP)(connection-capabilities <name>)# tcp-tls-vpn
(AP)(connection-capabilities <name>)# tcp-voip
(AP)(connection-capabilities <name>)# udp-ike2
(AP)(connection-capabilities <name>)# udp-ipsec-vpn
(AP)(connection-capabilities <name>)# udp-voip
(AP)(connection-capabilities <name>)# enable
```

Configuring an Operating-Class Profile

You can configure an operating-class profile to list the channels on which the hotspot is capable of operating. To configure an H2QP operating-class profile:

```
(AP)(config) # hotspot h2qp-oper-class-profile <name>
(AP)(operator-class <name>)# op-class <class-ID>
(AP)(operator-class <name>)# enable
```

Configuring a WAN Metrics Profile

You can configure a WAN metrics profile to define information about access network characteristics such as link status and metrics.

To configure a WAN metrics profile:

```
(AP)(config)# hotspot h2qp-wan-metrics-profile <name>
(AP)(WAN-metrics <name>)# at-capacity
(AP)(WAN-metrics <name>)# downlink-load <load>
(AP)(WAN-metrics <name>)# downlink-speed <speed>
(AP)(WAN-metrics <name>)# load-duration <duration>
(AP)(WAN-metrics <name>)# symm-link
(AP)(WAN-metrics <name>)# uplink-load <load>
```

```
(AP)(WAN-metrics <name>)# uplink-speed <speed>
```

```
(AP)(WAN-metrics <name>)# wan-metrics-link-status <status>
```

You can specify the following WAN downlink and uplink parameters:

- **Downlink load**—Indicates the percentage of the WAN downlink currently utilized. The default value of 0 indicates that the downlink speed is unknown or unspecified.
- **Downlink speed**—Indicates the WAN downlink speed in Kbps.
- **Uplink load**—Indicates the percentage of the WAN uplink currently utilized. The default value of 0 indicates that the downlink speed is unknown or unspecified.
- **Uplink speed**—Indicates the WAN uplink speed in Kbps.
- **Load duration**—Indicates the duration in seconds during which the downlink utilization is measured.
- **Symmetric links**—Indicates if the uplink and downlink have the same speed.
- **WAN Link Status**—Indicates if the WAN is down (link-down), up (link-up), or in test state (link-under-test).

Configuring an OSU Provider Profile

You can create an OSU provider profile and attach them to a hotspot profile to enable wireless devices to use OSU. The OSU providers list element provides information for one or more entities offering OSU service. For each OSU provider, information such as friendly name (in one or more human languages), NAI(used to authenticate to the OSU ESS if configured for OSEN), icon(s), and URI of the OSU Server are provided.

Downloading Icon Files to AP

To download the icon file to the AP, execute the following command:

```
(AP)# hs2-osu-icon-download <idx> <ftp/tftp/http URL syntax>
```

The icon file is downloaded from the specified location using the specified protocol and stored in the file system with the specified index as reference.

To Delete an icon file from AP, execute the following command:

```
(AP)# hs2-osu-icon-delete <idx>
```

Table 36- 3 HS2 OSU Icon Download Parameters

Parameter	Description
<idx>	Indicates the index of the file which can take values from 1 to 16.
<url>	The protocol that is used to download the icon file. The protocol can be FTP, TFTP, or HTTP.

Configuring OSU Provider Profile Parameters

```
(AP) (config) # hotspot h2qp-osu-provider-profile <name>

(AP) (osu-provider <name>) # frnd-name-count <count>

(AP) (osu-provider <name>) # frnd-name1-lang-code <lang code>

(AP) (osu-provider <name>) # frnd-name1 <OSU Friendly name>
```

```
(AP) (osu-provider <name>) # frnd-name1-hex <OSU Friendly name>

(AP) (osu-provider <name>) # frnd-name2-lang-code <lang code>

(AP) (osu-provider <name>) # frnd-name2 <OSU Friendly name>

(AP) (osu-provider <name>) # frnd-name2-hex <OSU Friendly name>

(AP) (osu-provider <name>) # iconfile-count <count>

(AP) (osu-provider <name>) # icon1-width <width>

(AP) (osu-provider <name>) # icon1-height <height>

(AP) (osu-provider <name>) # icon1-lang-code <lang code>

(AP) (osu-provider <name>) # icon1-type <file type>

(AP) (osu-provider <name>) # icon1-file <idx> <File Name>

(AP) (osu-provider <name>) # icon2-width <width>

(AP) (osu-provider <name>) # icon2-height <height>

(AP) (osu-provider <name>) # icon2-lang-code <lang code>

(AP) (osu-provider <name>) # icon2-type <file type>

(AP) (osu-provider <name>) # icon2-file <idx> <File Name>

(AP) (osu-provider <name>) # srvcdesc-count <count>

(AP) (osu-provider <name>) # srvc-desc1-lang-code <lang code>

(AP) (osu-provider <name>) # srvc-desc1 <description>

(AP) (osu-provider <name>) # srvc-desc1-hex <description>

(AP) (osu-provider <name>) # srvc-desc2-lang-code <lang code>

(AP) (osu-provider <name>) # srvc-desc2 <description>

(AP) (osu-provider <name>) # srvc-desc2-hex <description>

(AP) (osu-provider <name>) # osu-server-uri <OSU server URI>

(AP) (osu-provider <name>) # osu-method <OSU method>
```

Table 36- 4 HS2 OSU Provider Parameters

Parameter	Description	Range
enable	Enables the OSU provider profile. This is enabled by default.	—
frnd-name- count	Number of OSU friendly names to be configured.	1 - 2
frnd-name1	The first OSU friendly name if you selected the language code as English. A string value of maximum 64 characters.	—
frnd-name1-hex	The first OSU friendly name in hexadecimal format for language codes other than English.	—
frnd- name1- lang-code	The language code used for configuring the first OSU friendly name.	—
frnd-name2	The second OSU friendly name if the language code chosen is English. A string value of maximum 64 characters.	—

Parameter	Description	Range
frnd- name2-hex	The second OSU friendly name in hexadecimal format for language codes other than English	—
frnd- name2- lang-code	he language code used for configuring the second OSU friendly name.	—
icon1-file	The index and name of the first icon image file. **NOTE:** The index value and the filename value must match the file downloaded to AP. For more information on downloading the icon file, refer to Downloading Icon Files to AP (Page 470).	—
icon1- height	Height of the first icon image file.	1 - 256
icon1-lang- code	Indicates the language used in the first icon image	—
icon1-type	Type of the image file used as first icon.	—
icon1-width	Width of the first icon image file.	1 - 256
icon2-file	The index and name of the second icon image file. **NOTE**: The index value and the filename value must match the file downloaded to AP. For more information on downloading the icon file, refer to Downloading Icon Files to AP (Page 470).	—
icon2- height	Height of the second icon image file.	—
icon2-lang-code	Indicates the language used in the second icon image.	—
icon2-type	Type of the image file used as second icon.	—
icon2-width	Width of the second icon image file.	—
iconfile-count	Number of icon files to be used for the OSU provider.	1 - 2
no	Deletes the command.	—
osu- method	Indicates the method used by OSU to provision the HS2 client.	• OMA-DM • SOAP-XML
osu-server- uri	The URI of the OSU Server that is used for OSU with the service provider configured in the **frnd-name**1-parameter.	—
srvc-desc1	The first service description if you selected the language code as English.	—
srvc-desc1- hex	The first service description in hexadecimal format for language codes other than English.	—
srvc-desc1-lang-code	The language code used for the first description.	—
srvc-desc2	The second service description if you selected the language code as English.	—
srvc-desc2- hex	The second service description in hexadecimal format for language codes other than English.	—
srvc-desc2-lang-code	The second service description if you selected the language code as English.	—
srvcdesc.count	Number of descriptions to be provided for the OSU provider.	—

36.2.2 Creating a Hotspot Profile

To create a hotspot profile:

```
(AP)(config)# hotspot hs-profile <name> (AP)(Hotspot2.0 <name>)# asra

(AP)(Hotspot2.0 <name>)# access-network-type <type>

(AP)(Hotspot2.0 <name>)# addtl-roam-cons-ois <roam-consortium-OIs>

(AP)(Hotspot2.0 <name>)# comeback-mode

(AP)(Hotspot2.0 <name>)# gas-comeback <delay-interval>

(AP)(Hotspot2.0 <name>)# group-frame-block

(AP)(Hotspot2.0 <name>)# hessid <hotspot-essid>

(AP)(Hotspot2.0 <name>)# internet

(AP)(Hotspot2.0 <name>)# osu-nai <osu-nai>

(AP)(Hotspot2.0 <name>)# osu-ssid <ssid>

(AP)(Hotspot2.0 <name>)# p2p-cross-connect

(AP)(Hotspot2.0 <name>)# p2p-dev-mgmt

(AP)(Hotspot2.0 <name>)# pame-bi

(AP)(Hotspot2.0 <name>)# qos-map-excp

(AP)(Hotspot2.0 <name>)# qos-map-range

(AP)(Hotspot2.0 <name>)# query-response-length-limit <integer>

(AP)(Hotspot2.0 <name>)# roam-cons-len-1 <integer>

(AP)(Hotspot2.0 <name>)# roam-cons-len-2 <integer>

(AP)(Hotspot2.0 <name>)# roam-cons-len-3 <integer>

(AP)(Hotspot2.0 <name>)# roam-cons-oi-1 <integer>

(AP)(Hotspot2.0 <name>)# roam-cons-oi-2 <integer>

(AP)(Hotspot2.0 <name>)# roam-cons-oi-3 <integer>

(AP)(Hotspot2.0 <name>)# venue-group <group>

(AP)(Hotspot2.0 <name>)# venue-type <type>

(AP)(Hotspot2.0 <name>)# enable
```

OSU ESS can either be open or encrypted. When OSU ESS is using open encryption, create an SSID profile with the same name as provided in the hotspot profile and set the operation mode to open. When OSU ESS is encypted, create a hotspot profile with only **osen** enabled and attach it to an SSID that broadcasts OSEN capable network. In this case, choose the operation mode to WPA2-AES.
To configure Online Sign-Up SSID in Encryption mode (OSEN), create a separate hotspot profile to enable OSEN and attach it to the SSID that broadcasts OSEN capable network:

```
(AP)(config)# hotspot hs-profile <name>

(AP)(Hotspot2.0 <name>)# osen
```

Note

Ensure that all parameters except OSEN are disabled in the separate hotspot profile created for OSEN.

The hotspot profile configuration parameters are described in the following table:

Table 36- 5 Hotspot Profile Configuration Parameters

Parameter	Description	Range	Default
access-network-type <type>	Specify any of the following 802.11u network types. • **private**—This network is accessible for authorized users only. For example, home networks or enterprise networks that require user authentication. The corresponding integer value for this network type is 0. • **private-with-guest**—This network is accessible to guest users based on guest authentication methods. For example, enterprise networks that allow guest users with captive portal authentication. The corresponding integer value for this network type is 1. • **chargeable-public**—This network provides access to the Internet based on payment. For example, a subscription-based Internet access in a coffee shop or a hotel offering chargeable in-room Internet access service. The corresponding integer value for this network type is 2. • **free-public**—This network is accessible to all without any charges applied. For example, a hotspot in airport or other public places that provide Internet access with no additional cost. The corresponding integer value for this network type is 3. • **personal-device**—This network is accessible for personal devices. For example, a laptop or camera configured with a printer for the purpose of printing. The corresponding integer value for this network type is 4. • **emergency-services**—This network is limited to accessing emergency services only. The corresponding integer value for this network type is 5. • **test**—This network is used for test purposes only. The corresponding integer value for this network type is 14. • **wildcard**—This network indicates a wildcard network. The corresponding integer value for this network type is 15.	private, private-with-guest,chargeable-public, free- public, personal- device, emergency-services, test, wildcard	chargeable-public
addtl-roam-cons-ois <addtl-roam-cons-ois>	Configures the number of additional roaming consortium OIs advertised by the AP. This feature supports up to three additional OIs, which are defined using the roam-cons-oi-1, roam-cons-oi-2 and roam-cons-oi-3 parameters.		

Parameter	Description	Range	Default
advertisement-profile	Associates an advertisement profile with the hotspot profile. You can associate any of the following advertisement profiles: • anqp-3gpp-profile • anqp-domain-name-profile • anqp-ip-addr--profile • anqp-nai-realm-profile • anqp-nwk-auth-profile • anqp-roam-cons-profile • anqp-venue-name-profile • h2qp-conn-cap-profile • h2qp-oper-class-profile • h2qp-osu-provider-profile • h2qp-oper-name-profile • h2qp-wan-metrics-profile		
<profile-name>	Allows you to associate a specific advertisement profile to the hotspot profile.		
asra	Indicates if any additional steps are required for network access.		
comeback-mode	By default, ANQP information is obtained from a GAS Request and Response. If you enable the comeback-mode option, advertisement information is obtained using a GAS Request and Response. as well as a Comeback-Request and Comeback-Response. This option is disabled by default.		
enable	Enables the hotspot profile.		
gas-comeback-delay <delay>	Configures a GAS comeback delay interval after which the client can attempt to retrieve the query response using a Comeback Request Action frame.	100—2000 milliseconds	1000
group-frame-block	Configures the DGAF Disabled Mode. This feature ensures that the AP does not forward downstream group-addressed frames. It is disabled by default, allowing the AP to forward downstream group-addressed frames.		
hessid	Configures a homogenous ESS identifier.	MAC address in colon-separated hexadecimalformat	
internet	Allows the AP to send an Information Element indicating that the network allows the Internet access. By default, a hotspot profile does not advertise network internet access.		
no	Removes any existing configuration.		

Parameter	Description	Range	Default
osen	Uses the OSEN information element to advertise and select an OSEN capable network. **NOTE:** You must create a separate hotspot profile only with OSEN enabled and attach it to the Online Sign-UP (OSU) SSID profile. Ensure that all the other parameters of the OSEN hotspot profile are disabled.		Disabled
osu-nai	Indicates the Network Access Identifier (NAI) that is used for OSU with the service provider configured in the OSU provider profile. When the OSU NAI is configured, the OSU ESS employs a link-layer encryption. For open OSU ESS, this parameter is not applicable.		
osu-ssid	Configures the SSID that the wireless devices use for OSU with all the OSU providers.		
p2p-cross-connect	Advertises support for P2P Cross Connections.		Disabled
p2p-dev-mgmt	Advertises support for P2P device management.		Disabled
pame-bi	Enables the PAME-BI bit, which is used by an AP to indicate whether the AP indicates that the Advertisement Server can return a query response that is independent of the BSSID used for the GAS Frame exchange.		
qos-map-excp	Includes the DSCP exceptions in the QoS map set. You can configure a maximum of 21 sets of DSCP exception fields. It must be entered in Hexadecimal format. It is in the format, <value>-<up> separated by ',' where <value> can be 0- 3F or FF, and user priority <up> can be 0-7).		
qos-map-range	Configures the DSCP range value between 0 and 63 inclusive, or 255. It must be entered in Hexadecimal format. You must configure 8 sets each corresponding to a user priority. The format is <low>-<high> separated by a ',' where low and high are 0-3F and FF. For Example: 08-0F,00-07,FF-FF,10-1F,20- 27,FF-FF,28-2F,30-3F		
query-response-length- limit <len>	Configures the maximum length of the GAS query response. GAS enables advertisement services that allow the clients to query multiple 802.11 networks at once, while also allowing the client to learn more about a network’s 802.11 infrastructure before associating. If a client transmits a GAS Query using a GAS Initial Request frame, the responding AP will provide the query response (or information on how to receive the query response) in a GAS Initial Response frame.	1-6	1
roam-cons-len-1	Configures the length of the OI. The value of the **roam-cons-len-1** parameter is based upon the number of octets of the **roam-cons-oi-1** field.	**0:** Zero Octets in the OI (Null) **3:** OI length is 24-bits (3 Octets) **5:** OI length is 36-bits (5 Octets)	

Parameter	Description	Range	Default
roam-cons-len-2	Configures the length of the OI. The value of the **roam-cons-len-2** parameter is based upon the number of octets of the **roam-cons-oi-2** field.	**0:** Zero Octets in the OI (Null) **3:** OI length is 24-bits (3 Octets) **5:** OI length is 36-bits (5 Octets)	
roam-cons-len-3	Configures the length of the OI. The value of the **roam-cons-len-3** parameter is based upon the number of octets of the **roam-cons-oi-3** field.	**0:** Zero Octets in the OI (Null) **3:** OI length is 24-bits (3 Octets) **5:** OI length is 36-bits (5 Octets)	
roam-cons-oi-1 roam-cons-oi-2 roam-cons-oi-3	Configures the roaming consortium OI to assign to one of the service provider's top three roaming partners. This additional OI will only be sent to a client if the **addtl-roam-cons-<oisaddtl-roam-cons-ois>** parameter is set to 1 or higher. **NOTE:** The service provider's own roaming consortium OI is configured using the hotspot anqp-roam-cons-profile command.		
venue-group	Configures one of the following venue groups to be advertised in the IEs from APs associated with this hotspot profile. • assembly • business • educational • factory-and-industrial • institutional • mercantile • outdoor • residential • storage • unspecified • utility-misc • vehicular **NOTE:** This parameter only defines the venue group advertised in the IEs from hotspot APs. To define the venue group to be included in ANQP responses, use **anqp-venue-name-profile <profile- name>** command	assembly, business, educational, factory-and- industrial, institutional, mercantile, outdoor, residential, storage, unspecified, utility-and-misc, vehicular	business
venue-type	Specifies the venue type to be advertised in the IEs from APs associated with this hotspot profile. The complete list of supported venue types is described in Creating a Hotspot Profile (Page 458). This parameter only defines the venue type advertised in the IEs from hotspot APs. To define the venue type to be included in ANQP responses, use the hotspot anqp-venue-name-profile<profile-name> command		

36.2.3 Associating an Advertisement Profile to a Hotspot Profile

To associate a hotspot profile with an advertisement profile:

```
(AP)(config)# hotspot hs-profile <name>

(AP)(Hotspot2.0 <name>)# advertisement-protocol <protocol> (AP)(Hotspot2.0 <name>)#
advertisement-profile anqp-3gpp <name>

(AP)(Hotspot2.0 <name>)# advertisement-profile anqp-domain-name <name>

(AP)(Hotspot2.0 <name>)# advertisement-profile anqp-ip-addr-avail <name>

(AP)(Hotspot2.0 <name>)# advertisement-profile anqp-nai-realm <name>

(AP)(Hotspot2.0 <name>)# advertisement-profile anqp-nwk-auth <name>

(AP)(Hotspot2.0 <name>)# advertisement-profile anqp-roam-cons <name>

(AP)(Hotspot2.0 <name>)# advertisement-profile anqp-venue-name <name>

(AP)(Hotspot2.0 <name>)# advertisement-profile h2qp-conn-cap <name>

(AP)(Hotspot2.0 <name>)# advertisement-profile h2qp-oper-class <name>

(AP)(Hotspot2.0 <name>)# advertisement-profile h2qp-oper-name <name>

(AP)(Hotspot2.0 <name>)# advertisement-profile h2qp-osu-provider <name>
```

The configuration parameters for associating an advertisement profile with a hotspot profile are described in the following table:

Table 36- 6 Advertisement Profile Association Parameters

Parameter	Description
advertisement-profile	Specify the advertisement profile to associate with this hotspot profile. For information on advertisement profiles, see Creating Advertisement Profiles for Hotspot Configuration (Page 458).
advertisement-protocol	Specify the advertisement protocol type; for example, specify the ANQP as **anqp**.

36.2.4 Creating a WLAN SSID and Associating Hotspot Profile

To create a WLAN SSID with Enterprise Security and WPA-2 Encryption Settings:

```
(AP)(config)# wlan ssid-profile <name>

(AP)(SSID Profile <name>)# essid <ESSID-name>

(AP)(SSID Profile <name>)# type {<Employee> | <Voice>| <Guest>}

(AP)(SSID Profile <name>)# vlan <vlan-ID>

(AP)(SSID Profile <name>)# set-vlan <attribute>{equals|not-equals|starts-with|ends-
with|contains} <operator> <VLAN-ID>| value-of}

(AP)(SSID Profile <name>)# opmode {wpa2-aes|wpa-tkip,wpa2-aes}

(AP)(SSID Profile <name>)# blacklist

(AP)(SSID Profile <name>)# mac-authentication

(AP)(SSID Profile <name>)# l2-auth-failthrough

(AP)(SSID Profile <name>)# termination

(AP)(SSID Profile <name>)# external-server

(AP)(SSID Profile <name>)# auth-server <server-name>

(AP)(SSID Profile <name>)# server-load-balancing

(AP)(SSID Profile <name>)# radius-accounting

(AP)(SSID Profile <name>)# radius-accounting-mode {user-authentication| user-
association}

(AP)(SSID Profile <name>)# radius-interim-accounting-interval <minutes>

(AP)(SSID Profile <name>)# radius-reauth-interval <minutes>

(AP)(SSID Profile <name>)# set-role-by-ssid
```

36.3 Sample Configuration

Step 1: Creating ANQP and H2QP Advertisement Profiles

```
(AP)# configure terminal

(AP)(config)# hotspot anqp-nai-realm-profile nr1

(AP)(nai-realm "nr1")# nai-realm-name name1

(AP)(nai-realm "nr1")# nai-realm-encoding utf8

(AP)(nai-realm "nr1")# nai-realm-eap-method eap-sim

(AP)(nai-realm "nr1")# nai-realm-auth-id-1 non-eap-inner-auth

(AP)(nai-realm "nr1")# nai-realm-auth-value-1 mschapv2

(AP)(nai-realm "nr1")# nai-home-realm

(AP)(nai-realm "nr1")# exit


(AP)(config)# hotspot anqp-venue-name-profile vn1

(AP)(venue-name "vn1")# venue-group business

(AP)(venue-name "vn1")# venue-type research-and-dev-facility

(AP)(venue-name "vn1")# venue-lang-code eng

(AP)(venue-name "vn1")# venue-name VenueName

(AP)(venue-name "vn1")# exit


(AP)(config)# hotspot anqp-nwk-auth-profile na1

(AP)(network-auth "na1")# nwk-auth-type accept-term-and-cond

(AP)(network-auth "na1")# url www.nwkauth.com

(AP)(network-auth "na1")# exit

(AP)(config)# hotspot anqp-roam-cons-profile rc1

(AP)(roaming-consortium "rc1")# roam-cons-oi-len 3

(AP)(roaming-consortium "rc1")# roam-cons-oi 888888

(AP)(roaming-consortium "rc1")# exit


(AP)(config)# hotspot anqp-3gpp-profile 3g

(AP)(3gpp "3g")# 3gpp-plmn1 40486

(AP)(3gpp "3g")# exit


(AP)(config)# hotspot anqp-ip-addr-avail-profile ip1

(AP)(IP-addr-avail "ip1")# no ipv4-addr-avail
```

```
(AP)(IP-addr-avail "ip1")# ipv6-addr-avail

(AP)(IP-addr-avail "ip1")# exit


(AP)(config)# hotspot anqp-domain-name-profile dn1

(AP)(domain-name "dn1")# domain-name DomainName

(AP)(domain-name "dn1")# exit


(AP)(config)# hotspot h2qp-oper-name-profile on1

(AP)(operator-friendly-name"on1")# op-lang-code eng

(AP)(operator-friendly-name"on1")# op-fr-name OperatorFriendlyName

(AP)(operator-friendly-name"on1")# exit


(AP)(config) # hotspot h2qp-conn-cap-profile cc1

(AP)(connection-capabilities "cc1")# esp-port

(AP)(connection-capabilities "cc1")# icmp

(AP)(connection-capabilities "cc1")# tcp-ftp

(AP)(connection-capabilities "cc1")# tcp-http

(AP)(connection-capabilities "cc1")# tcp-pptp-vpn

(AP)(connection-capabilities "cc1")# tcp-ssh

(AP)(connection-capabilities "cc1")# tcp-tls-vpn

(AP)(connection-capabilities "cc1")# tcp-voip

(AP)(connection-capabilities "cc1")# udp-ike2

(AP)(connection-capabilities "cc1")# udp-ipsec-vpn

(AP)(connection-capabilities "cc1")# udp-voip

(AP)(connection-capabilities "cc1")# enable

(AP)(connection-capabilities "cc1")# exit


(AP)(config) # hotspot h2qp-oper-class-profile oc1

(AP)(operator-class "oc1")# op-class <class-ID>

(AP)(operator-class "oc1")# enable

(AP)(operator-class "oc1")# exit


(AP) (config) # hotspot h2qp-osu-provider-profile osu1

(AP) (osu-provider "osu1") # frnd-name-count 2

(AP) (osu-provider "osu1") # frnd-name1-lang-code "eng"
```

```
(AP) (osu-provider "osu1") # frnd-name1 "SP Red Test Only"

(AP) (osu-provider "osu1") # frnd-name1-hex

(AP) (osu-provider "osu1") # frnd-name2-lang-code "kor"

(AP) (osu-provider "osu1") # frnd-name2 ""

(AP) (osu-provider "osu1") # frnd-name2-hex
535020ebb9a8eab09520ed858cec8aa4ed8ab820eca084ec9aa9

(AP) (osu-provider "osu1") # iconfile-count 2

(AP) (osu-provider "osu1") # icon1-width 128

(AP) (osu-provider "osu1") # icon1-height 61

(AP) (osu-provider "osu1") # icon1-lang-code zxx

(AP) (osu-provider "osu1") # icon1-type image/png

(AP) (osu-provider "osu1") # icon1-file 1 "icon_red_zxx.png"

(AP) (osu-provider "osu1") # icon2-width 160

(AP) (osu-provider "osu1") # icon2-height 76

(AP) (osu-provider "osu1") # icon2-lang-code eng

(AP) (osu-provider "osu1") # icon2-type image/png

(AP) (osu-provider "osu1") # icon2-file 2 "icon_red_eng.png"

(AP) (osu-provider "osu1") # srvcdesc-count 2

(AP) (osu-provider "osu1") # srvc-desc1-lang-code eng

(AP) (osu-provider "osu1") # srvc-desc1 "Free service for test purpose"

(AP) (osu-provider "osu1") # srvc-desc1-hex

(AP) (osu-provider "osu1") # srvc-desc2-lang-code kor

(AP) (osu-provider "osu1") # srvc-desc2 ""

(AP) (osu-provider "osu1") # srvc-desc2-hex
ed858cec8aa4ed8ab820ebaaa9eca081ec9cbceba19c20ebacb4eba38c20ec849cebb984ec8aa4

(AP) (osu-provider "osu1") # osu-server-uri https://osu-server.r2-testbed-aru.wi-
fi.org:443/guest/HotSpot2OnlineSignUp.php

(AP) (osu-provider "osu1") # osu-method SOAP-XML (AP)(WAN-metrics "osu1")# exit


(AP)(config)# hotspot h2qp-wan-metrics-profile wm1

(AP)(WAN-metrics "wm1")# at-capacity

(AP)(WAN-metrics "wm1")# downlink-load <load>

(AP)(WAN-metrics "wm1")# downlink-speed <speed>

(AP)(WAN-metrics "wm1")# load-duration <duration>

(AP)(WAN-metrics "wm1")# symm-link
```

```
(AP)(WAN-metrics "wm1")# uplink-load <load>

(AP)(WAN-metrics "wm1")# uplink-speed <speed>

(AP)(WAN-metrics "wm1")# wan-metrics-link-status <status>

(AP)(WAN-metrics "wm1")# exit
```

Step 2: Creating a hotspot profile

```
(AP)# configure terminal

(AP)(config)# hotspot hs-profile hs1 (AP)(Hotspot2.0 "hs1")# enable (AP)(Hotspot2.0
"hs1")# comeback-mode

(AP)(Hotspot2.0 "hs1")# gas-comeback-delay 100

(AP)(Hotspot2.0 "hs1")# no asra

(AP)(Hotspot2.0 "hs1")# no internet (AP)(Hotspot2.0 "hs1")# osu-ssid OSU-SSID

(AP)(Hotspot2.0 "hs1")# qos-map-excp 35-2,16-6

(AP)(Hotspot2.0 "hs1")# qos-map-range 08-0F,00-07,FF-FF,10-1F,20-27,FF-FF,28-2F,30-3F

(AP)(Hotspot2.0 "hs1")# query-response-length-limit 2

(AP)(Hotspot2.0 "hs1")# access-network-type chargeable-public

(AP)(Hotspot2.0 "hs1")# roam-cons-len-1 3

(AP)(Hotspot2.0 "hs1")# roam-cons-oi-1 123456

(AP)(Hotspot2.0 "hs1")# roam-cons-len-2 3

(AP)(Hotspot2.0 "hs1")# roam-cons-oi-2 223355

(AP)(Hotspot2.0 "hs1")# addtl-roam-cons-ois 0

(AP)(Hotspot2.0 "hs1")# venue-group business

(AP)(Hotspot2.0 "hs1")# venue-type research-and-dev-facility

(AP)(Hotspot2.0 "hs1")# pame-bi

(AP)(Hotspot2.0 "hs1")# group-frame-block

(AP)(Hotspot2.0 "hs1")# p2p-dev-mgmt (AP)(Hotspot2.0 "hs1")# p2p-cross-connect
```

Step 3 (Optional): Creating a hotspot profile for OSEN

```
(AP) (config) # hotspot hs-profile hs2

(AP) (Hotspot2.0 "hs2") # osen

(AP) (Hotspot2.0 "hs2") # no enable
```

Step 4: Associating advertisement profiles with the hotspot profile

```
(AP)# configure terminal

(AP)(config)# hotspot hs-profile hs1

(AP)(Hotspot2.0 "hs1")# advertisement-profile anqp-nai-realm-profile nr1

(AP)(Hotspot2.0 "hs1")# advertisement-profile anqp-venue-name-profile vn1
```

```
(AP)(Hotspot2.0 "hs1")# advertisement-profile anqp-nwk-auth-profile na1

(AP)(Hotspot2.0 "hs1")# advertisement-profile anqp-roam-cons-profile rc1

(AP)(Hotspot2.0 "hs1")# advertisement-profile anqp-3gpp-profile 3g1

(AP)(Hotspot2.0 "hs1")# advertisement-profile anqp-ip-addr-avail-profile ip1

(AP)(Hotspot2.0 "hs1")# advertisement-profile anqp-domain-name-profile dn1

(AP)(Hotspot2.0 "hs1")# advertisement-profile h2qp-oper-name-profile on1

(AP)(Hotspot2.0 "hs1")# advertisement-profile h2qp-wan-metrics-profile wm1

(AP)(Hotspot2.0 "hs1")# advertisement-profile h2qp-conn-cap-profile cc1

(AP)(Hotspot2.0 "hs1")# advertisement-profile h2qp-oper-class-profile oc1

(AP)(Hotspot2.0 "hs1")# advertisement-profile h2qp-osu-provider-profile osu1
```

Step 5: Associating the hotspot profile with production WLAN SSID:

```
(AP)# configure terminal

(AP)# wlan ssid-profile ssidProfile1

(AP)(SSID Profile "ssidProfile1")# essid hsProf

(AP)(SSID Profile "ssidProfile1")# type employee

(AP)(SSID Profile "ssidProfile1")# vlan 200

(AP)(SSID Profile "ssidProfile1")# opmode wpa2-aes

(AP)(SSID Profile "ssidProfile1")# auth-server RADIUS1

(AP)(SSID Profile "ssidProfile1")# hotspot-profile hs1
```

Step 6 (Only if Step 3 is configured): Associating OSEN hotspot profile with an SSID that broadcasts OSEN capable network:

```
(AP)# configure terminal

(AP)# wlan ssid-profile OSU-SSID

(AP)(SSID Profile "OSU-SSID")# hotspot-profile hs2
```

Note

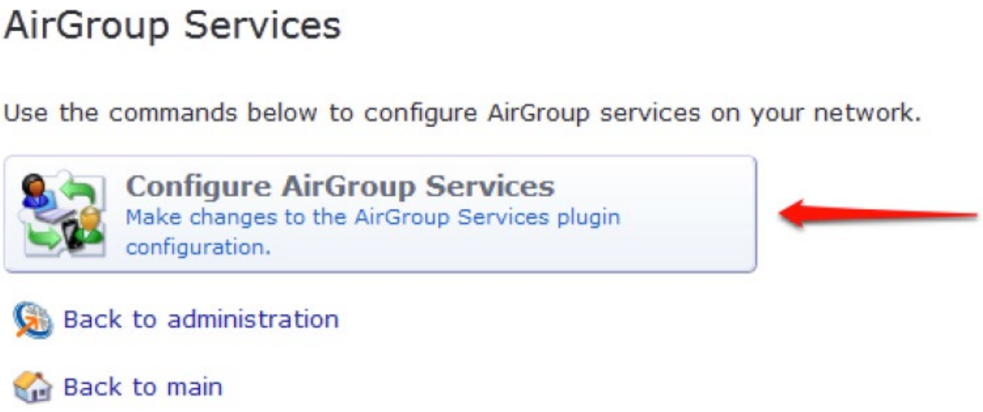
OSU ESS can either be open or encrypted. When OSU ESS is using open encryption, create an SSID profile with the same name as provided in the hotspot profile and set the operation mode to open. When OSU ESS is encypted, create a hotspot profile with only **osen** enabled and attach it to an SSID that broadcasts OSEN capable network. In this case, choose the operation mode to WPA2-AES.

ClearPass Guest Setup 37

37.1 Configuring ClearPass Guest

To configure ClearPass Guest:

1. From the ClearPass Guest UI, navigate to **Administration > AirGroup Services**.
2. Click **Configure AirGroup Services**.



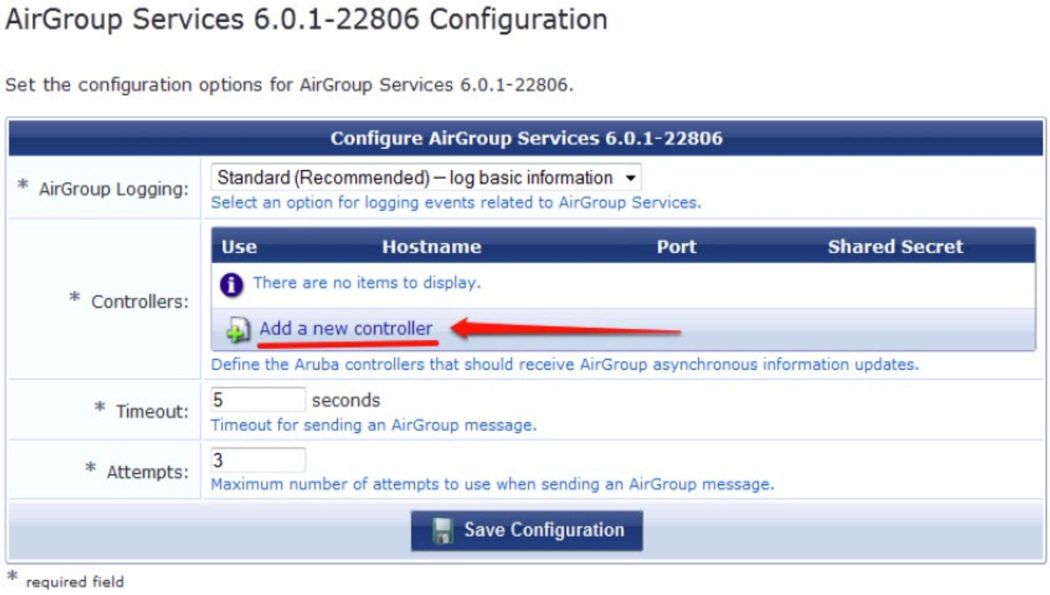
AirGroup Services

Use the commands below to configure AirGroup services on your network.

Configure AirGroup Services
Make changes to the AirGroup Services plugin configuration.
Back to administration
Back to main

Figure 38-1 Configure AirGroup Services

3. Click **Add a new controller**.



AirGroup Services 6.0.1-22806 Configuration

Set the configuration options for AirGroup Services 6.0.1-22806.

Configure AirGroup Services 6.0.1-22806

* AirGroup Logging: Standard (Recommended) — log basic information
Select an option for logging events related to AirGroup Services.

* Controllers:

Use	Hostname	Port	Shared Secret
There are no items to display.			

Add a new controller

Define the Aruba controllers that should receive AirGroup asynchronous information updates.

* Timeout: 5 seconds
Timeout for sending an AirGroup message.

* Attempts: 3
Maximum number of attempts to use when sending an AirGroup message.

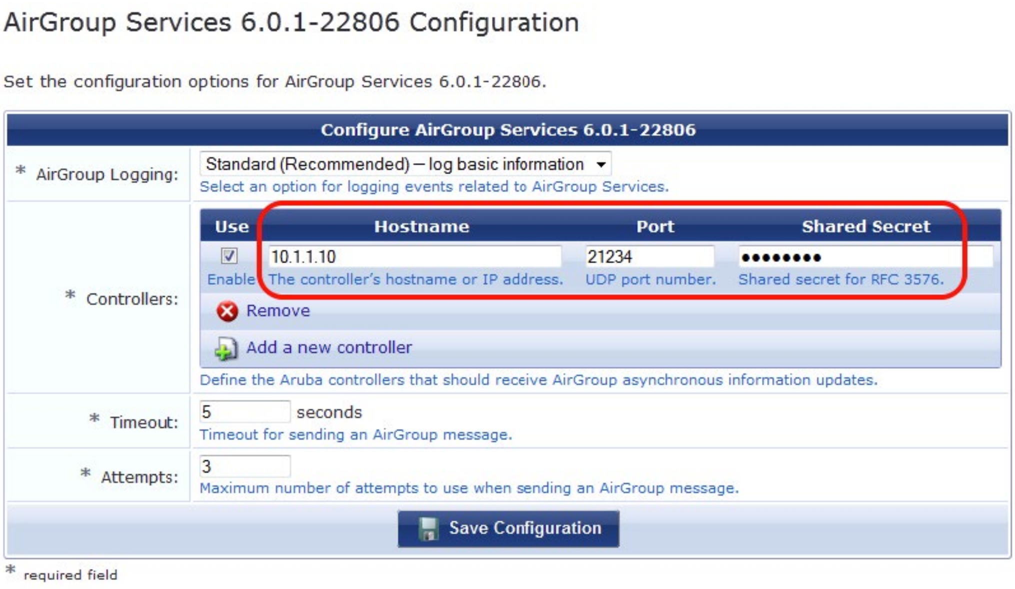
* required field

Figure 38-2 Add a New Controller for AirGroup Services

4. Update the parameters with appropriate values.

Note

Ensure that the port configured matches the CoA port (RFC 3576) set on the AP configuration.



AirGroup Services 6.0.1-22806 Configuration

Set the configuration options for AirGroup Services 6.0.1-22806.

Configure AirGroup Services 6.0.1-22806

* AirGroup Logging: Standard (Recommended) — log basic information
Select an option for logging events related to AirGroup Services.

* Controllers:

Use	Hostname	Port	Shared Secret
☑ Enable	10.1.1.10 The controller's hostname or IP address.	21234 UDP port number.	●●●●●●●● Shared secret for RFC 3576.

Define the Aruba controllers that should receive AirGroup asynchronous information updates.

* Timeout: 5 seconds
Timeout for sending an AirGroup message.

* Attempts: 3
Maximum number of attempts to use when sending an AirGroup message.

* required field

Figure 38-3 Configure AirGroup Services: Controller Settings

5. Click **Save Configuration**.

In order to demonstrate AirGroup, either an AirGroup Administrator or an AirGroup Operator account must be created.

Creating AirGroup Administrator and Operator Account

To create a AirGroup administrator and AirGroup operator account using the ClearPass Policy Manager UI:

1. Navigate to the ClearPass Policy Manager UI, and navigate to **Configuration > Identity > Local Users**.

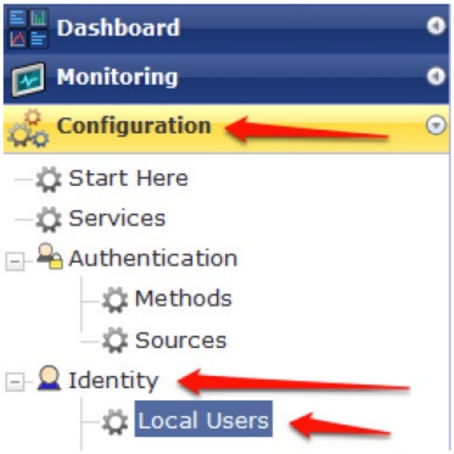
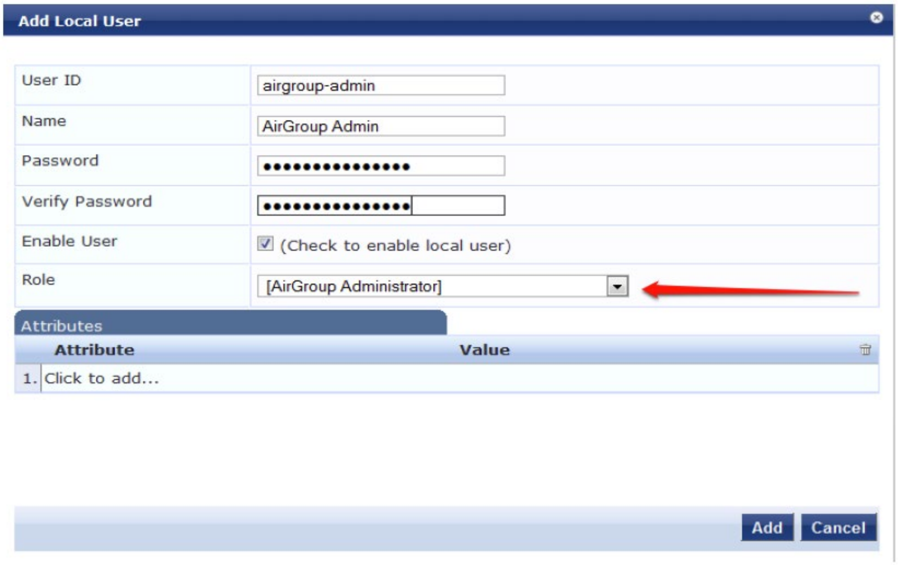


Figure 38-4 Configuration > Identity > Local Users Selection

2. Click **Add User**.
3. Create an **AirGroup Administrator** by entering the required values.



Add Local User

User ID	airgroup-admin
Name	AirGroup Admin
Password	●●●●●●●●●●●●●●●
Verify Password	●●●●●●●●●●●●●●●
Enable User	☑ (Check to enable local user)
Role	[AirGroup Administrator]

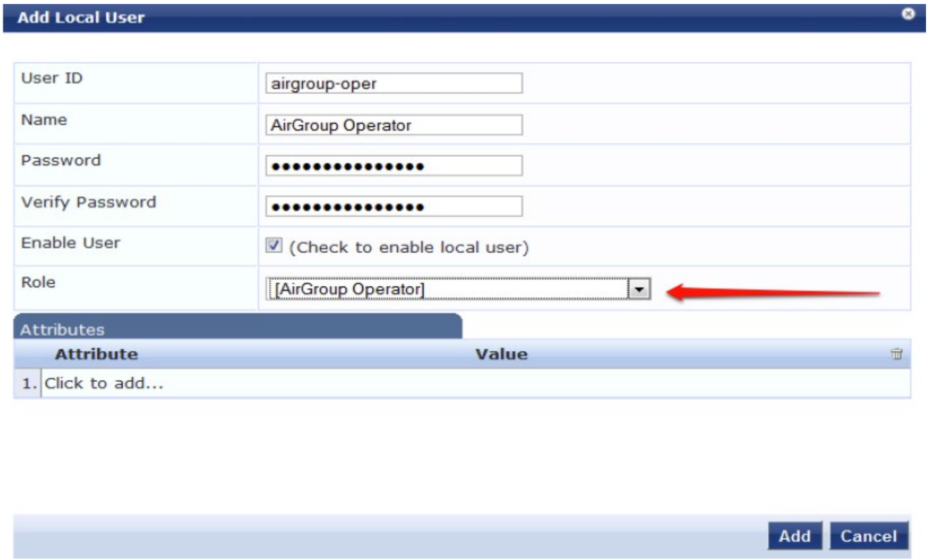
Attributes

	Attribute	Value
1.	Click to add...	

Figure 38-5 Create an AirGroup Administrator

4. Click **Add**.

5. Now click **Add User** to create an **AirGroup Operator**.



Add Local User

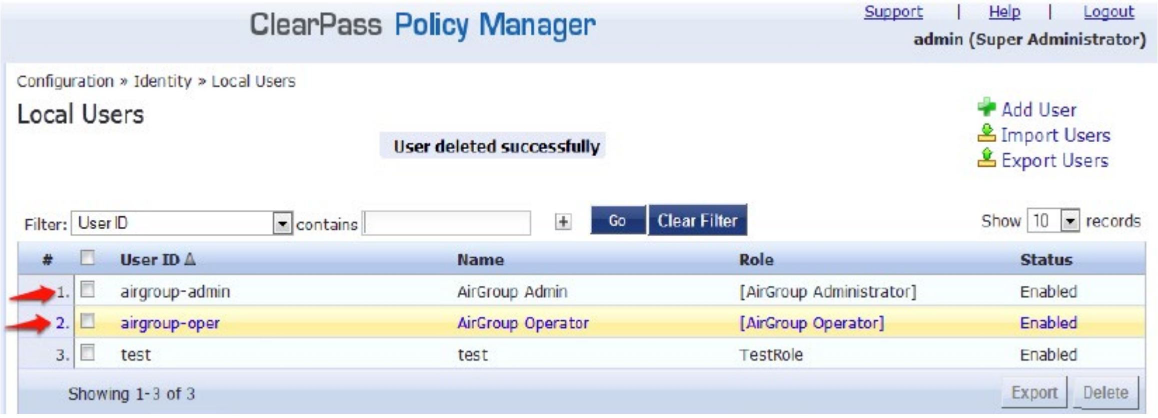
User ID	airgroup-oper
Name	AirGroup Operator
Password	●●●●●●●●●●●●●●●●
Verify Password	●●●●●●●●●●●●●●●●
Enable User	☑ (Check to enable local user)
Role	[AirGroup Operator]

Attributes

	Attribute	Value
1.	Click to add...	

Figure 38-6 Create an AirGroup Operator

6. Click **Add** to save the user with an **AirGroup Operator** role. The **AirGroup Administrator** and **AirGroup Operator IDs** will be displayed in the **Local Users** UI screen.



ClearPass Policy Manager

admin (Super Administrator)

Configuration » Identity » Local Users

Local Users

User deleted successfully

Filter: User ID contains

Show 10 records

#	□	User ID ∆	Name	Role	Status
1.	□	airgroup-admin	AirGroup Admin	[AirGroup Administrator]	Enabled
2.	□	airgroup-oper	AirGroup Operator	[AirGroup Operator]	Enabled
3.	□	test	test	TestRole	Enabled

Showing 1-3 of 3

Figure 38-7 Local Users UI Screen

7. Navigate to the ClearPass Guest UI and click **Logout**. The **ClearPass Guest Login** page is displayed. Use the AirGroup admin credentials to log in.

8. After logging in, click **Create Device**.

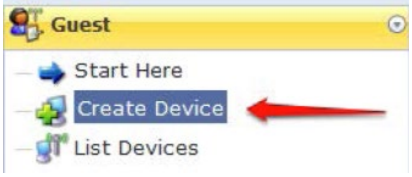
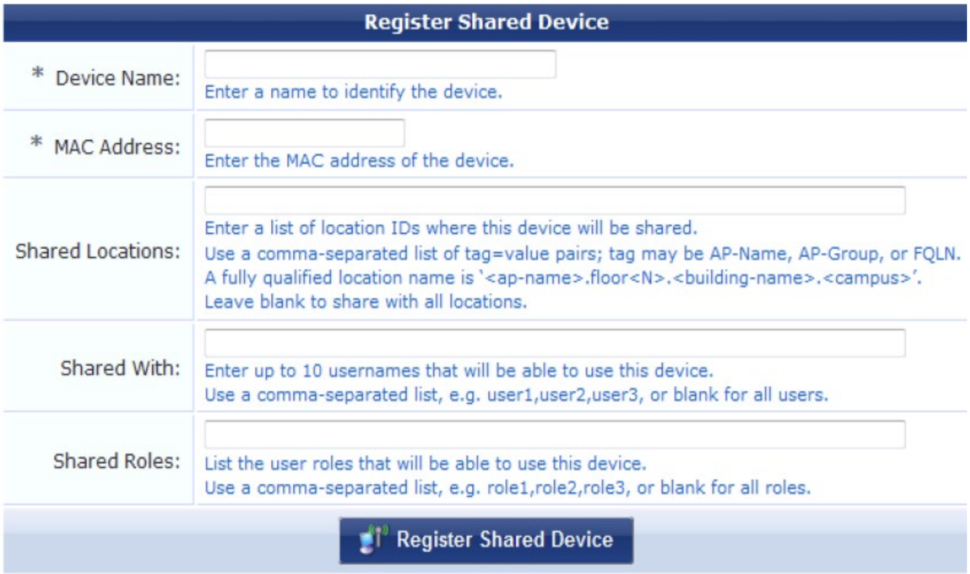


Figure 38-8 Create a Device

The **Register Shared Device** page is displayed.



Register Shared Device

* Device Name:	Enter a name to identify the device.
* MAC Address:	Enter the MAC address of the device.
Shared Locations:	Enter a list of location IDs where this device will be shared. Use a comma-separated list of tag=value pairs; tag may be AP-Name, AP-Group, or FQLN. A fully qualified location name is '<ap-name>.floor<N>.<building-name>.<campus>'. Leave blank to share with all locations.
Shared With:	Enter up to 10 usernames that will be able to use this device. Use a comma-separated list, e.g. user1,user2,user3, or blank for all users.
Shared Roles:	List the user roles that will be able to use this device. Use a comma-separated list, e.g. role1,role2,role3, or blank for all roles.

Figure 38-9 ClearPass Guest- Register Shared Device

For this test, add your AppleTV device name and MAC address but leave all other boxes empty

9. Click **Register Shared Device**.

37.2 Verifying ClearPass Guest Setup

1. Disconnect your AppleTV and OSX Mountain Lion or iOS 6 devices if they were previously connected to the wireless network. Remove their entries from the controller’s user table using these commands:
   – Find the MAC address—**show user table**
   – Delete the address from the table—**aaa user delete mac 00:aa:22:bb:33:cc**
2. Reconnect both devices. To limit access to the AppleTV, access the ClearPass Guest UI using either the AirGroup admin or the AirGroup operator credentials. Next, navigate to **List Devices > Test Apple TV > Edit**. Add a username that is not used to log in to the Apple devices in the **Shared With** box.
3. Disconnect and remove the OSX Mountain Lion or iOS 6 device from the controller’s user table. Reconnect the device by not using the username that you added to the **Shared With** box. The AppleTV should not be available to this device.
4. Disconnect the OSX Mountain Lion or iOS 6 device and delete it from the controller’s user table. Reconnect using the username that was added to the **Shared With** box. The OSX Mountain Lion or iOS 6 device should once again have access to the AppleTV.

37.3 Troubleshooting

Table 38- 1 Troubleshooting

Problem	Solution
Limiting devices has no effect.	Ensure IPv6 is disabled.
Apple Macintosh running Mountain Lion can use AirPlay but iOS devices cannot.	Ensure IPv6 is disabled.

Appendix A

A.1 Glossary of terms

The following table provides a brief description of the terminology used in this guide.

3DES	Triple Data Encryption Standard. 3DES is a symmetric-key block cipher that applies the DES cipher algorithm three times to each data block.
3G	Third Generation of Wireless Mobile Telecommunications Technology. See W-CDMA.
3GPP	Third Generation Partnership Project. 3GPP is a collaborative project aimed at developing globally acceptable specifications for third generation mobile systems.
4G	Fourth Generation of Wireless Mobile Telecommunications Technology. See LTE.
802.11	802.11 is an evolving family of specifications for wireless LANs developed by a working group of the Institute of Electrical and Electronics Engineers (IEEE). 802.11 standards use the Ethernet protocol and Carrier Sense Multiple Access with collision avoidance (CSMA/CA) for path sharing.
802.11 bSec	802.11 bSec is an alternative to 802.11i. The difference between bSec and standard 802.11i is that bSec implements Suite B algorithms wherever possible. Notably, Advanced Encryption Standard-Counter with CBC- MAC is replaced by Advanced Encryption Standard - Galois/Counter Mode, and the Key Derivation Function (KDF) of 802.11i is upgraded to support SHA-256 and SHA-384.
802.11a	802.11a provides specifications for wireless systems. Networks using 802.11a operate at radio frequencies in the 5 GHz band. The specification uses a modulation scheme known as orthogonal frequency-division multiplexing (OFDM) that is especially well suited to use in office settings. The maximum data transfer rate is 54 Mbps.
802.11ac	802.11ac is a wireless networking standard in the 802.11 family that provides high-throughput WLANs on the 5 GHz band.
802.11b	802.11b is a WLAN standard often called Wi-Fi and is backward compatible with 802.11. Instead of the Phase- Shift Keying (PSK) modulation method used in 802.11 standards, 802.11b uses Complementary Code Keying (CCK) that allows higher data speeds and makes it less susceptible to multi-path-propagation interference. 802.11b operates in the 2.4 GHz band and the maximum data transfer rate is 11 Mbps.
802.11d	802.11d is a wireless network communications specification for use in countries where systems using other standards in the 802.11 family are not allowed to operate. Configuration can be fine-tuned at the Media Access Control (MAC) layer level to comply with the rules of the country or district in which the network is to be used. Rules are subject to variation and include allowed frequencies, allowed power levels, and allowed signal bandwidth. 802.11d facilitates global roaming.

802.11e

802.11e is an enhancement to the 802.11a and 802.11b specifications that enhances the 802.11 Media Access Control layer with a coordinated Time Division Multiple Access (TDMA) construct. It adds error- correcting mechanisms for delay-sensitive applications such as voice and video. The 802.11e specification provides seamless interoperability between business, home, and public environments such as airports and hotels, and offers all subscribers high-speed Internet access with full-motion video, high-fidelity audio, and VoIP.

802.11g

802.11g offers transmission over relatively short distances at up to 54 Mbps, compared with the 11 Mbps theoretical maximum of 802.11b standard. 802.11g employs Orthogonal Frequency Division Multiplexing (OFDM), the modulation scheme used in 802.11a, to obtain higher data speed. Computers or terminals set up for 802.11g can fall back to speed of 11 Mbps, so that 802.11b and 802.11g devices can be compatible within a single network.

802.11h

802.11h is intended to resolve interference issues introduced by the use of 802.11a in some locations, particularly with military Radar systems and medical devices. Dynamic Frequency Selection (DFS) detects the presence of other devices on a channel and automatically switches the network to another channel if and when such signals are detected. Transmit Power Control (TPC) reduces the radio frequency (RF) output power of each network transmitter to a level that minimizes the risk of interference.

802.11i

802.11i provides improved encryption for networks that use 802.11a, 802.11b, and 802.11g standards. It requires new encryption key protocols, known as Temporal Key Integrity Protocol (TKIP) and Advanced Encryption Standard (AES).

802.11j

802.11j is a proposed addition to the 802.11 family of standards that incorporates Japanese regulatory extensions to 802.11a the main intent is to add channels in the radio frequency (RF) band of 4.9 GHz to 5.0 GHz.

802.11k

802.11k is an IEEE standard that enables APs and client devices to discover the best available radio resources for seamless BSS transition in a WLAN.

802.11m

802.11m is an Initiative to perform editorial maintenance, corrections, improvements, clarifications, and interpretations relevant to documentation for 802.11 family specifications.

802.11n

802.11n is a wireless networking standard to improve network throughput over the two previous standards, 802.11a and 802.11g. With 802.11n, there will be a significant increase in the maximum raw data rate from 54 Mbps to 600 Mbps with the use of four spatial streams at a channel width of 40 MHz.

802.11r

802.11r is an IEEE standard for enabling seamless BSS transitions in a WLAN. 802.11r standard is also referred to as Fast BSS transition.

802.11u

802.11u is an amendment to the IEEE 802.11 WLAN standards for connection to external networks using common wireless devices such as smartphones and tablet PCs. The 802.11u protocol provides wireless clients with a streamlined mechanism to discover and authenticate to suitable networks, and allows mobile users to roam between partner networks without additional authentication. An 802.11u-capable device supports the Passpoint technology from the Wi-Fi Alliance Hotspot 2.0 R2 Specification that simplifies and automates access to public Wi-Fi.

802.11v	802.11v is an IEEE standard that allows client devices to exchange information about the network topology and RF environment. This information is used for assigning best available radio resources for the client devices to provide seamless connectivity.
802.1Q	802.1Q is an IEEE standard that enables the use of VLANs on an Ethernet network. 802.1Q supports VLAN tagging.
802.1X	802.1X is an IEEE standard for port-based network access control designed to enhance 802.11 WLAN security. 802.1X provides an authentication framework that allows a user to be authenticated by a central authority.
802.3af	802.3af is an IEEE standard for Power over Ethernet (PoE) version that supplies up to 15.4W of DC power. See PoE.
802.3at	802.3at is an IEEE standard for PoE version that supplies up to 25.5W of DC power. See PoE+.
AAA	Authentication, Authorization, and Accounting. AAA is a security framework to authenticate users, authorize the type of access based on user credentials, and record authentication events and information about the network access and network resource consumption.
ABR	Area Border Router. ABR is used for establishing connection between the backbone networks and the Open Shortest Path First (OSPF) areas. ABR is located near the border of one or more OSPF areas.
AC	Access Category. As per the IEEE 802.11e standards, AC refers to various levels of traffic prioritization in Enhanced Distributed Channel Access (EDCA) operation mode. The WLAN applications prioritize traffic based on the Background, Best Effort, Video, and Voice access categories. AC can also refer to Alternating Current, a form of electric energy that flows when the appliances are plugged to a wall socket.
ACC	Advanced Cellular Coexistence. The ACC feature in APs enable WLANs to perform at peak efficiency by minimizing interference from 3G/4G/LTE networks, distributed antenna systems, and commercial small cell/femtocell equipment.
Access-Accept	Response from the RADIUS server indicating successful authentication and containing authorization information.
Access-Reject	Response from RADIUS server indicating that a user is not authorized.
Access-Request	RADIUS packet sent to a RADIUS server requesting authorization.
Accounting-Request	RADIUS packet type sent to a RADIUS server containing accounting summary information.
Accounting-Response	RADIUS packet sent by the RADIUS server to acknowledge receipt of an Accounting-Request.
ACE	Access Control Entry. ACE is an element in an ACL that includes access control information.
ACI	Adjacent Channel Interference. ACI refers to interference or interruptions detected on a broadcasting channel, caused by too much power on an adjacent channel in the spectrum.
ACL	Access Control List. ACL is a common way of restricting certain types of traffic on a physical port.

Active Directory Microsoft Active Directory. The directory server that stores information about a variety of things, such as organizations, sites, systems, users, shares, and other network objects or components. It also provides authentication and authorization mechanisms, and a framework within which related services can be deployed.

ActiveSync Mobile data synchronization app developed by Microsoft that allows a mobile device to be synchronized with either a desktop or a server running compatible software products.

ad hoc network An ad hoc network is a network composed of individual devices communicating with each other directly. Many ad hoc networks are Local Area Networks (LANs) where computers or other devices are enabled to send data directly to one another rather than going through a centralized access point.

ADO Active X Data Objects is a part of Microsoft Data Access Components (MDACs) that enables client applications to access data sources through an (Object Linking and Embedding Database) OLE DB provider. ADO supports key features for building client-server and Web-based applications.

ADP Aruba Discovery Protocol. ADP is an Aruba proprietary Layer 2 protocol. It is used by the APs to obtain the IP address of the TFTP server from which it downloads the AP boot image.

AES Advanced Encryption Standard. AES is an encryption standard used for encrypting and protecting electronic data. The AES encrypts and decrypts data in blocks of 128 bits (16 bytes), and can use keys of 128 bits, 192 bits, and 256 bits.

AIFSN Arbitrary Inter-frame Space Number. AIFSN is set by the AP in beacon frames and probe responses. AIFS is a method of prioritizing a particular category of traffic over the other, for example prioritizing voice or video messages over email.

AirGroup The application that allows the end users to register their personal mobile devices on a local network and define a group of friends or associates who are allowed to share them. AirGroup is primarily designed for colleges and other institutions. AirGroup uses zero configuration networking to allow Apple mobile devices, such as the AirPrint wireless printer service and the AirPlay mirroring service, to communicate over a complex access network topology.

AirWave Management Client AirWave Management Client is a Windows software utility that enables client devices (such as a laptop) to act as passive RF sensors and augments the AirWave RAPIDS module.

ALE Analytics and Location Engine. ALE gives visibility into everything the wireless network knows. This enables customers and partners to gain a wealth of information about the people on their premises. This can be very important for many different verticals and use cases. ALE includes a location engine that calculates associated and unassociated device location periodically using context streams, including RSSI readings, from WLAN controllers or SCALANCE W clusters.

ALG Application Layer Gateway. ALG is a security component that manages application layer protocols such as SIP, FTP and so on.

AM Air Monitor. AM is a mode of operation supported on wireless APs. When an AP operates in the Air Monitor mode, it enhances the wireless networks by collecting statistics, monitoring traffic, detecting intrusions, enforcing security policies, balancing wireless traffic load, self-healing coverage gaps, and more. However, clients cannot connect to APs operating in the AM mode.

AMON Advanced Monitoring. AMON is used in Aruba WLAN deployments for improved network management, monitoring and diagnostic capabilities.

AMP AirWave Management Platform. AMP is a network management system for configuring, monitoring, and upgrading wired and wireless devices on your network.

A-MPDU Aggregate MAC Protocol Data Unit. A-MPDU is a method of frame aggregation, where several MPDUs are combined into a single frame for transmission.

A-MSDU Aggregate MAC Service Data Unit. A-MSDU is a structure containing multiple MSDUs, transported within a single (unfragmented) data MAC MPDU.

ANQP Access Network Query Protocol. ANQP is a query and a response protocol for Wi-Fi hotspot services. ANQP includes information Elements (IEs) that can be sent from the AP to the client to identify the AP network and service provider. The IEs typically include information about the domain name of the AP operator, the IP addresses available at the AP, and information about potential roaming partners accessible through the AP. If the client responds with a request for a specific IE, the AP will send a Generic Advertisement Service (GAS) response frame with the configured ANQP IE information.

ANSI American National Standards Institute. It refers to the ANSI compliance standards for products, systems, services, and processes.

API Application Programming Interface. Refers to a set of functions, procedures, protocols, and tools that enable users to build application software.

app Short form for application. It generally refers to the application that is downloaded and used on mobile devices.

ARM Adaptive Radio Management. ARM dynamically monitors and adjusts the network to ensure that all users are allowed ready access. It enables full utilization of the available spectrum to support maximum number of users by intelligently choosing the best RF channel and transmit power for APs in their current RF environment.

ARP Address Resolution Protocol. ARP is used for mapping IP network address to the hardware MAC address of a device.

ASCII American Standard Code for Information Interchange. An ASCII code is a numerical representation of a character or an action.

band Band refers to a specified range of frequencies of electromagnetic radiation.

BGP Border Gateway Protocol. BGP is a routing protocol for exchanging data and information between different host gateways or autonomous systems on the Internet.

BLE Bluetooth Low Energy. The BLE functionality is offered by BluetoothÂ® to enable devices to run for long durations with low power consumption.

BMC Beacon Management Console. BMC manages and monitors beacons from the BLE devices. The BLE devices are used for location tracking and proximity detection.

BPDU Bridge Protocol Data Unit. A BPDU is a data message transmitted across a local area network to detect loops in network topologies.

B-RAS Broadband Remote Access Server. A B-RAS is a server that facilitates and converges traffic from multiple Internet traffic resources such as cable, DSL, Ethernet, or Broadband wireless.

BRE Basic Regular Expression. The BRE syntax standards designed by the IEEE provides extension to the traditional Simple Regular Expressions syntax and allows consistency between utility programs such as grep, sed, and awk.

BSS Basic Service Set. A BSS is a set of interconnected stations that can communicate with each other. BSS can be an independent BSS or infrastructure BSS. An independent BSS is an ad hoc network that does not include APs, whereas the infrastructure BSS consists of an AP and all its associated clients.

BSSID Basic Service Set Identifier. The BSSID identifies a particular BSS within an area. In infrastructure BSS networks, the BSSID is the MAC address of the AP. In independent BSS or ad hoc networks, the BSSID is generated randomly.

BYOD Bring Your Own Device. BYOD refers to the use of personal mobile devices within an enterprise network infrastructure.

CA Certificate Authority or Certification Authority. Entity in a public key infrastructure system that issues certificates to clients. A certificate signing request received by the CA is converted into a certificate when the CA adds a signature generated with a private key. See digital certificate.

CAC Call Admission Control. CAC regulates traffic volume in voice communications. CAC can also be used to ensure or maintain a certain level of audio quality in voice communications networks.

CALEA Communications Assistance for Law Enforcement Act. To comply with the CALEA specifications and to allow lawful interception of Internet traffic by the law enforcement and intelligence agencies, the telecommunications carriers and manufacturers of telecommunications equipment are required to modify and design their equipment, facilities, and services to ensure that they have built-in surveillance capabilities.

Campus AP Campus APs are used in private networks where APs connect over private links (LAN, WLAN, WAN or MPLS) and terminate directly on controllers. Campus APs are deployed as part of the indoor campus solution in enterprise office buildings, warehouses, hospitals, universities, and so on.

captive portal A captive portal is a web page that allows the users to authenticate and sign in before connecting to a public- access network. Captive portals are typically used by business centers, airports, hotel lobbies, coffee shops, and other venues that offer free Wi-Fi hotspots for the guest users.

CCA Clear Channel Assessment. In wireless networks, the CCA method detects if a channel is occupied or clear, and determines if the channel is available for data transmission.

CDP Cisco Discovery Protocol. CDP is a proprietary Data Link Layer protocol developed by Cisco Systems. CDP runs on Cisco devices and enables networking applications to learn about the neighboring devices directly connected to the network.

CDR	Call Detail Record. A CDR contains the details of a telephone or VoIP call, such as the origin and destination addresses of the call, the start time and end time of the call, any toll charges that were added through the network or charges for operator services, and so on.
CEF	Common Event Format. The CEF is a standard for the interoperability of event or log-generating devices and applications. The standard syntax for CEF includes a prefix and a variable extension formatted as key-value pairs.
CGI	Common Gateway Interface. CGI is a standard protocol for exchanging data between the web servers and executable programs running on a server to dynamically process web pages.
CHAP	Challenge Handshake Authentication Protocol. CHAP is an authentication scheme used by PPP servers to validate the identity of remote clients.
CIDR	Classless Inter-Domain Routing. CIDR is an IP standard for creating and allocating unique identifiers for networks and devices. The CIDR IP addressing scheme is used as a replacement for the older IP addressing scheme based on classes A, B, and C. With CIDR, a single IP address can be used to designate many unique IP addresses. A CIDR IP address ends with a slash followed by the IP network prefix, for example, 192.0.2.0/24.
ClearPass	ClearPass is an access management system for creating and enforcing policies across a network to all devices and applications. The ClearPass integrated platform includes applications such as Policy Manager, Guest, Onboard, OnGuard, Insight, Profile, QuickConnect, and so on.
ClearPass Guest	ClearPass Guest is a configurable ClearPass application for secure visitor network access management.
ClearPass Policy Manager	ClearPass Policy Manager is a baseline platform for policy management, AAA, profiling, network access control, and reporting. With ClearPass Policy Manager, the network administrators can configure and manage secure network access that accommodates requirements across multiple locations and multivendor networks, regardless of device ownership and connection method.
CLI	Command-Line Interface. A console interface with a command line shell that allows users to execute text input as commands and convert these commands to appropriate functions.
CN	Common Name. CN is the primary name used to identify a certificate.
CNA	Captive Network Assistant. CNA is a popup page shown when joining a network that has a captive portal.
CoA	Change of Authorization. The RADIUS CoA is used in the AAA service framework to allow dynamic modification of the authenticated, authorized, and active subscriber sessions.
CoS	Class of Service. CoS is used in data and voice protocols for classifying packets into different types of traffic (voice, video, or data) and setting a service priority. For example, voice traffic can be assigned a higher priority over email or HTTP traffic.
CPE	Customer Premises Equipment. It refers to any terminal or equipment located at the customer premises.

CPsec Control Plane Security. CPsec is a secure form of communication between a controller and APs to protect the control plane communications. This is performed by means of using public-key self-signed certificates created by each master controller.

CPU Central Processing Unit. A CPU is an electronic circuitry in a computer for processing instructions.

CRC Cyclic Redundancy Check. CRC is a data verification method for detecting errors in digital data during transmission, storage, or retrieval.

CRL Certificate Revocation List. CRL is a list of revoked certificates maintained by a certification authority.

cryptobinding Short for cryptographic binding. A procedure in a tunneled EAP method that binds together the tunnel protocol and the tunneled authentication methods, ensuring the relationship between a collection of data assets. Cryptographic binding focuses on protecting the server; mutual cryptographic binding protects both peer and server.

CSA Channel Switch Announcement. The CSA element enables an AP to advertise that it is switching to a new channel before it begins transmitting on that channel. This allows the clients, which support CSA, to transition to the new channel with minimal downtime.

CSMA/CA Carrier Sense Multiple Access / Collision Avoidance. CSMA/CA is a protocol for carrier transmission in networks using the 802.11 standard. CSMA/CA aims to prevent collisions by listening to the broadcasting nodes, and informing devices not to transmit any data until the broadcasting channel is free.

CSR Certificate Signing Request. In PKI systems, a CSR is a message sent from an applicant to a CA to apply for a digital identity certificate.

CSV Comma-Separated Values. A file format that stores tabular data in the plain text format separated by commas.

CTS Clear to Send. The CTS refers to the data transmission and protection mechanism used by the 802.11 wireless networking protocol to prevent frame collision occurrences. See RTS.

CW Contention Window. In QoS, CW refers to a window set for access categories based on the type of traffic. Based on the type and volume of the traffic, the minimum and maximum values can be calculated to provide a wider window when necessary.

DAI Dynamic ARP inspection. A security feature that validates ARP packets in a network.

DAS Distributed Antenna System. DAS is a network of antenna nodes strategically placed around a geographical area or structure for additional cellular coverage.

dB Decibel. Unit of measure for sound or noise and is the difference or ratio between two signal levels.

dBm Decibel-Milliwatts. dBm is a logarithmic measurement (integer) that is typically used in place of mW to represent receive-power level. AMP normalizes all signals to dBm, so that it is easy to evaluate performance between various vendors.

DCB Data Center Bridging. DCB is a collection of standards developed by IEEE for creating a converged data center network using Ethernet.

DCE	Data Communication Equipment. DCE refers to the devices that establish, maintain, and terminate communication network sessions between a data source and its destination.
DCF	Distributed Coordination Function. DCF is a protocol that uses carrier sensing along with a four-way handshake to maximize the throughput while preventing packet collisions.
DDMO	Distributed Dynamic Multicast Optimization. DDMO is similar to Dynamic Multicast Optimization (DMO) where the multicast streams are converted into unicast streams on the AP instead of the controller, to enhance the quality and reliability of streaming videos, while preserving the bandwidth available to non-video clients.
DES	Data Encryption Standard. DES is a common standard for data encryption and a form of secret key cryptography, which uses only one key for encryption and decryption.
designated router	Designated router refers to a router interface that is elected to originate network link advertisements for networks using the OSPF protocol.
destination NAT	Destination Network Address Translation. Destination NAT is a process of translating the destination IP address of an end route packet in a network. Destination NAT is used for redirecting the traffic destined to a virtual host to the real host, where the virtual host is identified by the destination IP address and the real host is identified by the translated IP address.
DFS	Dynamic Frequency Selection. DFS is a mandate for radio systems operating in the 5 GHz band to be equipped with means to identify and avoid interference with Radar systems.
DFT	Discrete Fourier Transform. DFT converts discrete-time data sets into a discrete-frequency representation. See FFT.
DHCP	Dynamic Host Configuration Protocol. A network protocol that enables a server to automatically assign an IP address to an IP-enabled device from a defined range of numbers configured for a given network.
DHCP snooping	DHCP snooping enables the switch to monitor and control DHCP messages received from untrusted devices that are connected to the switch.
digital certificate	A digital certificate is an electronic document that uses a digital signature to bind a public key with an identityâ€”information such as the name of a person or an organization, address, and so forth.
Digital wireless pulse	A wireless technology for transmitting large amounts of digital data over a wide spectrum of frequency bands with very low power for a short distance. Ultra Wideband radio can carry a huge amount of data over a distance up to 230 ft at very low power (less than 0.5 mW), and has the ability to carry signals through doors and other obstacles that tend to reflect signals at more limited bandwidths and a higher power.
Disconnect-Ack	Disconnect-Ack is a NAS response packet to a Disconnect-Request, which indicates that the session was disconnected.
Disconnect-Nak	Disconnect-Nak is NAS response packet to a Disconnect-Request, which indicates that the session was not disconnected.
Disconnect-Request	Disconnect-Request is a RADIUS packet type sent to a NAS requesting that a user or session be disconnected.

distribution certificate
Distribution certificate is used for digitally signing iOS mobile apps to enable enterprise app distribution. It verifies the identity of the app publisher.

DLNA
Digital Living Network Alliance. DLNA is a set of interoperability guidelines for sharing digital media among multimedia devices.

DMO
Dynamic Multicast Optimization. DMO is a process of converting multicast streams into unicast streams over a wireless link to enhance the quality and reliability of streaming videos, while preserving the bandwidth available to non-video clients.

DN
Distinguished Name. A series of fields in a digital certificate that, taken together, constitute the unique identity of the person or device that owns the digital certificate. Common fields in a DN include country, state, locality, organization, organizational unit, and the â€œcommon nameâ€□, which is the primary name used to identify the certificate.

DNS
Domain Name System. A DNS server functions as a phone book for the intranet and Internet users. It converts human-readable computer host names into IP addresses and IP addresses into host names. It stores several records for a domain name such as an address 'A' record, name server (NS), and mail exchanger (MX) records. The Address 'A' record is the most important record that is stored in a DNS server, because it provides the required IP address for a network peripheral or element.

DOCSIS
Data over Cable Service Interface Specification. A telecommunication standard for Internet access through cable modem.

DoS
Denial of Service. DoS is any type of attack where the attackers send excessive messages to flood traffic and thereby preventing the legitimate users from accessing the service.

DPD
Dead Peer Detection. A method used by the network devices to detect the availability of the peer devices.

DPI
Deep Packet Inspection. DPI is an advanced method of network packet filtering that is used for inspecting data packets exchanged between the devices and systems over a network. DPI functions at the Application layer of the Open Systems Interconnection (OSI) reference model and enables users to identify, categorize, track, reroute, or stop packets passing through a network.

DRT
Downloadable Regulatory Table. The DRT feature allows new regulatory approvals to be distributed for APs without a software upgrade or patch.

DS
Differentiated Services. The DS specification aims to provide uninterrupted quality of service by managing and controlling the network traffic, so that certain types of traffic get precedence.

DSCP
Differentiated Services Code Point. DSCP is a 6-bit packet header value used for traffic classification and priority assignment.

DSL
Digital Subscriber Line. The DSL technology allows the transmission of digital data over telephone lines. A DSL modem is a device used for connecting a computer or router to a telephone line that offers connectivity to the Internet.

DSSS	Direct-Sequence Spread Spectrum. DSSS is a modulation technique used for reducing overall signal interference. This technique multiplies the original data signal with a pseudo random noise spreading code. Spreading of this signal makes the resulting wideband channel more noisy, thereby increasing the resistance to interference. See FHSS.
DST	Daylight Saving Time. DST is also known as summer time that refers to the practice of advancing clocks, so that evenings have more daylight and mornings have less. Typically clocks are adjusted forward one hour near the start of spring and are adjusted backward in autumn.
DTE	Data Terminal Equipment. DTE refers to a device that converts user information into signals or re-converts the received signals.
DTIM	Delivery Traffic Indication Message. DTIM is a kind of traffic indication map. A DTIM interval determines when the APs must deliver broadcast and multicast frames to their associated clients in power save mode.
DTLS	Datagram Transport Layer Security. DTLS communications protocol provides communications security for datagram protocols.
dynamic authorization	Dynamic authorization refers to the ability to make changes to a visitor accountâ€™s session while it is in progress. This might include disconnecting a session or updating some aspect of the authorization for the session.
dynamic NAT	Dynamic Network Address Translation. Dynamic NAT maps multiple public IP addresses and uses these addresses with an internal or private IP address. Dynamic NAT helps to secure a network by masking the internal configuration of a private network.
EAP	Extensible Authentication Protocol. An authentication protocol for wireless networks that extends the methods used by the PPP, a protocol often used when connecting a computer to the Internet. EAP can support multiple authentication mechanisms, such as token cards, smart cards, certificates, one-time passwords, and public key encryption authentication.
EAP-FAST	EAP â€“ Flexible Authentication Secure Tunnel (tunneled).
EAP-GTC	EAP â€“ Generic Token Card. (non-tunneled).
EAP-MD5	EAP â€“ Method Digest 5. (non-tunneled).
EAP-MSCHAP	EAP Microsoft Challenge Handshake Authentication Protocol.
EAP-MSCHAPv2	EAP Microsoft Challenge Handshake Authentication Protocol Version 2.
EAPoL	Extensible Authentication Protocol over LAN. A network port authentication protocol used in IEEE 802.1X standards to provide a generic network sign-on to access network resources.
EAP-PEAP	EAPâ€“Protected EAP. A widely used protocol for securely transporting authentication data across a network (tunneled).
EAP-PWD	EAP-Password. EAP-PWD is an EAP method that uses a shared password for authentication.
EAP-TLS	EAPâ€“Transport Layer Security. EAP-TLS is a certificate-based authentication method supporting mutual authentication, integrity-protected ciphersuite negotiation and key exchange between two endpoints. See RFC 5216.
EAP-TTLS	EAPâ€“Tunneled Transport Layer Security. EAP-TTLS is an EAP method that encapsulates a TLS session, consisting of a handshake phase and a data phase. See RFC 5281.

ECC Elliptical Curve Cryptography or Error correcting Code memory. Elliptical Curve Cryptography is a public-key encryption technique that is based on elliptic curve theory used for creating faster, smaller, and more efficient cryptographic keys. Error Correcting Code memory is a type of computer data storage that can detect and correct the most common kinds of internal data corruption. ECC memory is used in most computers where data corruption cannot be tolerated under any circumstances, such as for scientific or financial computing.

ECDSA Elliptic Curve Digital Signature Algorithm. ECDSA is a cryptographic algorithm that supports the use of public or private key pairs for encrypting and decrypting information.

EDCA Enhanced Distributed Channel Access. The EDCA function in the IEEE 802.11e Quality of Service standard supports differentiated and distributed access to wireless medium based on traffic priority and Access Category types. See WMM and WME.

EIGRP Enhanced Interior Gateway Routing Protocol. EIGRP is a routing protocol used for automating routing decisions and configuration in a network.

EIRP Effective Isotropic Radiated Power or Equivalent Isotropic Radiated Power. EIRP refers to the output power generated when a signal is concentrated into a smaller area by the Antenna.

ESI External Services Interface. ESI provides an open interface for integrating security solutions that solve interior network problems such as viruses, worms, spyware, and corporate compliance.

ESS Extended Service Set. An ESS is a set of one or more interconnected BSSs that form a single sub network.

ESSID Extended Service Set Identifier. ESSID refers to the ID used for identifying an extended service set.

Ethernet Ethernet is a network protocol for data transmission over LAN.

EULA End User License Agreement. EULA is a legal contract between a software application publisher or author and the users of the application.

FCC Federal Communications Commission. FCC is a regulatory body that defines standards for the interstate and international communications by radio, television, wire, satellite, and cable.

FFT Fast Fourier Transform. FFT is a frequency analysis mechanism that aims at faster conversion of a discrete signal in time domain into a discrete frequency domain representation. See also DFT.

FHSS Frequency Hopping Spread Spectrum. FHSS is transmission technique that allows modulation and transmission of a data signal by rapidly switching a carrier among many frequency channels in a random but predictable sequence. See also DSSS.

FIB Forwarding Information Base. FIB is a forwarding table that maps MAC addresses to ports. FIB is used in network bridging, routing, and similar functions to identify the appropriate interface for forwarding packets.

FIPS Federal Information Processing Standards. FIPS refers to a set of standards that describe document processing, encryption algorithms, and other information technology standards for use within non-military government agencies, and by government contractors and vendors who work with these agencies.

firewall	Firewall is a network security system used for preventing unauthorized access to or from a private network.
FQDN	Fully Qualified Domain Name. FQDN is a complete domain name that identifies a computer or host on the Internet.
FQLN	Fully Qualified Location Name. FQLN is a device location identifier in the format: APname.Floor.Building.Campus.
frequency allocation	Use of radio frequency spectrum as regulated by governments.
FSPL	Free Space Path Loss. FSPL refers to the loss in signal strength of an electromagnetic wave that would result from a line-of-sight path through free space (usually air), with no obstacles nearby to cause reflection or diffraction.
FTP	File Transfer Protocol. A standard network protocol used for transferring files between a client and server on a computer network.
GARP	Generic Attribute Registration Protocol. GVRP is a LAN protocol that allows the network nodes to register and de-register attributes, such as network addresses, with each other.
GAS	Generic Advertisement Service. GAS is a request-response protocol, which provides Layer 2 transport mechanism between a wireless client and a server in the network prior to authentication. It helps in determining a wireless network infrastructure before associating clients, and allows clients to send queries to multiple 802.11 networks in parallel.
gateway	Gateway is a network node that allows traffic to flow in and out of the network.
Gbps	Gigabits per second.
GBps	Gigabytes per second.
GET	GET refers HTTP request method or an SNMP operation method. The GET HTTP request method submits data to be processed to a specified resource. The GET SNMP operation method obtains information from the Management Information Base (MIB).
GHz	Gigahertz.
GMT	Greenwich Mean Time. GMT refers to the mean solar time at the Royal Observatory in Greenwich, London. GMT is the same as Coordinated Universal Time (UTC) standard, written as an offset of UTC +/- 00:00.
goodput	Goodput is the application level throughput that refers to the ratio of the total bytes transmitted or received in the network to the total air time required for transmitting or receiving the bytes.
GPS	Global Positioning System. A satellite-based global navigation system.
GRE	Generic Routing Encapsulation. GRE is an IP encapsulation protocol that is used to transport packets over a network.
GTC	Generic Token Card. GTC is a protocol that can be used as an alternative to MSCHAPv2 protocol. GTC allows authentication to various authentication databases even in cases where MSCHAPv2 is not supported by the database.
GVRP	GARP VLAN Registration Protocol or Generic VLAN Registration Protocol. GARP is an IEEE 802.1Q-compliant protocol that facilitates VLAN registration and controls VLANs within a larger network.

H2QP Hotspot 2.0 Query Protocol.

hot zone Wireless access area created by multiple hotspots that are located in close proximity to one another. Hot zones usually combine public safety APs with public hotspots.

hotspot Hotspot refers to a WLAN node that provides Internet connection and virtual private network (VPN) access from a given location. A business traveler, for example, with a laptop equipped for Wi-Fi can look up a local hotspot, contact it, and get connected through its network to reach the Internet.

HSPA High-Speed Packet Access.

HT High Throughput. IEEE 802.11n is an HT WLAN standard that aims to achieve physical data rates of close to 600 Mbps on the 2.4 GHz and 5 GHz bands.

HTTP Hypertext Transfer Protocol. The HTTP is an application protocol to transfer data over the web. The HTTP protocol defines how messages are formatted and transmitted, and the actions that the w servers and browsers should take in response to various commands.

HTTPS Hypertext Transfer Protocol Secure. HTTPS is a variant of the HTTP that adds a layer of security on the data in transit through a secure socket layer or transport layer security protocol connection.

IAS Internet Authentication Service. IAS is a component of Windows Server operating systems that provides centralized user authentication, authorization, and accounting.

ICMP Internet Control Message Protocol. ICMP is an error reporting protocol. It is used by network devices such as routers, to send error messages and operational information to the source IP address when network problems prevent delivery of IP packets.

IDS Intrusion Detection System. IDS monitors a network or systems for malicious activity or policy violations and reports its findings to the management system deployed in the network.

IEEE Institute of Electrical and Electronics Engineers.

IGMP Internet Group Management Protocol. Communications protocol used by hosts and adjacent routers on IP networks to establish multicast group memberships.

IGMP snooping IGMP snooping prevents multicast flooding on Layer 2 network by treating multicast traffic as broadcast traffic. Without IGMP snooping, all streams could be flooded to all ports on that VLAN. When multicast flooding occurs, end-hosts that happen to be in the same VLAN would receive all the streams only to be discarded without snooping.

IGP Interior Gateway Protocol. IGP is used for exchanging routing information between gateways within an autonomous system (for example, a system of corporate local area networks).

IGRP Interior Gateway Routing Protocol. IGRP is a distance vector interior routing protocol used by routers to exchange routing data within an autonomous system.

IKE Internet Key Exchange. IKE is a key management protocol used with IPsec protocol to establish a secure communication channel. IKE provides additional feature, flexibility, and ease of configuration for IPsec standard.

IKEv1	Internet Key Exchange version 1. IKEv1 establishes a secure authenticated communication channel by using either the pre-shared key (shared secret), digital signatures, or public key encryption. IKEv1 operates in Main and Aggressive modes. See RFC 2409.
IKEv2	Internet Key Exchange version 2. IKEv2 uses the secure channel established in Phase 1 to negotiate Security Associations on behalf of services such as IPsec. IKEv2 uses pre-shared key and Digital Signature for authentication. See RFC 4306.
IoT	Internet of Things. IoT refers to the internetworking of devices that are embedded with electronics, software, sensors, and network connectivity features allowing data exchange over the Internet.
IPM	Intelligent Power Monitoring. IPM is a feature supported on certain APs that actively measures the power utilization of an AP and dynamically adapts to the power resources.
IPS	Intrusion Prevention System. The IPS monitors a network for malicious activities such as security threats or policy violations. The main function of an IPS is to identify suspicious activity, log the information, attempt to block the activity, and report it.
IPsec	Internet Protocol security. IPsec is a protocol suite for secure IP communications that authenticates and encrypts each IP packet in a communication session.
IPSG	Internet Protocol Source Guard. IPSG restricts IP address from untrusted interface by filtering traffic based on list of addresses in the DHCP binding database or manually configured IP source bindings. It prevents IP spoofing attacks.
IrDA	An industry-sponsored organization set up in 1993 to create international standards for the hardware and software used in infrared communication links. In this special form of radio transmission, a focused ray of light in the infrared frequency spectrum, measured in terahertz (THz), or trillions of hertz (cycles per second), is modulated with information and sent from a transmitter to a receiver over a relatively short distance.
ISAKMP	Internet Security Association and Key Management Protocol. ISAKMP is used for establishing Security Associations and cryptographic keys in an Internet environment.
ISP	Internet Service Provider. An ISP is an organization that provides services for accessing and using the Internet.
JSON	JavaScript Object Notation. JSON is an open-standard, language-independent, lightweight data-interchange format used to transmit data objects consisting of attributeâ€“value pairs. JSON uses a "self-describing" text format that is easy for humans to read and write, and that can be used as a data format by any programming language.
Kbps	Kilobits per second.
KBps	Kilobytes per second.
keepalive	Signal sent at periodic intervals from one device to another to verify that the link between the two devices is working. If no reply is received, data will be sent by a different path until the link is restored. A keepalive can also be used to indicate that the connection should be preserved so that the receiving device does not consider it timed out and drop it.

L2TP — Layer-2 Tunneling Protocol. L2TP is a networking protocol used by the ISPs to enable VPN operations.

LACP — Link Aggregation Control Protocol. LACP is used for the collective handling of multiple physical ports that can be seen as a single channel for network traffic purposes.

LAG — Link Aggregation Group . A LAG combines a number of physical ports together to make a single high- bandwidth data path. LAGs can connect two switches to provide a higher-bandwidth connection to a public network.

LAN — Local Area Network. A LAN is a network of connected devices within a distinct geographic area such as an office or a commercial establishment and share a common communications line or wireless link to a server.

LCD — Liquid Crystal Display. LCD is the technology used for displays in notebook and other smaller computers. Like LED and gas-plasma technologies, LCDs allow displays to be much thinner than the cathode ray tube technology.

LDAP — Lightweight Directory Access Protocol. LDAP is a communication protocol that provides the ability to access and maintain distributed directory information services over a network.

LDPC — Low-Density Parity-Check. LDPC is a method of transmitting a message over a noisy transmission channel using a linear error correcting code. An LDPC is constructed using a sparse bipartite graph.

LEAP — Lightweight Extensible Authentication Protocol. LEAP is a Cisco proprietary version of EAP used in wireless networks and Point-to-Point connections.

LED — Light Emitting Diode. LED is a semiconductor light source that emits light when an electric current passes through it.

LEEF — Log Event Extended Format. LEEF is a type of customizable syslog event format. An extended log file contains a sequence of lines containing ASCII characters terminated by either the sequence LF or CRLF.

LI — Lawful Interception. LI refers to the procedure of obtaining communications network data by the Law Enforcement Agencies for the purpose of analysis or evidence.

LLDP — Link Layer Discovery Protocol. LLDP is a vendor-neutral link layer protocol in the Internet Protocol suite used by network devices for advertising their identity, capabilities, and neighbors on an IEEE 802 local area network, which is principally a wired Ethernet.

LLDP-MED — LLDPâ€“Media Endpoint Discovery. LLDP-MED facilitates information sharing between endpoints and network infrastructure devices.

LMS — Local Management Switch. In multi-controller networks, each controller acts as an LMS and terminates user traffic from the APs, processes, and forwards the traffic to the wired network.

LNS — L2TP Network Server. LNS is an equipment that connects to a carrier and handles the sessions from broadband lines. It is also used for dial-up and mobile links. LNS handles authentication and routing of the IP addresses. It also handles the negotiation of the link with the equipment and establishes a session.

LTE — Long Term Evolution. LTE is a 4G wireless communication standard that provides high-speed wireless communication for mobile phones and data terminals. See 4G.

MAB MAC Authentication Bypass. Endpoints such as network printers, Ethernet-based sensors, cameras, and wireless phones do not support 802.1X authentication. For such endpoints, MAC Authentication Bypass mechanism is used. In this method, the MAC address of the endpoint is used to authenticate the endpoint.

MAC Media Access Control. A MAC address is a unique identifier assigned to network interfaces for communications on a network.

MAM Mobile Application Management. MAM refers to software and services used to secure, manage, and distribute mobile applications used in enterprise settings on mobile devices like smartphones and tablet computers. Mobile Application Management can apply to company-owned mobile devices as well as BYOD.

Mbps Megabits per second

MBps Megabytes per second

MCS Modulation and Coding Scheme. MCS is used as a parameter to determine the data rate of a wireless connection for high throughput.

MD4 Message Digest 4. MD4 is an earlier version of MD5 and is an algorithm used to verify data integrity through the creation of a 128-bit message digest from data input.

MD5 Message Digest 5. The MD5 algorithm is a widely used hash function producing a 128-bit hash value from the data input.

MDAC Microsoft Data Access Components. MDAC is a framework of interrelated Microsoft technologies that provides a standard database for Windows OS.

MDM Mobile Device Management. MDM is an administrative software to manage, monitor, and secure mobile devices of the employees in a network.

mDNS Multicast Domain Name System. mDNS provides the ability to perform DNS-like operations on the local link in the absence of any conventional unicast DNS server. The mDNS protocol uses IP multicast User Datagram Protocol (UDP) packets, and is implemented by the Apple Bonjour and Linux NSS-mDNS services. mDNS works in conjunction with DNS Service Discovery (DNS-SD), a companion zero-configuration technique specified. See RFC 6763.

MFA Multi-factor Authentication. MFA lets you require multiple factors, or proofs of identity, when authenticating a user. Policy configurations define how often multi-factor authentication will be required, or conditions that will trigger it.

MHz Megahertz

MIB Management Information Base. A hierarchical database used by SNMP to manage the devices being monitored.

microwave Electromagnetic energy with a frequency higher than 1 GHz, corresponding to wavelength shorter than 30 centimeters.

MIMO Multiple Input Multiple Output. An antenna technology for wireless communications in which multiple antennas are used at both source (transmitter) and destination (receiver). The antennas at each end of the communications circuit are combined to minimize errors and optimize data speed.

MISO Multiple Input Single Output. An antenna technology for wireless communications in which multiple antennas are used at the source (transmitter). The antennas are combined to minimize errors and optimize data speed. The destination (receiver) has only one antenna.

MLD Multicast Listener Discovery. A component of the IPv6 suite. It is used by IPv6 routers for discovering multicast listeners on a directly attached link.

MPDU MAC Protocol Data Unit. MPDU is a message exchanged between MAC entities in a communication system based on the layered OSI model.

MPLS Multiprotocol Label Switching. The MPLS protocol speeds up and shapes network traffic flows.

MPPE Microsoft Point-to-Point Encryption. A method of encrypting data transferred across PPP-based dial-up connections or PPTP-based VPN connections.

MS-CHAP Microsoft Challenge Handshake Authentication Protocol. MS-CHAP is Password-based, challenge-response, mutual authentication protocol that uses MD4 and DES encryption.

MS-CHAPv1 Microsoft Challenge Handshake Authentication Protocol version 1. MS-CHAPv1 extends the user authentication functionality provided on Windows networks to remote workstations. MS-CHAPv1 supports only one-way authentication.

MS-CHAPv2 Microsoft Challenge Handshake Authentication Protocol version 2. MS-CHAPv2 is an enhanced version of the MS-CHAP protocol that supports mutual authentication.

MSS Maximum Segment Size. MSS is a parameter of the options field in the TCP header that specifies the largest amount of data, specified in bytes, that a computer or communications device can receive in a single TCP segment.

MSSID Mesh Service Set Identifier. MSSID is the SSID used by the client to access a wireless mesh network.

MSTP Multiple Spanning Tree Protocol. MSTP configures a separate Spanning Tree for each VLAN group and blocks all but one of the possible alternate paths within each spanning tree.

MTU Maximum Transmission Unit. MTU is the largest size packet or frame specified in octets (eight-bit bytes) that can be sent in networks such as the Internet.

MU-MIMO Multi-User Multiple-Input Multiple-Output. MU-MIMO is a set of multiple-input and multiple-output technologies for wireless communication, in which users or wireless terminals with one or more antennas communicate with each other.

MVRP Multiple VLAN Registration Protocol. MVRP is a Layer 2 network protocol used for automatic configuration of VLAN information on switches.

mW milliWatts. mW is 1/1000 of a Watt. It is a linear measurement (always positive) that is generally used to represent transmission.

NAC Network Access Control. NAC is a computer networking solution that uses a set of protocols to define and implement a policy that describes how devices can secure access to network nodes when they initially attempt to connect to a network.

NAD Network Access Device. NAD is a device that automatically connects the user to the preferred network, for example, an AP or an Ethernet switch.

NAK	Negative Acknowledgement. NAK is a response indicating that a transmitted message was received with errors or it was corrupted, or that the receiving end is not ready to accept transmissions.
NAP	Network Access Protection. The NAP feature in the Windows Server allows network administrators to define specific levels of network access based on identity, groups, and policy compliance. The NAP Agent is a service that collects and manages health information for NAP client computers. If a client is not compliant, NAP provides a mechanism to automatically bring the client back into compliance and then dynamically increase its level of network access.
NAS	Network Access Server. NAS provides network access to users, such as a wireless AP, network switch, or dial- in terminal server.
NAT	Network Address Translation. NAT is a method of remapping one IP address space into another by modifying network address information in Internet Protocol (IP) datagram packet headers while they are in transit across a traffic routing device.
NetBIOS	Network Basic Input/Output System. A program that lets applications on different computers communicate within a LAN.
netmask	Netmask is a 32-bit mask used for segregating IP address into subnets. Netmask defines the class and range of IP addresses.
NFC	Near-Field Communication. NFC is a short-range wireless connectivity standard (ECMA-340, ISO/IEC 18092) that uses magnetic field induction to enable communication between devices when they touch or are brought closer (within a few centimeters of distance). The standard specifies a way for the devices to establish a peer- to-peer (P2P) network to exchange data.
NIC	Network Interface Card. NIC is a hardware component that allows a device to connect to the network.
Nmap	Network Mapper. Nmap is an open-source utility for network discovery and security auditing. Nmap uses IP packets to determine such things as the hosts available on a network and their services, operating systems and versions, types of packet filters/firewalls, and so on.
NMI	Non-Maskable Interrupt. NMI is a hardware interrupt that standard interrupt-masking techniques in the system cannot ignore. It typically occurs to signal attention for non-recoverable hardware errors.
NMS	Network Management System. NMS is a set of hardware and/or software tools that allow an IT professional to supervise the individual components of a network within a larger network management framework.
NOE	New Office Environment. NOE is a proprietary VoIP protocol designed by Alcatel-Lucent Enterprise.
NTP	Network Time Protocol. NTP is a protocol for synchronizing the clocks of computers over a network.
OAuth	Open Standard for Authorization. OAuth is a token-based authorization standard that allows websites or third- party applications to access user information, without exposing the user credentials.
OCSP	Online Certificate Status Protocol. OCSP is used for determining the current status of a digital certificate without requiring a CRL.

OFDM	Orthogonal Frequency Division Multiplexing. OFDM is a scheme for encoding digital data on multiple carrier frequencies.
OID	Object Identifier. An OID is an identifier used to name an object. The OIDs represent nodes or managed objects in a MIB hierarchy. The OIDs are designated by text strings and integer sequences and are formally defined as per the ASN.1 standard.
OKC	Opportunistic Key Caching. OKC is a technique available for authentication between multiple APs in a network where those APs are under common administrative control. Using OKC, a station roaming to any AP in the network will not have to complete a full authentication exchange, but will instead just perform the 4-way handshake to establish transient encryption keys.
onboarding	The process of preparing a device for use on an enterprise network, by creating the appropriate access credentials and setting up the network connection parameters.
OpenFlow	OpenFlow is an open communications interface between control plane and the forwarding layers of a network.
OpenFlow agent	OpenFlow agent. OpenFlow is a software module in Software-Defined Networking (SDN) that allows the abstraction of any legacy network element, so that it can be integrated and managed by the SDN controller. OpenFlow runs on network devices such as switches, routers, wireless controllers, and APs.
Optical wireless	Optical wireless is combined use of conventional radio frequency wireless and optical fiber for telecommunication. Long-range links are provided by using optical fibers; the links from the long-range endpoints to end users are accomplished by RF wireless or laser systems. RF wireless at Ultra High Frequencies and microwave frequencies can carry broadband signals to individual computers at substantial data speeds.
OSI	Open Systems Interconnection. OSI is a reference model that defines a framework for communication between the applications in a network.
OSPF	Open Shortest Path First. OSPF is a link-state routing protocol for IP networks. It uses a link-state routing algorithm and falls into the group of interior routing protocols that operates within a single Autonomous System (AS).
OSPFv2	Open Shortest Path First version 2. OSPFv2 is the version 2 of the link-state routing protocol, OSPF. See RFC 2328.
OUI	Organizationally Unique Identifier. Synonymous with company ID or vendor ID, an OUI is a 24-bit, globally unique assigned number, referenced by various standards. The first half of a MAC address is OUI.
OVA	Open Virtualization Archive. OVA contains a compressed installable version of a virtual machine.
OVF	Open Virtualization Format. OVF is a specification that describes an open-standard, secure, efficient, portable and extensible format for packaging and distributing software for virtual machines.
PAC	Protected Access Credential. PAC is distributed to clients for optimized network authentication. These credentials are used for establishing an authentication tunnel between the client and the authentication server.
PAP	Password Authentication Protocol. PAP validates users by password. PAP does not encrypt passwords for transmission and is thus considered insecure.

PAPI Process Application Programming Interface. PAPI controls channels for ARM and Wireless Intrusion Detection System (WIDS) communication to the master controller. A separate PAPI control channel connects to the local controller where the SSID tunnels terminate.

PBR Policy-based Routing. PBR provides a flexible mechanism for forwarding data packets based on polices configured by a network administrator.

PDU Power Distribution Unit or Protocol Data Unit. Power Distribution Unit is a device that distributes electric power to the networking equipment located within a data center. Protocol Data Unit contains protocol control Information that is delivered as a unit among peer entities of a network.

PEAP Protected Extensible Authentication Protocol. PEAP is a type of EAP communication that addresses security issues associated with clear text EAP transmissions by creating a secure channel encrypted and protected by TLS.

PEF Policy Enforcement Firewall. PEF also known as PEFNG provides context-based controls to enforce application- layer security and prioritization. The customers using Aruba mobility controllers can avail PEF features and services by obtaining a PEF license. PEF for VPN usersâ€”Customers with PEF for VPN license can apply firewall policies to the user traffic routed to a controller through a VPN tunnel.

PEFNG Policy Enforcement Firewall. PEF also known as PEFNG provides context-based controls to enforce application- layer security and prioritization. The customers using Aruba mobility controllers can avail PEF features and services by obtaining a PEF license. PEF for VPN usersâ€”Customers with PEF for VPN license can apply firewall policies to the user traffic routed to a controller through a VPN tunnel.

PEFV Policy Enforcement Firewall. PEF also known as PEFNG provides context-based controls to enforce application- layer security and prioritization. The customers using Aruba mobility controllers can avail PEF features and services by obtaining a PEF license. PEF for VPN usersâ€”Customers with PEF for VPN license can apply firewall policies to the user traffic routed to a controller through a VPN tunnel.

PFS Perfect Forward Secrecy. PFS refers to the condition in which a current session key or long-term private key does not compromise the past or subsequent keys.

PHB Per-hop behavior. PHB is a term used in DS or MPLS. It defines the policy and priority applied to a packet when traversing a hop (such as a router) in a DiffServ network.

PIM Protocol-Independent Multicast. PIM refers to a family of multicast routing protocols for IP networks that provide one-to-many and many-to-many distribution of data over a LAN, WAN, or the Internet.

PIN Personal Identification Number. PIN is a numeric password used to authenticate a user to a system.

PKCS#n Public-key cryptography standard n. PKCS#n refers to a numbered standard related to topics in cryptography, including private keys (PKCS#1), digital certificates (PKCS#7), certificate signing requests (PKCS#10), and secure storage of keys and certificates (PKCS#12).

PKI
Public Key Infrastructure. PKI is a security technology based on digital certificates and the assurances provided by strong cryptography. See also certificate authority, digital certificate, public key, private key.

PLMN
Public Land Mobile Network. PLMS is a network established and operated by an administration or by a Recognized Operating Agency for the specific purpose of providing land mobile telecommunications services to the public.

PMK
Pairwise Master Key. PMK is a shared secret key that is generated after PSK or 802.1X authentication.

PoE
Power over Ethernet. PoE is a technology for wired Ethernet LANs to carry electric power required for the device in the data cables. The IEEE 802.3af PoE standard provides up to 15.4 W of power on each port.

PoE+
Power over Ethernet+. PoE+ is an IEEE 802.3at standard that provides 25.5W power on each port.

POST
Power On Self Test. An HTTP request method that requests data from a specified resource.

PPP
Point-to-Point Protocol. PPP is a data link (layer 2) protocol used to establish a direct connection between two nodes. It can provide connection authentication, transmission encryption, and compression.

PPPoE
Point-to-Point Protocol over Ethernet. PPPoE is a method of connecting to the Internet, typically used with DSL services, where the client connects to the DSL modem.

PPTP
Point-to-Point Tunneling Protocol. PPTP is a method for implementing virtual private networks. It uses a control channel over TCP and a GRE tunnel operating to encapsulate PPP packets.

private key
The part of a public-private key pair that is always kept private. The private key encrypts the signature of a message to authenticate the sender. The private key also decrypts a message that was encrypted with the public key of the sender.

PRNG
Pseudo-Random Number Generator. PRNG is an algorithm for generating a sequence of numbers whose properties approximate the properties of sequences of random numbers.

PSK
Pre-shared key. A unique shared secret that was previously shared between two parties by using a secure channel. This is used with WPA security, which requires the owner of a network to provide a passphrase to users for network access.

PSU
Power Supply Unit. PSU is a unit that supplies power to an equipment by converting mains AC to low-voltage regulated DC power.

public key
The part of a public-private key pair that is made public. The public key encrypts a message and the message is decrypted with the private key of the recipient.

PVST
Per-VLAN Spanning Tree. PVST provides load balancing of VLANs across multiple ports resulting in optimal usage of network resources.

PVST+
Per-VLAN Spanning Tree+. PVST+ is an extension of the PVST standard that uses the 802.1Q trunking technology.

QoS
Quality of Service. It refers to the capability of a network to provide better service and performance to a specific network traffic over various technologies.

RA	Router Advertisement. The RA messages are sent by the routers in the network when the hosts send multicast router solicitation to the multicast address of all routers.
Radar	Radio Detection and Ranging. Radar is an object-detection system that uses radio waves to determine the range, angle, or velocity of objects.
RADIUS	Remote Authentication Dial-In User Service. An Industry-standard network access protocol for remote authentication. It allows authentication, authorization, and accounting of remote users who want to access network resources.
RAM	Random Access Memory.
RAPIDS	Rogue Access Point identification and Detection System. An AMP module that is designed to identify and locate wireless threats by making use of all of the information available from your existing infrastructure.
RARP	Reverse Address Resolution Protocol. RARP is a protocol used by a physical machine in a local area network for determining the IP address from the ARP table or cache of the gateway server.
Regex	Regular Expression. Regex refers to a sequence of symbols and characters defining a search pattern.
Registration Authority	Type of Certificate Authority that processes certificate requests. The Registration Authority verifies that requests are valid and comply with certificate policy, and authenticates the user's identity. The Registration Authority then forwards the request to the Certificate Authority to sign and issue the certificate.
Remote AP	Remote APs extend corporate network to the users working from home or at temporary work sites. Remote APs are deplyed at branch office sites and are connected to the central network on a WAN link.
REST	Representational State Transfer. REST is a simple and stateless architecture that the web services use for providing interoperability between computer systems on the Internet. In a RESTful web service, requests made to the URI of a resource will elicit a response that may be in XML, HTML, JSON or some other defined format.
RF	Radio Frequency. RF refers to the electromagnetic wave frequencies within a range of 3 kHz to 300 GHz, including the frequencies used for communications or Radar signals.
RFC	Request For Comments. RFC is a commonly used format for the Internet standards documentss.
RFID	Radio Frequency Identification. RFID uses radio waves to automatically identify and track the information stored on a tag attached to an object.
RIP	Routing Information Protocol. RIP prevents the routing loops by limiting the number of hops allowed in a path from source to destination.
RJ45	Registered Jack 45. RJ45 is a physical connector for network cables.
RMA	Return Merchandise Authorization. RMA is a part of the product returning process that authorizes users to return a product to the manufacturer or distributor for a refund, replacement, or repair. The customers who want to return a product within its Warranty period contact the manufacturer to initiate the product returning process. The manufacturer or the seller generates an authorization number for the RMA, which is used by the customers, when returning a product to the warehouse.

RMON	Remote Monitoring. RMON provides standard information that a network administrator can use to monitor, analyze, and troubleshoot a group of distributed LANs.
RoW	Rest of World. RoW or RW is an operating country code of a device.
RSA	Rivest, Shamir, Adleman. RSA is a cryptosystem for public-key encryption, and is widely used for securing sensitive data, particularly when being sent over an insecure network such as the Internet.
RSSI	Received Signal Strength Indicator. RSSI is a mechanism by which RF energy is measured by the circuitry on a wireless NIC (0-255). The RSSI is not standard across vendors. Each vendor determines its own RSSI scale/values.
RSTP	Rapid Spanning Tree Protocol. RSTP provides significantly faster spanning tree convergence after a topology change, introducing new convergence behaviors and bridge port roles to do this.
RTCP	RTP Control Protocol. RTCP provides out-of-band statistics and control information for an Real-Time Transport Protocol session.
RTLS	Real-Time Location Systems. RTLS automatically identifies and tracks the location of objects or people in real time, usually within a building or other contained area.
RTP	Real-Time Transport Protocol. RTP is a network protocol used for delivering audio and video over IP networks.
RTS	Request to Send. RTS refers to the data transmission and protection mechanism used by the 802.11 wireless networking protocol to prevent frame collision occurrences. See CTS.
RTSP	Real Time Streaming Protocol. RTSP is a network control protocol designed for use in entertainment and communications systems to control streaming media servers.
RVI	Routed VLAN Interface. RVI is a switch interface that forwards packets between VLANs.
RW	Rest of World. RoW or RW is an operating country code of a device.
SA	Security Association. SA is the establishment of shared security attributes between two network entities to support secure communication.
SAML	Security Assertion Markup Language. SAML is an XML-based framework for communicating user authentication, entitlement, and attribute information. SAML enables single sign-on by allowing users to authenticate at an identity provider and then access service providers without additional authentication.
SCEP	Simple Certificate Enrollment Protocol. SCEP is a protocol for requesting and managing digital certificates.
SCP	Secure Copy Protocol. SCP is a network protocol that supports file transfers between hosts on a network.
SCSI	Small Computer System Interface. SCSI refers to a set of interface standards for physical connection and data transfer between a computer and the peripheral devices such as printers, disk drives, CD-ROM, and so on.
SDN	Software-Defined Networking. SDN is an umbrella term encompassing several kinds of network technology aimed at making the network as agile and flexible as the virtualized server and storage infrastructure of the modern data center.

SDR Server Derivation Rule. An SDR refers to a role assignment model used by the controllers running ArubaOS to assign roles and VLANs to the WLAN users based on the rules defined under a server group. The SDRs override the default authentication roles and VLANs defined in the AAA and Virtual AP profiles.

SDU Service Data Unit. SDU is a unit of data that has been passed down from an OSI layer to a lower layer and that has not yet been encapsulated into a PDU by the lower layer.

SD-WAN Software-Defined Wide Area Network. SD-WAN is an application for applying SDN technology to WAN connections that connect enterprise networks across disparate geographical locations.

SFP The Small Form-factor Pluggable. SFP is a compact, hot-pluggable transceiver that is used for both telecommunication and data communications applications.

SFP+ Small Form-factor Pluggable+. SFP+ supports up to data rates up to 16 Gbps.

SFTP Secure File Transfer Protocol. SFTP is a network protocol that allows file access, file transfer, and file management functions over a secure connection.

SHA Secure Hash Algorithm. SHA is a family of cryptographic hash functions. The SHA algorithm includes the SHA, SHA-1, SHA-2 and SHA-3 variants.

SIM Subscriber Identity Module. SIM is an integrated circuit that is intended to securely store the International Mobile Subscriber Identity (IMSI) number and its related key, which are used for identifying and authenticating subscribers on mobile telephony devices.

SIP Session Initiation Protocol. SIP is used for signaling and controlling multimedia communication session such as voice and video calls.

SIRT Security Incident Response Team. SIRT is responsible for reviewing as well as responding to computer security incident reports and activity.

SKU Stock Keeping Unit. SKU refers to the product and service identification code for the products in the inventory.

SLAAC Stateless Address Autoconfiguration. SLAAC provides the ability to address a host based on a network prefix that is advertised from a local network router through router advertisements.

SMB Server Message Block or Small and Medium Business. Server Message Block operates as an application- layer network protocol mainly used for providing shared access to files, printers, serial ports, and for miscellaneous communications between the nodes on a network.

SMS Short Message Service. SMS refers to short text messages (up to 140 characters) sent and received through mobile phones.

SMTP Simple Mail Transfer Protocol. SMTP is an Internet standard protocol for electronic mail transmission.

SNIR Signal-to-Noise-Plus-Interference Ratio. SNIR refers to the power of a central signal of interest divided by the sum of the interference power and the power of the background noise. SINR is defined as the power of a certain signal of interest divided by the sum of the interference power (from all the other interfering signals) and the power of some background noise.

SNMP Simple Network Management Protocol. SNMP is a TCP/IP standard protocol for managing devices on IP networks. Devices that typically support SNMP include routers, switches, servers, workstations, printers, modem racks, and more. It is used mostly in network management systems to monitor network-attached devices for conditions that warrant administrative attention.

SNMPv1 Simple Network Management Protocol version 1. SNMPv1 is a widely used network management protocol.

SNMPv2 Simple Network Management Protocol version 2. SNMPv2 is an enhanced version of SNMPv1, which includes improvements in the areas of performance, security, confidentiality, and manager-to-manager communications.

SNMPv2c Community-Based Simple Network Management Protocol version 2. SNMPv2C uses the community-based security scheme of SNMPv1 and does not include the SNMPv2 security model.

SNMPv3 Simple Network Management Protocol version 3. SNMPv3 is an enhanced version of SNMP that includes security and remote configuration features.

SNR Signal-to-Noise Ratio. SNR is used for comparing the level of a desired signal with the level of background noise.

SNTP Simple Network Time Protocol. SNTP is a less complex implementation of NTP. It uses the same , but does not require the storage of state over extended periods of time.

SOAP imple Object Access Protocol. SOAP enables communication between the applications running on different operating systems, with different technologies and programming languages. SOAP is an XML-based messaging protocol for exchanging structured information between the systems that support web services.

SoC System on a Chip. SoC is an Integrated Circuit that integrates all components of a computer or other electronic system into a single chip.

source NAT Source NAT changes the source address of the packets passing through the router. Source NAT is typically used when an internal (private) host initiates a session to an external (public) host.

SSH Secure Shell. SSH is a network protocol that provides secure access to a remote device.

SSID Service Set Identifier. SSID is a name given to a WLAN and is used by the client to access a WLAN network.

SSL Secure Sockets Layer. SSL is a computer networking protocol for securing connections between network application clients and servers over the Internet.

SSO Single Sign-On. SSO is an access-control property that allows the users to log in once to access multiple related, but independent applications or systems to which they have privileges. The process authenticates the user across all allowed resources during their session, eliminating additional login prompts.

STBC Space-Time Block Coding. STBC is a technique used in wireless communications to transmit multiple copies of a data stream across a number of antennas and to exploit the various received versions of the data to improve the reliability of data transfer.

STM Station Management. STM is a process that handles AP management and user association.

STP Spanning Tree Protocol. STP is a network protocol that builds a logical loop-free topology for Ethernet networks.

subnet Subnet is the logical division of an IP network.

subscription A business model where a customer pays a certain amount as subscription price to obtain access to a product or service.

SU-MIMO Single-User Multiple-Input Multiple-Output. SU-MIMO allocates the full bandwidth of the AP to a single high- speed device during the allotted time slice.

SVP SpectraLink Voice Priority. SVP is an open, straightforward QoS approach that has been adopted by most leading vendors of WLAN APs. SVP favors isochronous voice packets over asynchronous data packets when contending for the wireless medium and when transmitting packets onto the wired LAN.

SWAN Structured Wireless-Aware Network. A technology that incorporates a Wireless Local Area Network (WLAN) into a wired Wide Area Network (WAN). SWAN technology can enable an existing wired network to serve hundreds of users, organizations, corporations, or agencies over a large geographic area. SWAN is said to be scalable, secure, and reliable.

TAC Technical Assistance Center.

TACACS Terminal Access Controller Access Control System. TACACS is a family of protocols that handles remote authentication and related services for network access control through a centralized server.

TACACS+ Terminal Access Controller Access Control System+. TACACS+ provides separate authentication, authorization, and accounting services. It is derived from, but not backward compatible with, TACACS.

TCP Transmission Control Protocol. TCP is a communication protocol that defines the standards for establishing and maintaining network connection for applications to exchange data.

TCP/IP Transmission Control Protocol/ Internet Protocol. TCP/IP is the basic communication language or protocol of the Internet.

TFTP Trivial File Transfer Protocol. The TFTP is a software utility for transferring files from or to a remote host.

TIM Traffic Indication Map. TIM is an information element that advertises if any associated stations have buffered unicast frames. APs periodically send the TIM within a beacon to identify the stations that are using power saving mode and the stations that have undelivered data buffered on the AP.

TKIP Temporal Key Integrity Protocol. A part of the WPA encryption standard for wireless networks. TKIP is the next- generation Wired Equivalent Privacy (WEP) that provides per-packet key mixing to address the flaws encountered in the WEP standard.

TLS Transport Layer Security. TLS is a cryptographic protocol that provides communication security over the Internet. TLS encrypts the segments of network connections above the Transport Layer by using asymmetric cryptography for key exchange, symmetric encryption for privacy, and message authentication codes for message integrity.

TLV Type-length-value or Tag-Length-Value. TLV is an encoding format. It refers to the type of data being processed, the length of the value, and the value for the type of data being processed.

ToS Type of Service. The ToS field is part of the IPv4 header, which specifies datagrams priority and requests a route for low-delay, high-throughput, or a highly reliable service.

TPC Transmit Power Control. TPC is a part of the 802.11h amendment. It is used to regulate the power levels used by 802.11a radio cards.

TPM Trusted Platform Module. TPM is an international standard for a secure cryptoprocessor, which is a dedicated microcontroller designed to secure hardware by integrating cryptographic keys into devices.

TSF Timing Synchronization Function. TSF is a WLAN function that is used for synchronizing the timers for all the stations in a BSS.

TSPEC Traffic Specification. TSPEC allows an 802.11e client or a QoS-capable wireless client to signal its traffic requirements to the AP.

TSV Tab-Separated Values. TSV is a file format that allows the exchange of tabular data between applications that use different internal data formats.

TTL Time to Live. TTL or hop limit is a mechanism that sets limits for data expiry in a computer or network.

TTY TeleTypeWriter. TTY-enabled devices allow telephones to transmit text communications for people who are deaf or hard of hearing as well as transmit voice communication.

TXOP Transmission Opportunity. TXOP is used in wireless networks supporting the IEEE 802.11e Quality of Service (QoS) standard. Used in both EDCA and HCF Controlled Channel Access modes of operation, TXOP is a bounded time interval in which stations supporting QoS are permitted to transfer a series of frames. TXOP is defined by a start time and a maximum duration.

UAM Universal Access Method. UAM allows subscribers to access a wireless network after they successfully log in from a web browser.

U-APSD Unscheduled Automatic Power Save Delivery. U-APSD is a part of 802.11e and helps considerably in increasing the battery life of VoWLAN terminals.

UCC Unified Communications and Collaboration. UCC is a term used to describe the integration of various communications methods with collaboration tools such as virtual whiteboards, real-time audio and video conferencing, and enhanced call control capabilities.

UDID Unique Device Identifier. UDID is used to identify an iOS device.

UDP User Datagram Protocol. UDP is a part of the TCP/IP family of protocols used for data transfer. UDP is typically used for streaming media. UDP is a stateless protocol, which means it does not acknowledge that the packets being sent have been received.

UDR User Derivation Rule. UDR is a role assignment model used by the controllers running ArubaOS to assign roles and VLANs to the WLAN users based on MAC address, BSSID, DHCP-Option, encryption type, SSID, and the location of a user. For example, for an SSID with captive portal in the initial role, a UDR can be configured for scanners to provide a role based on their MAC OUI.

UHF	Ultra high frequency. UHF refers to radio frequencies between the range of 300 MHz and 3 GHz. UHF is also known as the decimeter band as the wavelengths range from one meter to one decimeter.
UI	User Interface.
UMTS	Universal Mobile Telecommunication System. UMTS is a third generation mobile cellular system for networks. See 3G.
UPnP	Universal Plug and Play. UPnp is a set of networking protocols that permits networked devices, such as personal computers, printers, Internet gateways, Wi-Fi APs, and mobile devices to seamlessly discover each other's presence on the network and establish functional network services for data sharing, communications, and entertainment.
URI	Uniform Resource Identifier. URI identifies the name and the location of a resource in a uniform format.
URL	Uniform Resource Locator. URL is a global address used for locating web resources on the Internet.
USB	Universal Serial Bus. USB is a connection standard that offers a common interface for communication between the external devices and a computer. USB is the most common port used in the client devices.
UTC	Coordinated Universal Time. UTC is the primary time standard by which the world regulates clocks and time.
UWB	Ultra-Wideband. UWB is a wireless technology for transmitting large amounts of digital data over a wide spectrum of frequency bands with very low power for a short distance.
VA	Virtual Appliance. VA is a pre-configured virtual machine image, ready to run on a hypervisor.
VBR	Virtual Beacon Report. VBR displays a report with the MAC address details and RSSI information of an AP.
VHT	Very High Throughput. IEEE 802.11ac is an emerging VHT WLAN standard that could achieve physical data rates of close to 7 Gbps for the 5 GHz band.
VIA	Virtual Intranet Access. VIA provides secure remote network connectivity for Android, Apple iOS, Mac OS X, and Windows mobile devices and laptops. It automatically scans and selects the best secure connection to the corporate network.
VLAN	Virtual Local Area Network. In computer networking, a single Layer 2 network may be partitioned to create multiple distinct broadcast domains, which are mutually isolated so that packets can only pass between them through one or more routers; such a domain is referred to as a Virtual Local Area Network, Virtual LAN, or VLAN.
VM	Virtual Machine. A VM is an emulation of a computer system. VMs are based on computer architectures and provide functionality of a physical computer.
VoIP	Voice over IP. VoIP allows transmission of voice and multimedia content over an IP network.

VoWLAN Voice over WLAN. VoWLAN is a method of routing telephone calls for mobile users over the Internet using the technology specified in IEEE 802.11b. Routing mobile calls over the Internet makes them free, or at least much less expensive than they would be otherwise.

VPN Virtual Private Network. VPN enables secure access to a corporate network when located remotely. It enables a computer to send and receive data across shared or public networks as if it were directly connected to the private network, while benefiting from the functionality, security, and management policies of the private network. This is done by establishing a virtual point-to-point connection through the use of dedicated connections, encryption, or a combination of the two.

VRD Validated Reference Design. VRDs are guides that capture the best practices for a particular technology in field.

VRF VisualRF. VRF is an AirWave Management Platform (AMP) module that provides a real-time, network-wide views of your entire Radio Frequency environment along with floor plan editing capabilities. VRF also includes overlays on client health to help diagnose issues related to clients, floor plan, or a specific location.

VRF Plan VisualRF Plan. A stand-alone Windows client used for basic planning procedures such as adding a floor plan, provisioning APs, and generating a Bill of Materials report.

VRRP Virtual Router Redundancy Protocol. VRRP is an election protocol that dynamically assigns responsibility for a virtual router to one of the VRRP routers on a LAN.

VSA Vendor-Specific Attribute. VSA is a method for communicating vendor-specific information between NASs and RADIUS servers.

VTP VLAN Trunking Protocol. VTP is a Cisco proprietary protocol for propagating VLANs on a LAN.

walled garden Walled garden is a feature that allows blocking of unauthorized users from accessing network resources.

WAN Wide Area Network. WAN is a telecommunications network or computer network that extends over a large geographical distance.

WASP Wireless Application Service Provider. WASP provides a web-based access to applications and services that would otherwise have to be stored locally and makes it possible for customers to access the service from a variety of wireless devices, such as a smartphone or Personal Digital Assistant (PDA).

WAX Wireless abstract XML. WAX is an abstract markup language and a set of tools that is designed to help wireless application development as well as portability. Its tags perform at a higher level of abstraction than that of other wireless markup languages such as HTML, HDML, WML, XSL, and more.

W-CDMA Wideband Code-Division Multiple Access. W-CDMA is a third-generation (3G) mobile wireless technology that promises much higher data speeds to mobile and portable wireless devices.

web service Web services allow businesses to share and process data programmatically. Developers who want to provide integrated applications can use the API to programmatically perform actions that would otherwise require manual operation of the user interface.

WEP
Wired Equivalent Privacy. WEP is a security protocol that is specified in 802.11b and is designed to provide a WLAN with a level of security and privacy comparable to what is usually expected of a wired LAN.

WFA
Wi-Fi Alliance. WFA is a non-profit organization that promotes Wi-Fi technology and certifies Wi-Fi products if they conform to certain standards of interoperability.

WIDS
Wireless Intrusion Detection System. WIDS is an application that detects the attacks on a wireless network or wireless system.

Wi-Fi
Wi-Fi is a technology that allows electronic devices to connect to a WLAN network, mainly using the 2.4 GHz and 5 GHz radio bands. Wi-Fi can apply to products that use any 802.11 standard.

WiMAX
Worldwide Interoperability for Microwave Access. WiMAX refers to the implementation of IEEE 802.16 family of wireless networks standards set by the WiMAX forum.

WIP
Wireless Intrusion Protection. The WIP module provides wired and wireless AP detection, classification, and containment. It detects Denial of Service (DoS) and impersonation attacks, and prevents client and network intrusions.

WIPS
Wireless Intrusion Prevention System. WIPS is a dedicated security device or integrated software application that monitors the radio spectrum of WLAN network for rogue APs and other wireless threats.

WISP
Wireless Internet Service Provider. WISP allows subscribers to connect to a server at designated hotspots using a wireless connection such as Wi-Fi. This type of ISP offers broadband service and allows subscriber computers called stations, to access the Internet and the web from anywhere within the zone of coverage provided by the server antenna, usually a region with a radius of several kilometers.

WISPr
Wireless Internet Service Provider Roaming. The WISPr framework enables the client devices to roam between the wireless hotspots using different ISPs.

WLAN
Wireless Local Area Network. WLAN is a 802.11 standards-based LAN that the users access through a wireless connection.

WME
Wireless Multimedia Extension. WME is a Wi-Fi Alliance interoperability certification, based on the IEEE 802.11e standard. It provides basic QoS features to IEEE 802.11 networks. WMM prioritizes traffic according to four ACs: voice (AC_VO), video (AC_VI), best effort (AC_BE) and background (AC_BK). See WMM.

WMI
Windows Management Instrumentation. WMI consists of a set of extensions to the Windows Driver Model that provides an operating system interface through which instrumented components provide information and notification.

WMM
Wi-Fi Multimedia. WMM is also known as WME. It refers to a Wi-Fi Alliance interoperability certification, based on the IEEE 802.11e standard. It provides basic QoS features to IEEE 802.11 networks. WMM prioritizes traffic according to four ACs: voice (AC_VO), video (AC_VI), best effort (AC_BE), and background (AC_BK).

WPA Wi-Fi Protected Access. WPA is an interoperable wireless security specification subset of the IEEE 802.11 standard. This standard provides authentication capabilities and uses TKIP for data encryption.

WPA2 Wi-Fi Protected Access 2. WPA2 is a certification program maintained by IEEE that oversees standards for security over wireless networks. WPA2 supports IEEE 802.1X/EAP authentication or PSK technology, but includes advanced encryption mechanism using CCMP that is referred to as AES.

WSDL Web Service Description Language. WSDL is an XML-based interface definition language used to describe the functionality provided by a web service.

WSP Wireless Service Provider. The service provider company that offers transmission services to users of wireless devices through Radio Frequency (RF) signals rather than through end-to-end wire communication.

WWW World Wide Web.

X.509 X.509 is a standard for a public key infrastructure for managing digital certificates and public-key encryption. It is an essential part of the Transport Layer Security protocol used to secure web and email communication.

XAuth Extended Authentication. XAuth provides a mechanism for requesting individual authentication information from the user, and a local user database or an external authentication server. It provides a method for storing the authentication information centrally in the local network.

XML Extensible Markup Language. XML is a markup language that defines a set of rules for encoding documents in a format that is both human-readable and machine-readable.

XML-RPC ML Remote Procedure Call. XML-RPC is a protocol that uses XML to encode its calls and HTTP as a transport mechanism. Developers who want to provide integrated applications can use the API to programmatically perform actions that would otherwise require manual operation of the user interface.

ZTP Zero Touch Provisioning. ZTP is a device provisioning mechanism that allows automatic and quick provisioning of devices with a minimal or at times no manual intervention.