CONFIGURATION GUIDE

RUCKUS SmartZone (ST-GA) Traffic Management Guide, 7.0.0

Supporting SmartZone 7.0.0

Part Number: 800-73370-001 Rev A
Publication Date: February 2024

Export Restrictions

These products and associated technical data (in print or electronic form) may be subject to export control laws of the United States of America. It is your responsibility to determine the applicable regulations and to comply with them. The following notice is applicable for all products or technology subject to export control:

These items are controlled by the U.S. Government and authorized for export only to the country of ultimate destination for use by the ultimate consignee or end-user(s) herein identified. They may not be resold, transferred, or otherwise disposed of, to any other country or to any person other than the authorized ultimate consignee or end-user(s), either in their original form or after being incorporated into other items, without first obtaining approval from the U.S. government or as otherwise authorized by U.S. law and regulations.

Disclaimer

THIS CONTENT AND ASSOCIATED PRODUCTS OR SERVICES ("MATERIALS"), ARE PROVIDED "AS IS" AND WITHOUT WARRANTIES OF ANY KIND, WHETHER EXPRESS OR IMPLIED. TO THE FULLEST EXTENT PERMISSIBLE PURSUANT TO APPLICABLE LAW, COMMSCOPE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, TITLE, NON-INFRINGEMENT, FREEDOM FROM COMPUTER VIRUS, AND WARRANTIES ARISING FROM COURSE OF DEALING OR COURSE OF PERFORMANCE. CommScope does not represent or warrant that the functions described or contained in the Materials will be uninterrupted or error-free, that defects will be corrected, or are free of viruses or other harmful components. CommScope does not make any warranties or representations regarding the use of the Materials in terms of their completeness, correctness, accuracy, adequacy, usefulness, timeliness, reliability or otherwise. As a condition of your use of the Materials, you warrant to CommScope that you will not make use thereof for any purpose that is unlawful or prohibited by their associated terms of use.

Limitation of Liability

IN NO EVENT SHALL COMMSCOPE, COMMSCOPE AFFILIATES, OR THEIR OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS, LICENSORS AND THIRD PARTY PARTNERS, BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, PUNITIVE, INCIDENTAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER, EVEN IF COMMSCOPE HAS BEEN PREVIOUSLY ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, WHETHER IN AN ACTION UNDER CONTRACT, TORT, OR ANY OTHER THEORY ARISING FROM YOUR ACCESS TO, OR USE OF, THE MATERIALS. Because some jurisdictions do not allow limitations on how long an implied warranty lasts, or the exclusion or limitation of liability for consequential or incidental damages, some of the above limitations may not apply to you.

Trademarks

CommScope and the CommScope logo are registered trademarks of CommScope and/or its affiliates in the U.S. and other countries. For additional trademark information see https://www.commscope.com/trademarks. All product names, trademarks, and registered trademarks are the property of their respective owners.

Patent Marking Notice

For applicable patents, see www.cs-pat.com.

Contents

Contact Information, Resources, and Conventions

Contacting RUCKUS Customer Services and Support

The Customer Services and Support (CSS) organization is available to provide assistance to customers with active warranties on their RUCKUS products, and customers and partners with active support contracts.

For product support information and details on contacting the Support Team, go directly to the RUCKUS Support Portal using https://support.ruckuswireless.com, or go to https://www.ruckusnetworks.com and select **Support**.

What Support Do I Need?

Technical issues are usually described in terms of priority (or severity). To determine if you need to call and open a case or access the self-service resources, use the following criteria:

- Priority 1 (P1)—Critical. Network or service is down and business is impacted. No known workaround. Go to the **Open a Case** section.
- Priority 2 (P2)—High. Network or service is impacted, but not down. Business impact may be high. Workaround may be available. Go to the **Open a Case** section.
- Priority 3 (P3)—Medium. Network or service is moderately impacted, but most business remains functional. Go to the **Self-Service Resources** section.
- Priority 4 (P4)—Low. Requests for information, product documentation, or product enhancements. Go to the **Self-Service Resources** section.

Open a Case

When your entire network is down (P1), or severely impacted (P2), call the appropriate telephone number listed below to get help:

- Continental United States: 1-855-782-5871
- Canada: 1-855-782-5871
- Europe, Middle East, Africa, Central and South America, and Asia Pacific, toll-free numbers are available at https://support.ruckuswireless.com/contact-us and Live Chat is also available.
- Worldwide toll number for our support organization. Phone charges will apply: +1-650-265-0903

We suggest that you keep a physical note of the appropriate support number in case you have an entire network outage.

Self-Service Resources

The RUCKUS Support Portal at https://support.ruckuswireless.com offers a number of tools to help you to research and resolve problems with your RUCKUS products, including:

- Technical Documentation—https://support.ruckuswireless.com/documents
- Community Forums—https://community.ruckuswireless.com
- Knowledge Base Articles—https://support.ruckuswireless.com/answers
- Software Downloads and Release Notes—https://support.ruckuswireless.com/#products_grid
- Security Bulletins—https://support.ruckuswireless.com/security

Using these resources will help you to resolve some issues, and will provide TAC with additional data from your troubleshooting analysis if you still require assistance through a support case or RMA. If you still require help, open and manage your case at https://support.ruckuswireless.com/case_management.

Document Feedback

RUCKUS is interested in improving its documentation and welcomes your comments and suggestions.

You can email your comments to RUCKUS at #Ruckus-Docs@commscope.com.

When contacting us, include the following information:

- Document title and release number
- Document part number (on the cover page)
- Page number (if appropriate)

For example:

- RUCKUS SmartZone Upgrade Guide, Release 5.0
- Part number: 800-71850-001 Rev A
- Page 7

RUCKUS Product Documentation Resources

Visit the RUCKUS website to locate related documentation for your product and additional RUCKUS resources.

Release Notes and other user documentation are available at https://support.ruckuswireless.com/documents. You can locate the documentation by product or perform a text search. Access to Release Notes requires an active support contract and a RUCKUS Support Portal user account. Other technical documentation content is available without logging in to the RUCKUS Support Portal.

White papers, data sheets, and other product documentation are available at https://www.ruckusnetworks.com.

Online Training Resources

To access a variety of online RUCKUS training modules, including free introductory courses to wireless networking essentials, site surveys, and products, visit the RUCKUS Training Portal at https://commscopeuniversity.myabsorb.com/. The registration is a two-step process described in this video. You create a CommScope account and then register for, and request access for, CommScope University.

Document Conventions

The following table lists the text conventions that are used throughout this guide.

TABLE 1 Text Conventions

Convention	Description	Example
`monospace`	Identifies command syntax examples	`device(config)# interface ethernet 1/1/6`
bold	User interface (UI) components such as screen or page names, keyboard keys, software buttons, and field names	On the **Start** menu, click **All Programs**.
italics	Publication titles	Refer to the *RUCKUS Small Cell Release Notes* for more information.

Notes, Cautions, and Safety Warnings

Notes, cautions, and warning statements may be used in this document. They are listed in the order of increasing severity of potential hazards.

NOTE
A NOTE provides a tip, guidance, or advice, emphasizes important information, or provides a reference to related information.

ATTENTION
An ATTENTION statement indicates some information that you must read before continuing with the current action or task.

CAUTION
A CAUTION statement alerts you to situations that can be potentially hazardous to you or cause damage to hardware, firmware, software, or data.

DANGER
A DANGER statement indicates conditions or situations that can be potentially lethal or extremely hazardous to you. Safety labels are also attached directly to products to warn of these conditions or situations.

Command Syntax Conventions

Bold and italic text identify command syntax components. Delimiters and operators define groupings of parameters and their logical relationships.

Convention	Description
bold text	Identifies command names, keywords, and command options.
italic text	Identifies a variable.
[ ]	Syntax components displayed within square brackets are optional. Default responses to system prompts are enclosed in square brackets.
{**x** | **y** | **z**}	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options.
x | **y**	A vertical bar separates mutually exclusive elements.
< >	Nonprinting characters, for example, passwords, are enclosed in angle brackets.
...	Repeat the previous element, for example, *member*[*member*...].
\	Indicates a “soft” line break in command examples. If a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.

About This Document

New In This Document

TABLE 2 Key Features and Enhancements in *SmartZone 7.0.0 Rev A* (*February 2024*)

Feature	Description	Reference
Editorial updates	Minor editorial updates	Throughout the guide.

Application Control

Viewing an Application Control Summary

You can view an application-specific or port-specific summary in a chart or table format.

Complete the following steps to view the application control summary.

1. From the main menu, go to **Security** > **Application Control** > **Summary**.

   The **Summary** page is displayed.

2. The **Summary** page can be viewed with following options:

   - Top Applications by: Choose Application or Port from the menu.
   - Click to view by Chart or Table.
   - **Count:** Select **10** or **25**.
   - Total, 2.4 GHz, 5GHz, and 6GHz.
   - **Duration:** Select **Last 1 hour** or **Last 24 hours**.
   - APs: Select a specific AP or **All APs**.
   - All Clients: Select All Clients, Wired or Wireless clients.

Creating an Application Control Policy

An application control policy is created to limit and classify traffic into priority queues using QoS traffic shaping rules, or to completely block access to an application.

Complete the following steps to create an application control policy.

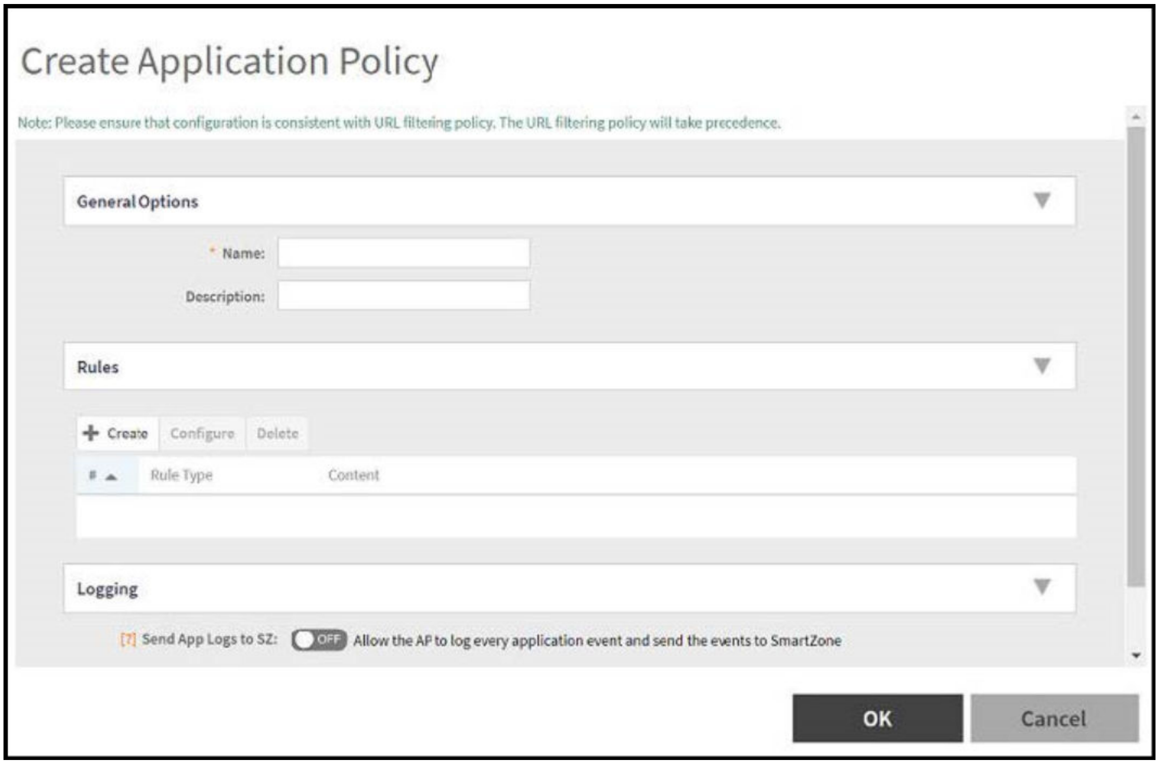
1. From the main menu, go to **Security** > **Application Control** > **Application Policy**.

   The **Application Policy** page is displayed.

2. Click **Create**.

   The **Create Application Policy** dialog box is displayed.

   FIGURE 1 Creating an Application Policy



Create Application Policy

Note: Please ensure that configuration is consistent with URL filtering policy. The URL filtering policy will take precedence.

[?] Send App Logs to SZ: OFF Allow the AP to log every application event and send the events to SmartZone

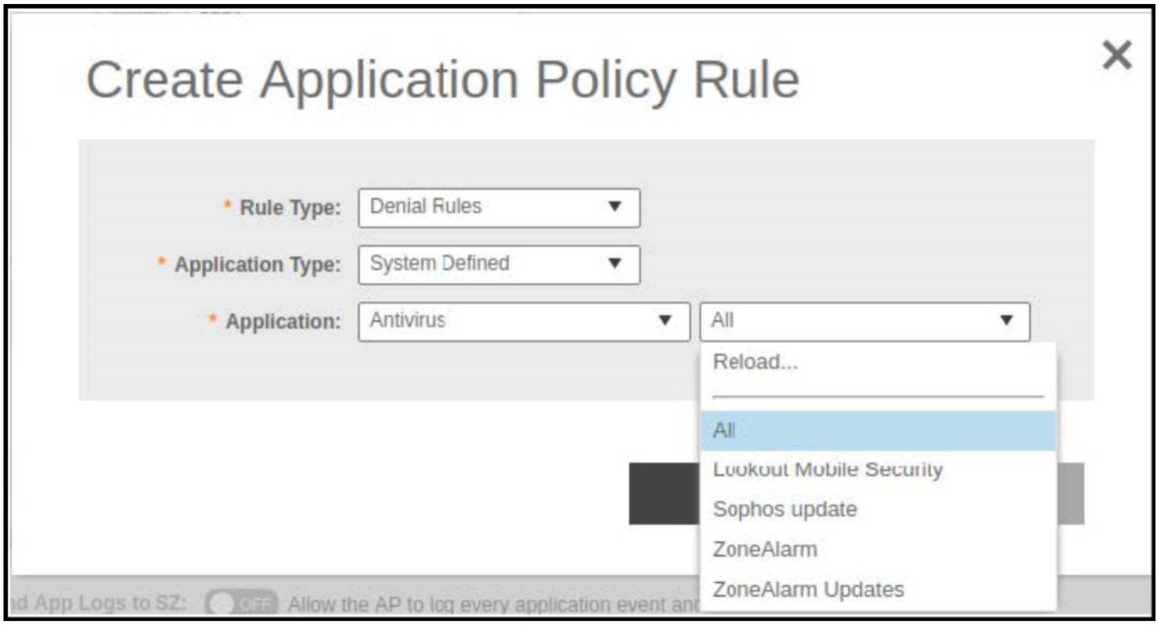
3. Under **General Options**, enter the policy name and description.

4. Under **Rules**, click **Create** to create a new rule.

   NOTE
   Each application policy can contain up to 128 rules.

   The **Create Application Policy Rule** dialog box is displayed.

   FIGURE 2 Creating an Application Policy Rule

   Create Application Policy Rule

   * Rule Type: Denial Rules

   * Application Type: System Defined

   * Application: Antivirus All

5. From the **Rule Type** list, select one of the following options:
   - **Denial Rules**
   - **QoS**
   - **Rate Limiting**
6. From the **Application Type** list, select an application type.
7. From the **Application** field, select the application for which you want to create a policy rule.

   For example, if you select **All** in the Anitvirus application category and save the application rule, the application rule list reflects all antivirus applications and is selected as a single entry in the rule list. A full category is counted as one rule in the allotment of 128 Layer 7 rules in a Layer 7 policy.
8. Click **OK** to save the rule.

   NOTE
   If a rule is already created, you can edit its configuration settings by selecting the rule and clicking **Configure** in the **Create Application Policy** dialog box.
9. Under **Logging**, select the appropriate option for the APs to log events:
   - **Allow the AP to log every application event and send the events to SmartZone**
   - **Allow the AP to log every application event and send the events to external syslog**
10. Click **OK** to save the application control policy.

You can continue to apply the application control policy to user traffic.

Working with Application Signature Packages

RUCKUS periodically releases and makes new application signature packages available for download.

The controller web user interface displays a notification on the **Dashboard**, when the latest signature application package is available for download.

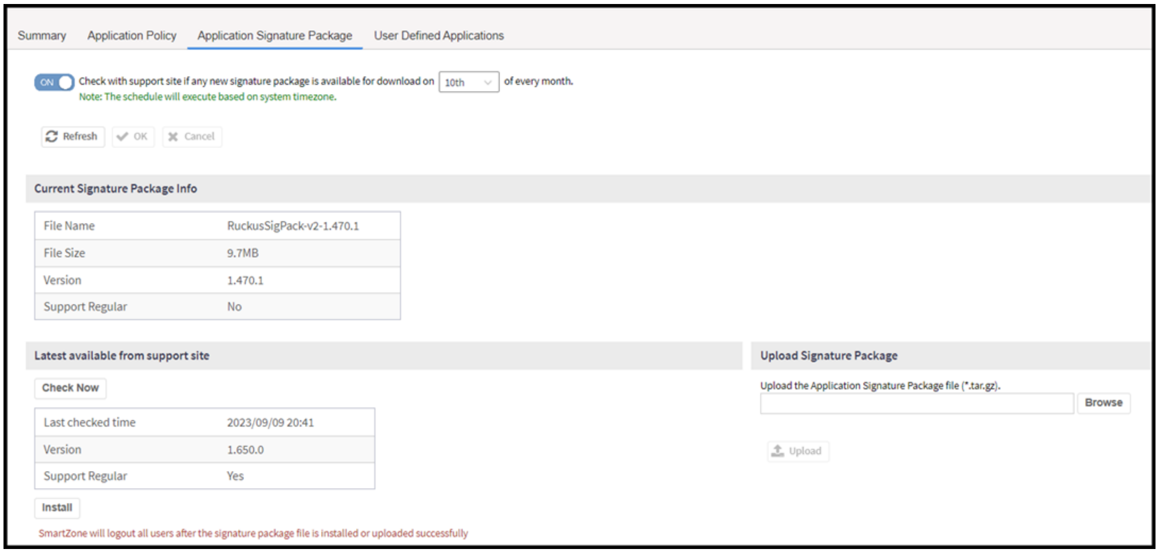
Alternatively, application signature package updates or downloads can be scheduled from the RUCKUS download center.

Complete the following steps to check for application signature package updates.

1. From the main menu, go to **Security** > **Application Control** > **Application Signature Package**.

   The **Application Signature Package** tab is displayed.

   FIGURE 3 Checking the Application Signature Package

   ON Check with support site if any new signature package is available for download on 10th of every month.
   Note: The schedule will execute based on system timezone.

   Current Signature Package Info

File Name	RuckusSigPack-v2-1.470.1
File Size	9.7MB
Version	1.470.1
Support Regular	No

   Latest available from support site

Last checked time	2023/09/09 20:41
Version	1.650.0
Support Regular	Yes

   SmartZone will logout all users after the signature package file is installed or uploaded successfully

   Upload Signature Package

   Upload the Application Signature Package file (*.tar.gz).

2. Switch **ON** the **Check with support site if any new signature package is available for download** option and select the date of the month from the date list to schedule updates every month. A periodic check for the latest available signature package is triggered at a random date.

   NOTE
   The schedule will run based on the system time zone.

   Under **Current Signature Package Info**, the file name, file size, version, and type of signature package are displayed.

3. Under the **Latest available from support site**, click **Check Now** to check for any latest update.

4. Click **Install** to install the latest signature package.

   After the signature package file is installed or uploaded successfully, controller logs out all users.

Creating a User-Defined Application

When an application is unrecognized and generically (or incorrectly) categorized, the controller is unable to monitor its traffic, unless you configure an explicit application identification policy based on IP address or mask, port, and protocol.

Complete the following steps to configure a user-defined application.

1. From the main menu, go to **Security** > **Application Control** > **User Defined Applications**.
2. Click **Create**.

   The **Create User Defined Application** dialog box is displayed.
3. Configure the following options:
   - **Name**: Enter a name for the application. This name that will identify this application on the dashboard.
   - **Type**: Select **Default** or **Port Mapping.**
   - **IP Mode**: Select **IPv4** or **IPv6** address.
   - **Destination IP/Netmask**: Enter the destination IP address of the application and the netmask of the destination IP address.
   - **Destination Port**: Enter the destination port for the application.
   - **Protocol**: Select the protocol used by the application. Options include **TCP** and **UDP**.
4. Click **OK**.

   NOTE
   You can also edit, clone, and delete the user-defined application by selecting the options **Configure**, **Clone**, and **Delete** respectively from the **User Defined** tab.

Core Network Tunnel Stats

Viewing Statistics for the L2oGRE Core Network Tunnel

An L2oGRE forwarding profile defines the gateway and tunnel configuration for the core network of L2oGRE tunnels.

Complete the following steps to view the statistics for the L2oGRE core network tunnel.

1. From the main menu, go to **Monitor** > **Report** > **Core Network Tunnel Stats**. The **L2oGRE** dialog box is displayed.
2. Configure the following options:
   - **Time Period:** Move the slider to set the duration for which you want to view the report.
   - **Data Plane:** Select the data plane.
   - **Gateway IP Address:** Enter the gateway IP address.
   - **MVNO Name:** Select the mobile network operation name (MVNO).
3. Click **Load Data** to view the report in the workspace or **Export CSV** to open or save the report in CSV file format.

Table 3 contains the report attributes based on the statistics for the L2oGRE core network tunnel.

TABLE 3 L2oGRE Core Network Tunnel Attributes

Attribute	Type	Description
Time	Long	Bin ID, which is stamped at 15-minute intervals; for example, 10:00, 10:15, 10:30.
TX Bytes	Long	Indicates the number of bytes sent.
RX Bytes	Long	Indicates the number of bytes received.
TX Packets	Long	Indicates the number of packets sent.
RX Packets	Long	Indicates the number of packets received.
Dropped Packets	Long	Indicates the number of packets dropped.

Viewing Statistics for the GTP Core Network Tunnel

GPRS Tunneling Protocol (GTP) transmits user data packets and signals between the controller and the gateway GPRS support node (GGSN).You can view historical traffic statistics and trends of the GTP core tunnels.

GTP encapsulates traffic and creates GTP tunnels, which act as virtual data channels for transmission of data between the controller and the GGSN. A GTP tunnel is established between the controller and the GGSN for a data session initiated from the user equipment (UE).

Complete the following steps to view the GTP core network tunnel statistics.

1. From the main menu, go to **Monitor** > **Report** > **RUCKUS AP Tunnel Stats**. The **SoftGRE** dialog box is displayed.
2. Select GTP and configure the following options:
   - **Time Period:** Move the slider to set the duration for which you want to view the report.
   - **Zone Name:** Select the zone name.

- **Gateway IP Address:** Enter the gateway IP address.
- **AP MAC or IP Address:** Enter the AP MAC address or IP address.

3. Click **Load Data** to view the report in the workspace or **Export CSV** to open or save the report in CSV file format.

The below table lists the attributes based on the statistics for the GTP. Each entry contains the cumulative data for the 15-minute interval.

TABLE 4 GTP Report Attributes

Attribute	Type	Description
Time	Long	Bin ID, which is stamped at 15-minute intervals; for example, 10:00, 10:15, 10:30.
TX Bytes	Long	Indicates the number of bytes sent.
RX Bytes	Long	Indicates the number of bytes received.
TX Packets	Long	Indicates the number of packets sent.
RX Packets	Long	Indicates the number of packets received.
Tx Dropped Packets	Long	Indicates the number of packets dropped while sending.
Rx Dropped Packets	Long	Indicates the number of packets dropped while receiving.
Bad GTPU	Long	Indicates a tunneling mechanism that provides a service for carrying user data packets dropped.
RX TEID Invalid	Long	Indicates the number of invalid packets received by Tunnel End Point Identifiers (TEID).
TX TEID Invalid	Long	Indicates the number of invalid packets sent by the Tunnel End Point Identifiers (TEID).
Echo RX	Long	Indicates the echo message received.
Last Echo RX Time	Long	Indicates the time when the last echo message was received.

DHCP and NAT

Viewing DHCP and NAT Information

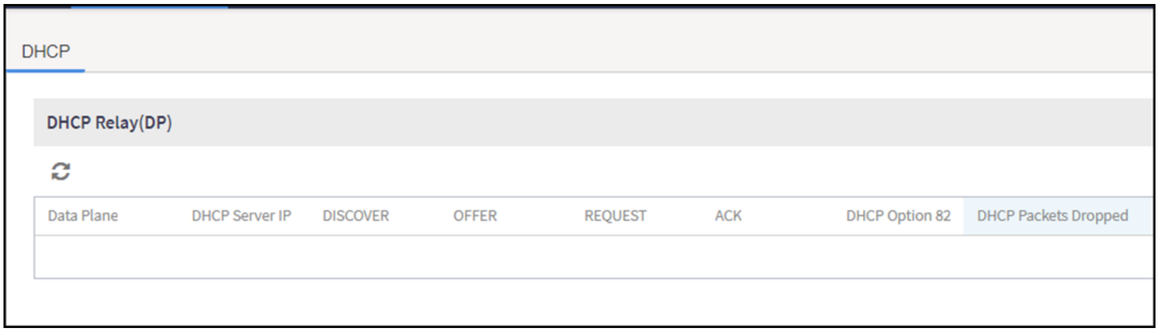
DHCP or NAT functionality on controller managed APs and DPs (data planes) allows customers to reduce costs and complexity by removing the need for DHCP server or NAT router to provide IP addresses to clients. For data traffic aggregation and services delivery, choose the appropriate user profile for DHCP and NAT services on the virtual controllers.

Complete the following steps to view DHCP servers and NAT router information.

NOTE
You must be aware of the DHCP and NAT information of the controller to monitor the health of the controller.

1. From the main menu go to **Monitor** > **Troubleshooting&Diagnostics** > **DHCP&NAT** in High or Enterprise virtual controllers or **Monitor** > **Troubleshooting&Diagnostics** > **DHCP** in SZ300 or SZ100 controller platforms.
2. Select **DHCP** to monitor **DHCP Relay (DP)** of the data planes. It displays information pertaining to relay packets, server packets and the number of IP addresses assigned when **DHCP Relay** is enabled in **Core Network Tunnel** > **Bridge or L2oGRE**.

FIGURE 4 DHCP Relay



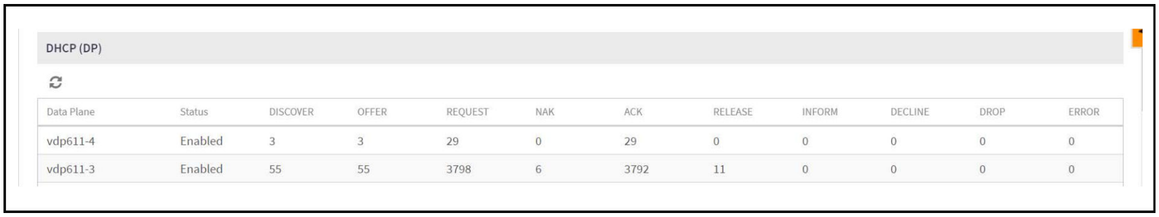
DHCP Relay(DP)

Data Plane	DHCP Server IP	DISCOVER	OFFER	REQUEST	ACK	DHCP Option 82	DHCP Packets Dropped

The following options are seen on virtual controllers.

3. From the main menu go to **Monitor** > **Troubleshooting&Diagnostics** > **DHCP&NAT** > > **DHCP (DP)** to monitor data planes. It displays information pertaining to data planes, status and other related information to data planes

FIGURE 5 DHCP DP

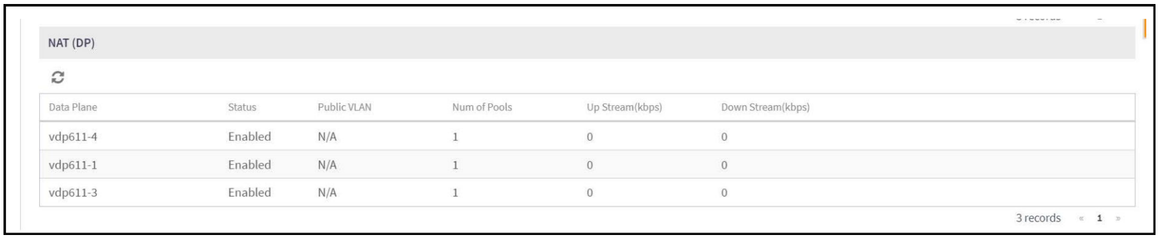


DHCP (DP)

Data Plane	Status	DISCOVER	OFFER	REQUEST	NAK	ACK	RELEASE	INFORM	DECLINE	DROP	ERROR
vdp611-4	Enabled	3	3	29	0	29	0	0	0	0	0
vdp611-3	Enabled	55	55	3798	6	3792	11	0	0	0	0

4. Select **NAT (DP)** to monitor the NAT router information of the data planes. It displays information the server packets and the number of used ports.

FIGURE 6 NAT DP



NAT (DP)

Data Plane	Status	Public VLAN	Num of Pools	Up Stream(kbps)	Down Stream(kbps)
vdp611-4	Enabled	N/A	1	0	0
vdp611-1	Enabled	N/A	1	0	0
vdp611-3	Enabled	N/A	1	0	0

3 records « 1 »

Working with DHCP

DHCP Server or NAT Router

DHCP or NAT functionality on controller managed APs and DPs (data planes) allows customers to reduce costs and complexity by removing the need for DHCP server or NAT router to provide IP addresses to clients. For data traffic aggregation and services delivery, choose the appropriate user profile for DHCP and NAT services on the Virtual SmartZone Data Plane (vSZ-D).

AP Based DHCP or NAT

In highly distributed environments, particularly those with only a few APs per site, the ability for an AP or a set of APs to provide DHCP or NAT support to local client devices simplifies deployment by providing all-in-one functionality on the AP, which eliminates the need for a separate router and DHCP server for each site. It also eases site management by providing central control and monitoring of the distributed APs and their clients.

NOTE
While changing from a non-DHCP or a non-NAT enabled zone to a DHCP or a NAT enabled zone, the AP will start the DHCP services on the gateway AP.

Three general DHCP scenarios are supported:

- SMB Single AP: DHCP is running on a single AP only. This AP also functions as the Gateway AP.
- SMB Multiple APs (<12): DHCP service is running on all APs, among which two of the APs will be Gateway APs. These two Gateway APs will provide the IP addresses as well as Internet connectivity to the clients through NAT.
- Enterprise (>12): For Enterprise sites, an additional on site vSZ-D will be deployed at the remote site which will assume the responsibilities of performing DHCP or NAT functions. Therefore, DHCP or NAT service will not be running on any APs (they will serve clients only), while the DHCP or NAT services are provided by the onsite vSZ-D.

Profile Based DHCP

The DHCP Server is designed in-line in the data plane and provides extreme scale in terms of IP address assignment to clients. This feature is especially useful in high density and dynamic deployments like stadiums, train stations where large number of clients continuously move in and out of Wi-Fi coverage. The DHCP server in the network needs to scale to meet these challenging requirements. The DHCP server on the vSZ-D provides high scale IP address assignment and management with minimal impact on forwarding latency. The DHCP server allows IP address assignment only when a DHCP license assignment policy is created for a specific vSZ-D. A maximum of 101k IP address assignments are allowed for each vSZ-D. Additional IP address assignments require additional licensing.

NOTE
DHCP server or NAT router if enabled, is supported only for wireless client IPv4 address assignment.

Profile-based NAT

With NAT service enabled, all the Wi-FI client traffic is NAT routed by the vSZ-D before forwarding to the core network. The NAT license assignment policy for the specific vSZ-D must be created. Each vSZ-D supports up to 2 million NAT ports (traffic sessions) and 128 public IP addresses for NAT. This feature reduces the network overhead significantly since it reduces the MAC-table considerations on the UP-stream switches significantly. This feature is very useful in high density deployments.

Network Topology

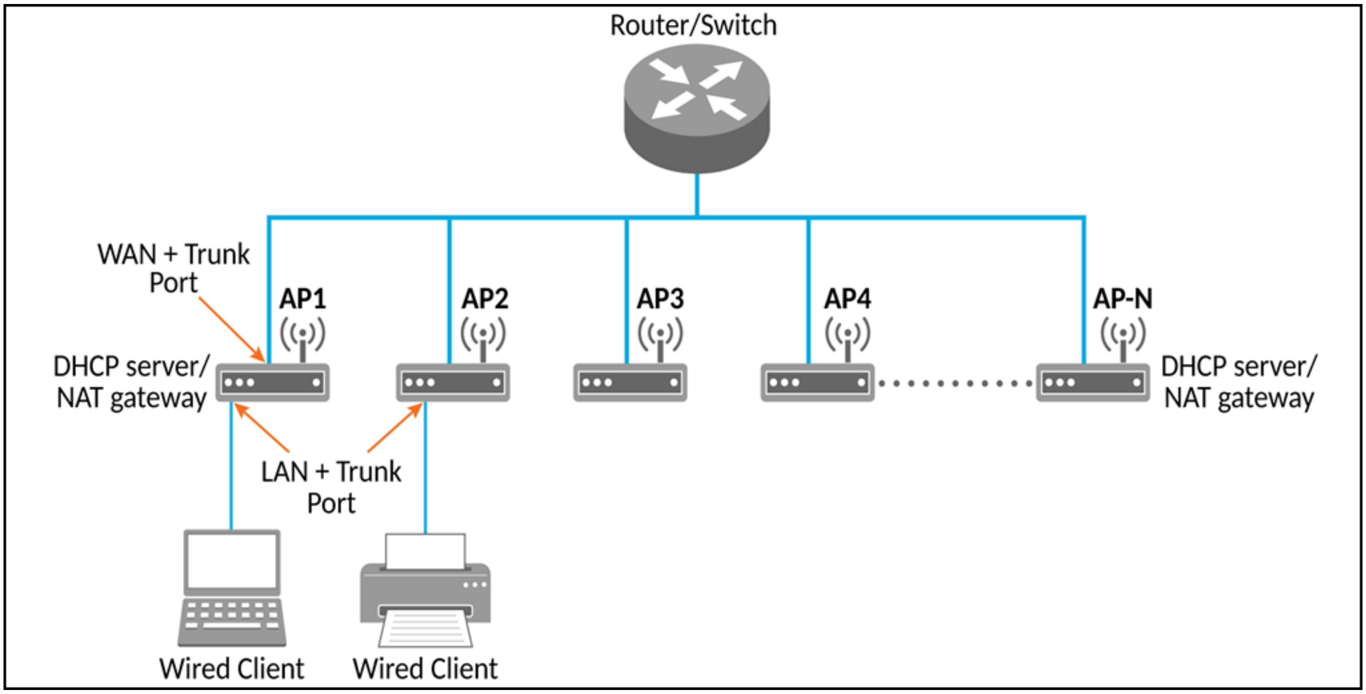
Access Points (APs) can be deployed in three types of topologies.

- Single AP Topology
- Multiple AP (Flat Network) Topology
- Hierarchical AP Topology

Single AP Topology

All the APs in the zone get their IP addresses from the WAN router and provides the DHCP or NAT service. For example,AP H510 or H320 is configured as GAP (Generation Application Protocol) as a manual port selection, then LAN1 and LAN2 configuration is pushed to Ethernet1 and Ethernet2 ports of the APs instead of Ethernet0 and Ethernet1 ports.

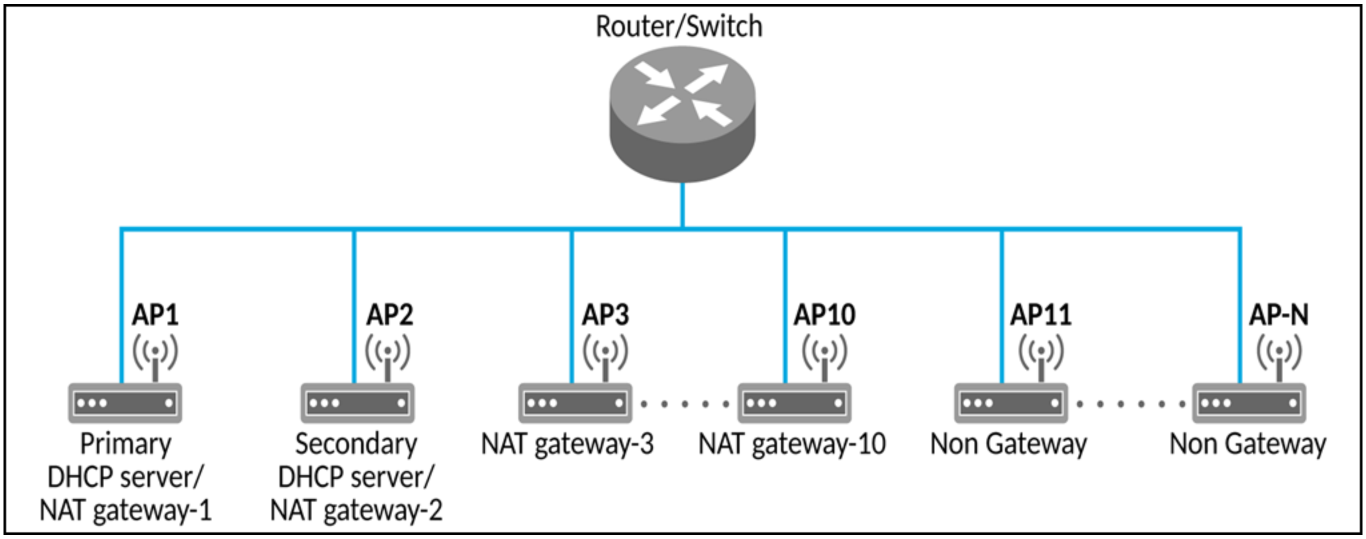
FIGURE 7 Single AP Topology



Multiple AP (Flat Network) Topology

All the APs in the zone get their IP address from the WAN router and designated APs provide the DHCP or NAT service. A maximum of two APs is selected for DHCP service (primary and secondary) and ten APs for NAT Gateway.

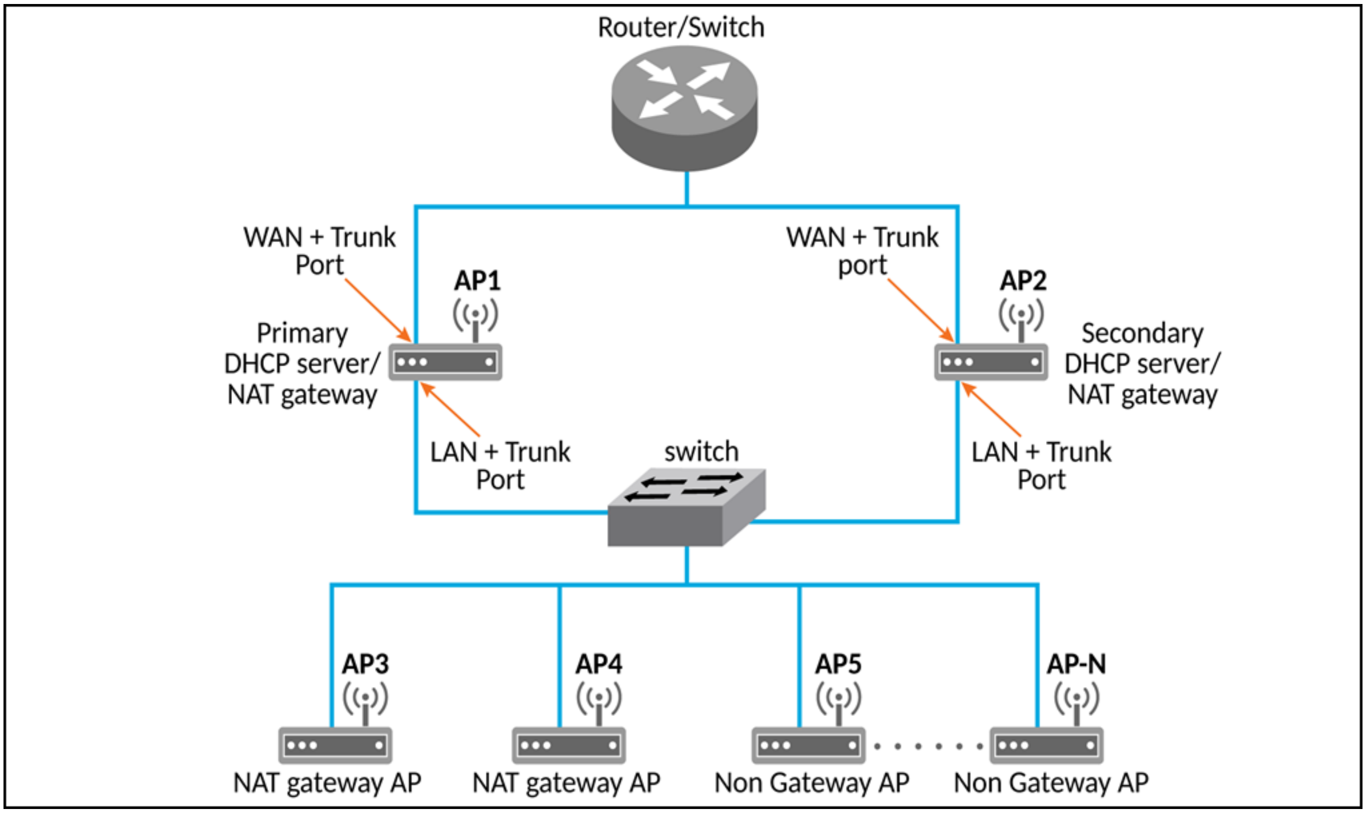
FIGURE 8 Multiple AP (Flat Network) Topology



Hierarchical AP Topology

Designated APs provide the DHCP or NAT service. Gateway APs get the IP address from the WAN router and non-gateway APs get the IP address from the Gateway APs. For example, AP H510 or H320 is configured as GAP by manual port selection, then LAN1 and LAN2 configuration is pushed of the APs to Ethernet1 and Ethernet2 ports instead of Ethernet0 and Ethernet1 ports. If Ethernet0 port needs to be configured, then LAN5 or LAN3 ports need to be configured.

FIGURE 9 Hierarchical AP Topology



Hierarchical Network Topology

Hierarchical network topology along with DHCP or NAT runs on single and multiple APs.

Gateway APs are directly connected to the service providers' router or switch to get the public IP addresses. The Non-Gateway APs (NGAP) gets the private IP addresses from the Gateway APs (GAP) through the DHCP or NAT service. Wired client such as printers and laptops are directly connected to the LAN port of the GAP or WAN ports of NGAP and are operational without the external DHCP or NAT. Basic Mesh topology is supported where GAP is the root AP and all other NGAPs are Mesh APs.

The Dynamic WAN Port Detection (DWPD) algorithm detects the WAN port among Ethernet0/Ethernet1/Ethernet2 of the APs, and marks only one port of the AP as WAN. LAN port selection is based on the availability of wired port with tunnel enabled. All other wired ports on the AP are marked as LAN.

Expected behavior of a three port APs are as follows:

- Ethernet0: Connected to WAN

  Result after DWPD: Ethernet0=WAN, Ethernet1=LAN, Ethernet2=WAN
- Ethernet1: Connected to WAN

  Result after DWPD: Ethernet0=LAN, Ethernet1=WAN, ETH2=WAN
- Ethernet2: Connected to WAN

  Result after DWPD: Ethernet0=LAN, Ethernet1=WAN, Ethernet2=WAN

Using DWPD a user can plug-n-play without configuring WAN or LAN ports. Wired client connectivity for each AP is possible where all the APs in the zone run DHCP or NAT service. All Ethernet ports can be configured as LAN ports allowing wired clients to connect.

LAN port profile enables APs with multiple Ethernet ports to be configured as LAN ports and a separate switch is not required if the multi-port AP is a GAPs. All the required wired and NGAPs are connected directly to the number of available Ethernet ports.

While using DHCP NAT-HN (Network Address Translation) with DWPD, the AP ignores the Ethernet port configuration, which is pushed from the interface. The AP selects the WAN and LAN ports, dynamically and on detecting the WAN port successfully, it marks the other port as a LAN port. When it marks an Ethernet port as a LAN port, the DWPD chooses the untagged VLAN ID as one (1) by default.

> **NOTE**
> The LAN port configuration cannot be changed.

Wired client gets the IP address from DHCP Pool VLAN ID 1. To configure Ethernet port VLAN ID to 100 through the interface, manually select WAN port and apply the appropriate Ethernet port profile to Ethernet0 and Ethernet1 ports of the AP.

> **NOTE**
> If APs or clients connected to a LAN switch come before the DWPD process completes on the GAPs, the clients or NGAPs get the IP addresses from WAN VLANS (the default VLAN or non-default VLAN, which is part of WAN).

Configuring AP-based DHCP Service Settings

Using DHCP service settings, configure an AP to assign private IP addresses to Wi-Fi clients and wired clients without the need for a separate DHCP server (router).

Before you configure the DHCP Service, consider the following:

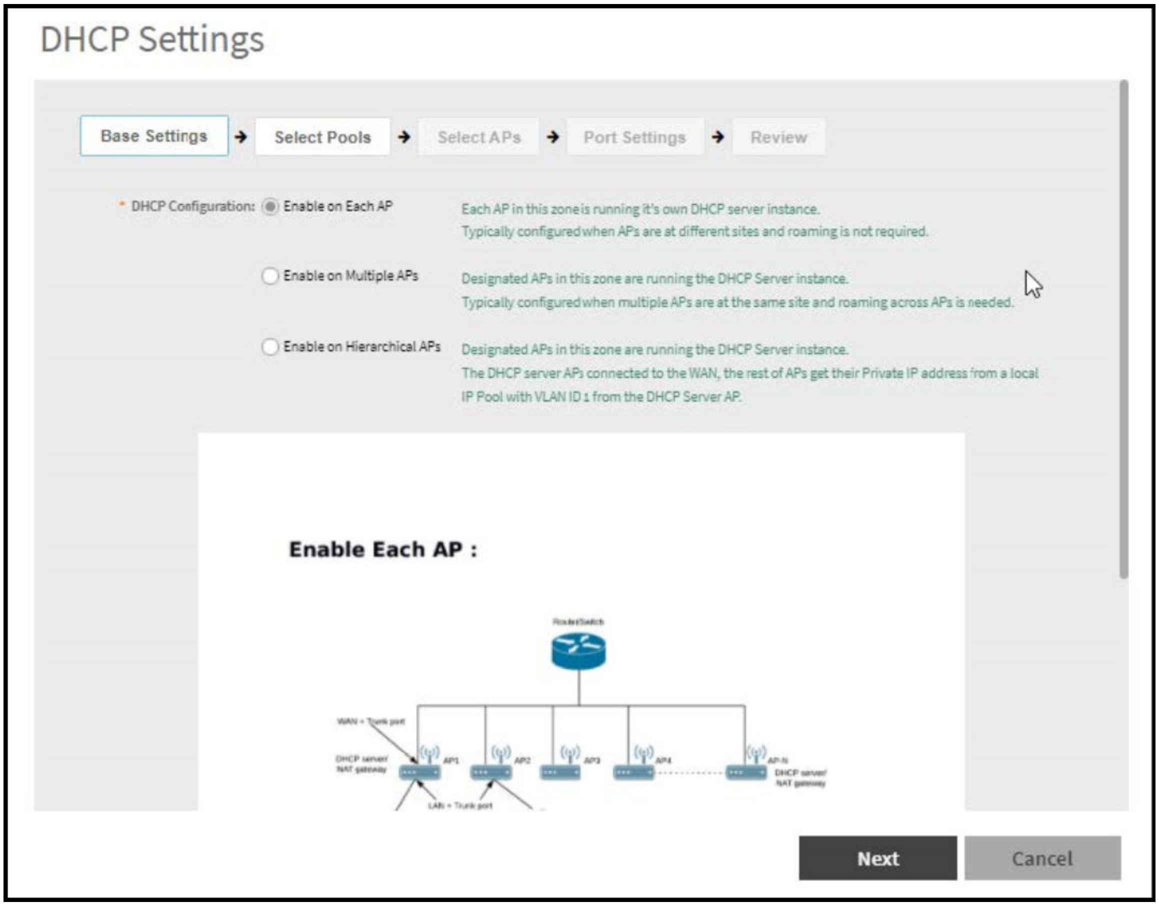
- There must be a minimum of one and a maximum of 10 APs acting as Gateway AP (GAP) based on the topology when configuring DHCP server and NAT router. There is no count on the number of APs acting as Non-Gateway APs (NGAP).
- For a single NGAP, connect Ethernet0 of NGAP to LAN port (usually Ethernet1) of GAP.
- For more than one NGAP, Layer2 switch is required to connect the LAN port of GAPs to all the NGAPs.
- For APs having more than two Ethernet ports, all the Ethernet ports except the WAN backhaul (usually Ethernet0) is configured as LAN ports. In such cases, a separate switch is not required.

To configure DHCP services:

1. From the main menu go to **Services** > **DHCP** > **DHCP Setting (AP)**.

2. Select a Zone from the zone list on the left side of the screen, and click **Enable DHCP Service**.

FIGURE 10 DHCP Settings Wizard



DHCP Settings

* DHCP Configuration:

● Enable on Each AP — Each AP in this zone is running it's own DHCP server instance. Typically configured when APs are at different sites and roaming is not required.

○ Enable on Multiple APs — Designated APs in this zone are running the DHCP Server instance. Typically configured when multiple APs are at the same site and roaming across APs is needed.

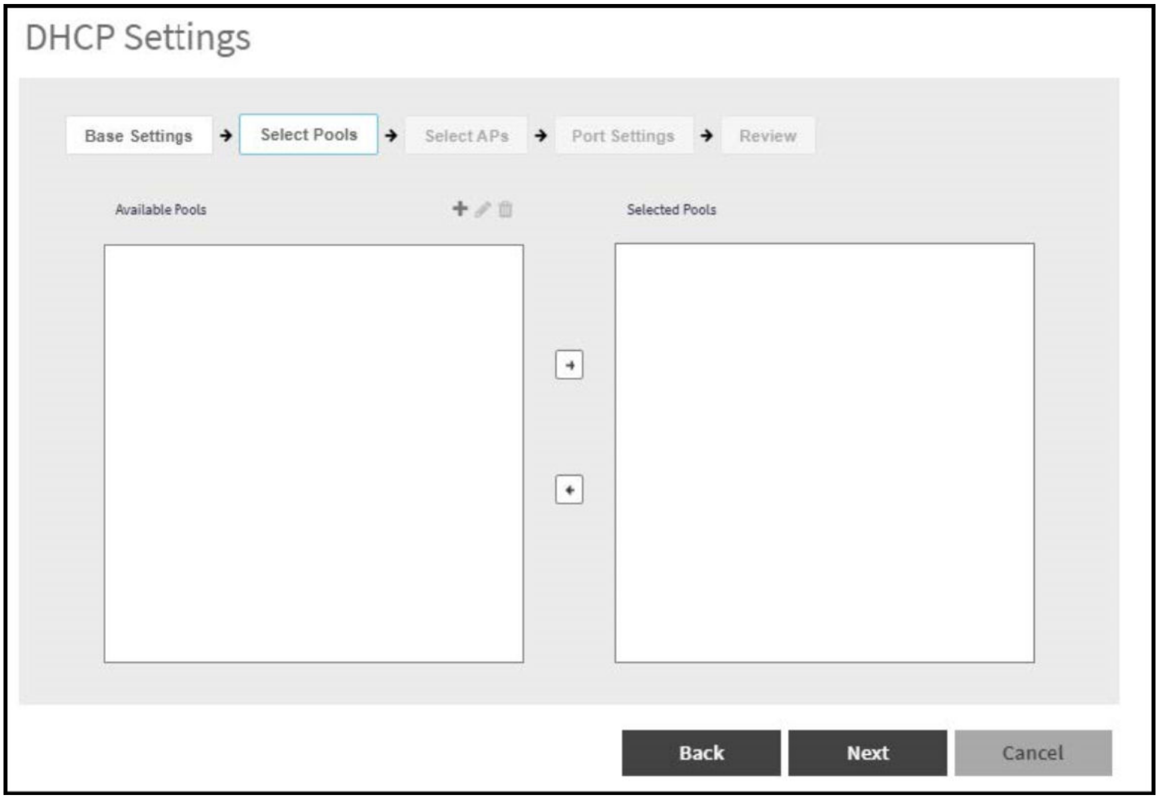
○ Enable on Hierarchical APs — Designated APs in this zone are running the DHCP Server instance. The DHCP server APs connected to the WAN, the rest of APs get their Private IP address from a local IP Pool with VLAN ID 1 from the DHCP Server AP.

3. On the first page of the wizard (**Base Settings**), configure the **DHCP Configuration** as follows:
   - **Enable on Each AP**: Each AP in this zone gets the IP address from the WAN router and runs its own DHCP server instance. This option is typically used when APs are at different sites and roaming is not required.
   - **Enable on Multiple APs**: Designate, which APs provide DHCP or NAT service. This option is typically used when multiple APs are at the same site and roaming is required. This option also allows whether to automatically or manually specify which APs provide DHCP service.
   - **Enable on Hierarchical APs**: Designate, which APs provide DHCP or NAT service. The DHCP server connects to the WAN AP and the other APs get their private IP address from the local IP address pool with VLAN ID 1 from the DHCP server AP.
4. Click **Next**.

5. On the next wizard screen, (**Select Pools**), select up to four DHCP pools to assign client IP addresses.

   NOTE
   For the **Enable on Hierarchical APs** DHCP configuration, one of the pools must be VLAN ID 1.

FIGURE 11 Selecting Pools



   NOTE

   If DHCP pools are not created, it can be done from the wizard. Click the Plus + icon and configure the IP address pool as described in the Creating an AP DHCP Pool on page 29.

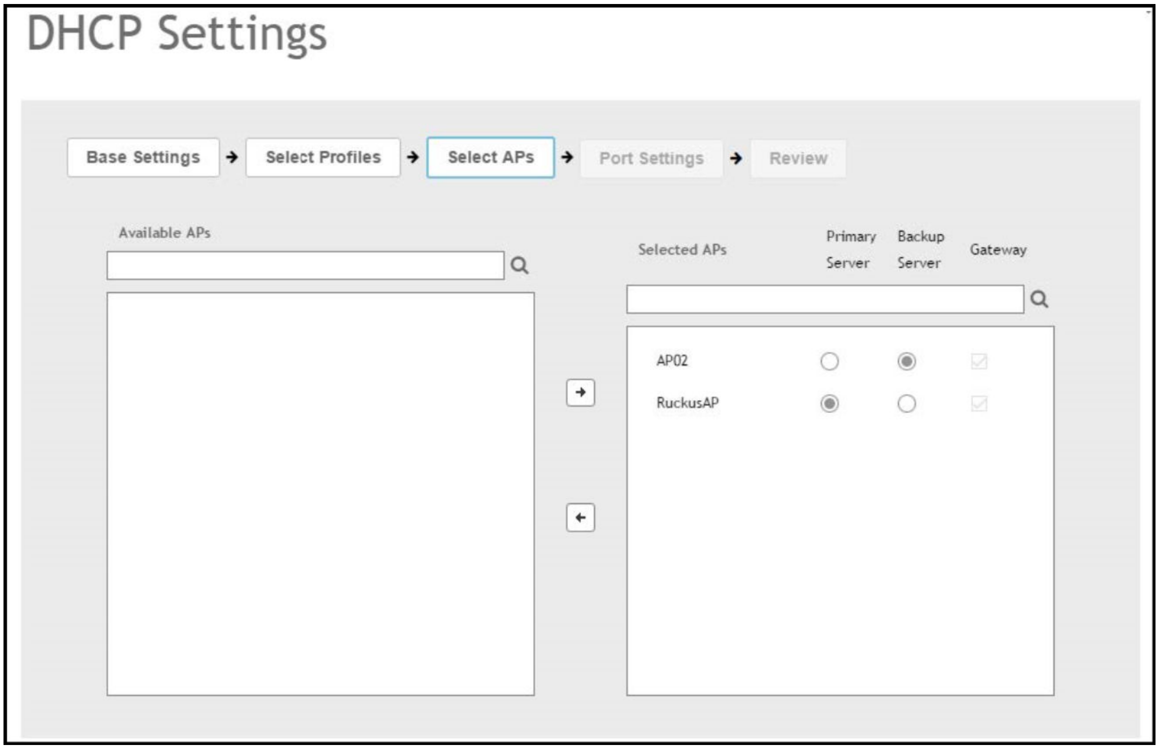
6. Click **Next**. The **Select APs** screen appears.

   NOTE
   If **Auto Select AP** is selected on the first wizard screen, this configuration screen is skipped.

7. On the **Select APs** wizard screen, select the APs specific to the base DHCP settings.

   NOTE
   For the **Enable on Multiple APs** DHCP configuration, select a maximum of two APs for DHCP service (primary and secondary) and a maximum of 10 APs for NAT Gateway.

FIGURE 12 Selecting APs



Selected APs	Primary Server	Backup Server	Gateway
AP02	○	●	☑
RuckusAP	●	○	☑

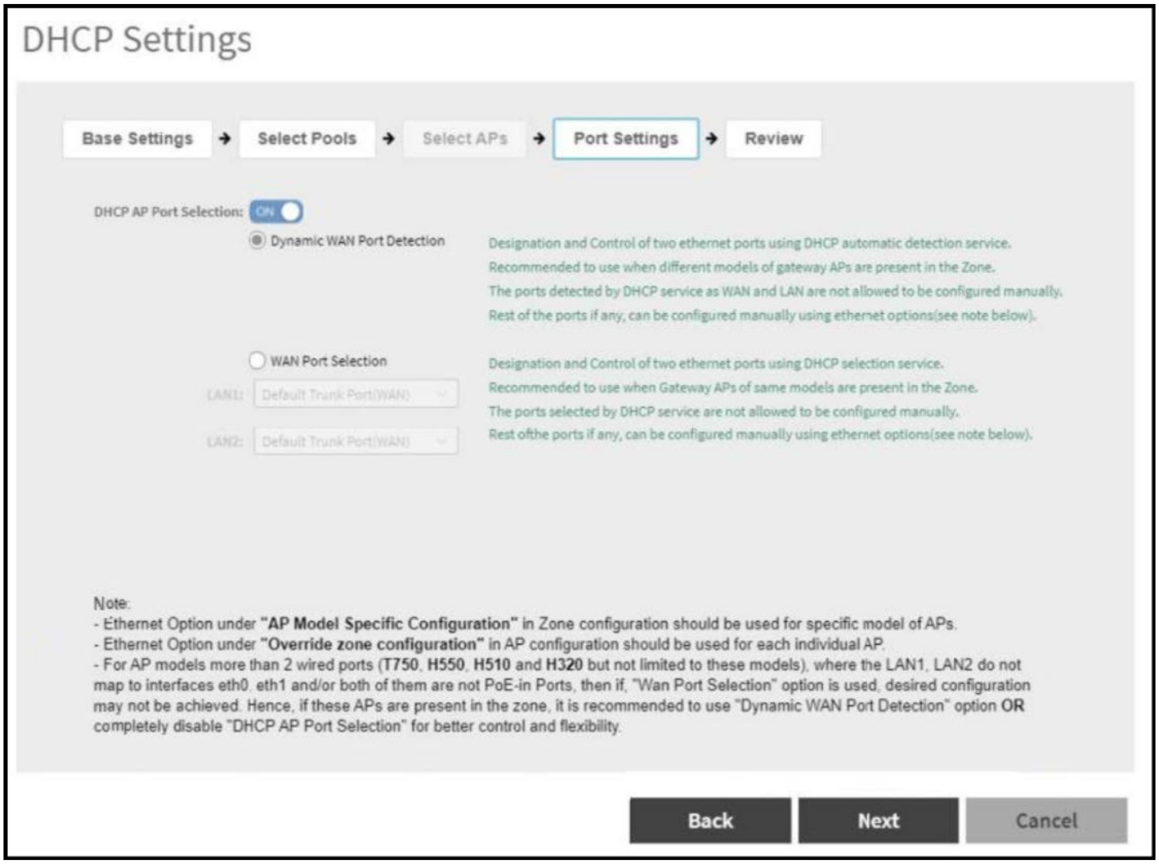
8. Click **Next**. The **Port Settings** screen is displayed.

9. On the **Port Settings** wizard screen, click **DHCP AP Port Selection** to configure the port settings for **Enable on Each AP** and **Enable on Hierarchical APs** options. Configure the following:

   NOTE
   It is recommended to use **Dynamic WAN Port Detection** option or disable **DHCP AP Port Selection** for AP models with more than two wired ports, where LAN1 and LAN2 do not map to Ethernet0 and Ethernet1 interfaces respectively, and where both are not PoE in ports.

   - **Dynamic WAN Port Detection**(DWPD): By default, WAN is identified, LAN selected and the non-DWPD ports are configured. It is recommended to use this option when different models of gateway APs are present in the zone. The ports detected by DHCP service as WAN and LAN cannot be configured manually. Remaining ports, if any, can be configured as follows:
     - For specific models of APs, use the Ethernet option in **AP Model Specific Configuration**. Refer to **Configuring Access Points** in *RUCKUS SmartZone AP Management Guide*.
     - For each individual AP, use the Ethernet option in **Override zone configuration**Refer to **Configuring Access Points** in *RUCKUS SmartZone AP Management Guide*.
   - **WAN Port Selection**: Manually assign port to WAN and LAN. This setting overrides the original port configuration of a zone. It is recommended to use GAP of the same model are present in the zone. The ports selected by the DHCP service cannot be configured manually. Rest of the ports, if any, can be configured manually using Ethernet options. Select the **LAN1** and **LAN2** options from the drop-down. Remaining ports, if any, can be configured as follows:
     - For specific models of APs, use the Ethernet option in **AP Model Specific Configuration**. Refer to **Configuring Access Points** in *RUCKUS SmartZone AP Management Guide*.
     - For each individual AP, use the Ethernet option in **Override zone configuration**Refer to **Configuring Access Points** in *RUCKUS SmartZone AP Management Guide*.

FIGURE 13 Port Settings



DHCP AP Port Selection: ON

● Dynamic WAN Port Detection

Designation and Control of two ethernet ports using DHCP automatic detection service.
Recommended to use when different models of gateway APs are present in the Zone.
The ports detected by DHCP service as WAN and LAN are not allowed to be configured manually.
Rest of the ports if any, can be configured manually using ethernet options(see note below).

○ WAN Port Selection

LAN1: Default Trunk Port(WAN)

LAN2: Default Trunk Port(WAN)

Designation and Control of two ethernet ports using DHCP selection service.
Recommended to use when Gateway APs of same models are present in the Zone.
The ports selected by DHCP service are not allowed to be configured manually.
Rest ofthe ports if any, can be configured manually using ethernet options(see note below).

Note:
- Ethernet Option under **"AP Model Specific Configuration"** in Zone configuration should be used for specific model of APs.
- Ethernet Option under **"Override zone configuration"** in AP configuration should be used for each individual AP.
- For AP models more than 2 wired ports (**T750**, **H550**, **H510** and **H320** but not limited to these models), where the LAN1, LAN2 do not map to interfaces eth0, eth1 and/or both of them are not PoE-in Ports, then if, "Wan Port Selection" option is used, desired configuration may not be achieved. Hence, if these APs are present in the zone, it is recommended to use "Dynamic WAN Port Detection" option **OR** completely disable "DHCP AP Port Selection" for better control and flexibility.

10. Click **Next**.
11. On the **Review** screen, review the settings to make sure everything is correct. Once you are satisfied with your settings, click **OK** to confirm.

You have configured the DHCP server settings and applied them to an AP (or multiple APs). These APs will now provide DHCP or NAT functionality and assign IP addresses to wireless clients from the DHCP address pools specified.

Creating an AP DHCP Pool

Creating a DHCP pool is necessary for assigning IP addresses to clients. Multiple address pools can be created and assigned to APs that are running DHCP services. When a client is then connected to the wireless network, it assigns an IP address from the DHCP pool(s) as specified.

Follow the steps below to configure a DHCP pool for an IP address allocation:

1. From the main menu go to **Services** > **DHCP** > **DHCP Pools (AP)**.
2. Select the zone to create the pool.
3. Click **Create**.

   The **Create DHCP Pool** page appears.

4. Configure the following:
   - **Name**: Type a name for the pool you want to create.
   - **Description**: Type a description of the pool you want to create.
   - **VLAN ID**: Type the VLAN ID for the pool.
   - **Subnet Network Address**: Type the IP subnet network address (for example, 192.168.0.0).
   - **Subnet Mask**: Type the subnet mask IP address (for example, 255.255.255.0).
   - **Pool Start Address**: Type the first IP address to be allocated to clients from the pool (for example, 192.168.0.1).
   - **Pool End Address**: Type the last IP address to be allocated to clients from the pool (for example, 192.168.0.253).
   - **Primary DNS IP**: Type the primary DNS server IP address.
   - **Secondary DNS IP**: Type the secondary DNS server IP address.
   - **Lease Time**: Enter the IP address lease time, after which clients will have to renew or request new IP addresses.
5. Click **OK**.

You have created a DHCP address pool. You can now apply this address pool to a DHCP service, as described in Configuring AP-based DHCP Service Settings on page 24.

> **NOTE**
> You can also edit, clone and delete the address pool by selecting the options **Configure**, **Clone** and **Delete** respectively, from the **Pool** tab.

Creating Profile-based DHCP

DHCP profile is configured and accessed through Virtual SmartZone Data Plane (vSZ-D). The vSZ-D server assigns the IP address to the user equipment based on the profile rule. Different pools with the same subnet are created without overlapping the IP address range.

You must configure the following settings to create a DHCP profile.

> **NOTE**
> DHCP supports only access-side network.

- Configuring DHCP Global Settings on page 30
- Configuring DHCP Pool Settings on page 31

Configuring DHCP Global Settings

A DHCP profile can be used simultaneously by multiple segments and gateways in the network.

To configure Profile-based DHCP Global settings follow these steps:

1. In the controller virtual platform web interface go to **Services** > **DHCP & NAT** > **DHCP Profiles (DP)**.
2. Click **Create**. The **Create DHCP Profile** page is displayed.

3. Configure the following:
   - **Profile Name**: Type a name for the DHCP profile. AP supports 32 bytes.
   - **Description**: Type a description of the settings.
   - **Domain Name**: Type the domain name.
   - **Primary DNS Server**: Type the primary domain name server address.
   - **Secondary DNS Server**: Type the secondary domain name server address.
   - **Lease Time**: Type the duration in Hours, Minutes and Seconds. Range: 1 through 86400 seconds.
   - **DHCP Option43 Space**: Click **Create**. The **Create DHCP Option43 Space** is displayed. Configure the following:
     - **Space Name**: Type a name for Option43 space.
     - **Description**: Type a description for Option43 space.
     - Under **Option43 Sub Option**, click **Create** and configure the following:
       - **Sub Option Name**: Type a sub option name.
       - **Type**: Select the required option from the drop-down.
       - **Code**: Enter a code. Range: 1 through 254.
       - Click **OK**. You have created Option43 Sub Option.
     - Click **OK**. You have created Option43 Space.
   - **Hosts**: Click **Create**. The **Create Host Configuration** form is displayed. Configure the following:
     - **General Options**
       - **Host**: Type a name for the host settings that you want to create.
       - **Description**: Type a description for the host settings that you want to create.
     - **Policy Options**
       - **MAC Address**: Type the MAC address of the DHCP host.
     - **Assigning Options**
       - **Broadcast Address**: Type the broadcast IP address.
       - **Fixed Address**: Type the fixed IP address of the host.
       - **Gateway**: Type the gateway IP address.
       - **DNS Server**: Type the IP address of the DNS server.
       - **Domain Name**: Type the domain name.
       - **Host Name**: Type the host name.
       - **Lease Time**: Type the duration in Hours, Minutes and Seconds. Range: 1 through 86400 seconds.
     - Click **OK**. You have created **DHCP Host** configuration.
4. Click **OK**.

   You have created DHCP Profile settings.

Configuring DHCP Pool Settings

For any *DHCP pool*, you can *configure* a primary subnet and any number of secondary subnets.

To configure DHCP pool settings follow these steps:

1. In the controller virtual platform web interface go to **Services** > **DHCP & NAT** > **DHCP Profiles (DP)**.
2. Select the DHCP profile from the list to configure the pool settings.
3. Select the **Pools** tab page.

4. Click Create and configure the following:
   - **General Options**
     - **Pool Name**: Type a name for the pool configuration.
     - **Description**: Type a description for the pool configuration.
   - **Policy Options**
     - **Policy Type**: Select **VLAN** or **VNI** option.

       NOTE
       For policy type:

       - Either VLAN range or QinQ VLAN must be configured.
       - QinQ VLAN cannot be configured when VLAN range is 1.
       - Combination of VLAN range and QinQ VLAN should be unique among DHCP pools in DHCP profile.
     - **VLAN Range**: Type the VLAN range. Range: 1, 2 through 4095. For example: 1, 2 or 2-3.
     - **QinQ VLAN**: Select the check box and update the following:

       NOTE
       This feature is supported only in vSZ-H platform.

       - **QinQ SVLAN Range**: Type a SVLAN range. Range: 2 through 4095.
       - **QinQ CVLAN Range**: Type a CVLAN range. Range: 2 through 4095.
   - **Assigning Options**
     - **Subnet**: Type the IP address.
     - **Subnet Mask**: Type the network IP address.
     - **Broadcast Address**: Type the broadcast IP address.
     - **Pool Range**: Type the IP address range for the pool.
     - **Exclude Pool**: Type the IP address range that must be excluded.
     - **Primary Gateway**: Type the primary gateway IP address.
     - **Secondary Gateway**: Type the secondary gateway IP address.
     - **Primary DNS Server**: Type the IP address of the primary DNS server.
     - **Secondary DNS Server**: Type the IP address of the secondary DNS server.
     - **Domain Name**: Type the domain name.
     - **Host Name**: Type the host name.
     - **Lease Time**: Type the duration in Hours, Minutes and Seconds. Range: 1 through 86400 seconds.
   - **Option43 Value**
     - Click **Create**. The **Create Option43 Value** form is displayed. Configure the following:
       - Choose the **Space Name** or click **Create** to add the Option 43 Space name.
       - Type a **Description**.
     - Click **OK**. You have configured **Option43 Value**.
5. Click **OK**.

   You have created DHCP pool configuration.

Creating Profile-based NAT

A NAT router profile is configured and accessed through Virtual SmartZone Data Plane (vSZ-D).

The NAT server settings work independently. You must configure the following settings to create a NAT profile.

NOTE

NAT does not support multiple public subnet/VLAN.

- Configuring NAT Global Settings on page 33
- Configuring NAT Pool Setting on page 33

Configuring NAT Global Settings

Network Address Translation (NAT) is a process in which one or more local IP address is translated into one or more Global IP address and vice versa in order to provide Internet access to the local hosts.

To create a NAT global setting follow these steps:

1. In the controller virtual platform web interface go to **Services** > **DHCP & NAT** > **NAT Profiles (DP)**.
2. Click **Create**. The **Create NAT Profile** page is displayed.
3. Configure the following:
   - **Profile Name**: Type a name for the NAT profile that you want to create. AP supports 32 bytes.
   - **Description**: Type a description for the profile that you want to create.
   - **Subnet**: Type the IP address.
   - **Prefix**: Type a prefix value. Maximum range: 31.
   - **Public VLAN**: Type the VLAN range. Range: 2 through 4095.
   - **Gateway**: Type the gateway IP address.
4. Click **OK**.

   You have created a NAT Profile.

Configuring NAT Pool Setting

To configure NAT pool settings follow these steps.

1. In the controller virtual platform web interface go to **Services** > **DHCP & NAT** > **NAT Profiles (DP)**.
2. Select the NAT profile from the list and click the **Pools** tab.
3. Click **Create**. The **Create Pool Configuration** page is displayed.

4. Configure the following:
   - **General Options**
     - **Pool Name**: Type a name for the NAT pool settings that you want to create.
     - **Description**: Type a description for the pool settings that you want to create.
   - **Policy Options**
     - **Policy Type**: Select **VLAN** or **VNI** option.

       NOTE
       For policy type choose one of the following:

       - Update the VLAN range.
       - Update the QinQ VLAN range.
       - Leave both the fields blank for RADIUS NAT server setup.

     - **Private VLAN Range**: Type the VLAN range and click **Add**. Range: 1 through 4095. For example: 1 or 1-2.
     - **Private QinQ VLAN Range**: Type **SVLAN** range, **CVLAN** range and click **Add**. Range: 2 through 4095. For example: 2 or 2-3.

       NOTE
       This feature is supported only in vSZ-H platform.

   - **Translation Options**
     - **Port Range**: Type the port range. Range: 10000 through 65534. For example: 10000-20000.
     - **Public Address Range**: Type the public IP address range.

       NOTE
       This public address must not be a duplicate of the other public addresses in the same subnet, which includes applied NAT profile and vSZ-D's *Access and Core Interface Address*.

5. Click **OK**.

   You have created a NAT pool setting.

Configuring DHCP Server or NAT Router with Mesh Options

DHCP or NAT functionality on controller managed APs and DPs (data planes) allows customers to reduce costs and complexity by removing the need for DHCP server or NAT router to provide IP addresses to clients.

To configure DHCP or NAT with mesh option follow these steps.

1. To configure DHCP or NAT with mesh enable the Mesh option at the Zone level. Refer to the section *Mesh Options* in *RUCKUS SmartZone AP Management Guide*.
2. From the Access Points page, select the AP to be assigned as the root AP.
3. Click **Configure**.
4. Select the Mesh specific options and the root AP mode.
5. Create multiple address pools and assign it to the APs, which are on DHCP services. Refer to Creating an AP DHCP Pool on page 29.
6. From the Services page, enable DHCP on the zone.
7. Edit the DHCP Service on the AP by selecting the required VLANs and APs as Gateway APs. Refer, Configuring AP-based DHCP Service Settings on page 24.

Location Services

If your organization purchased the RUCKUS Smart Positioning Technology (SPoT) location service, the controller must be configured with the venue information that is displayed in the SPoT Administration Portal.

After completing purchase of the SPoT location service, you will be given account login information that you can use to log in to the SPoT Administration Portal. The SPot Administration Portal provides tools for configuring and managing all of your venues (the physical locations in which SPoT service is deployed). After a venue is successfully set up, you must enter the same venue information in the controller.

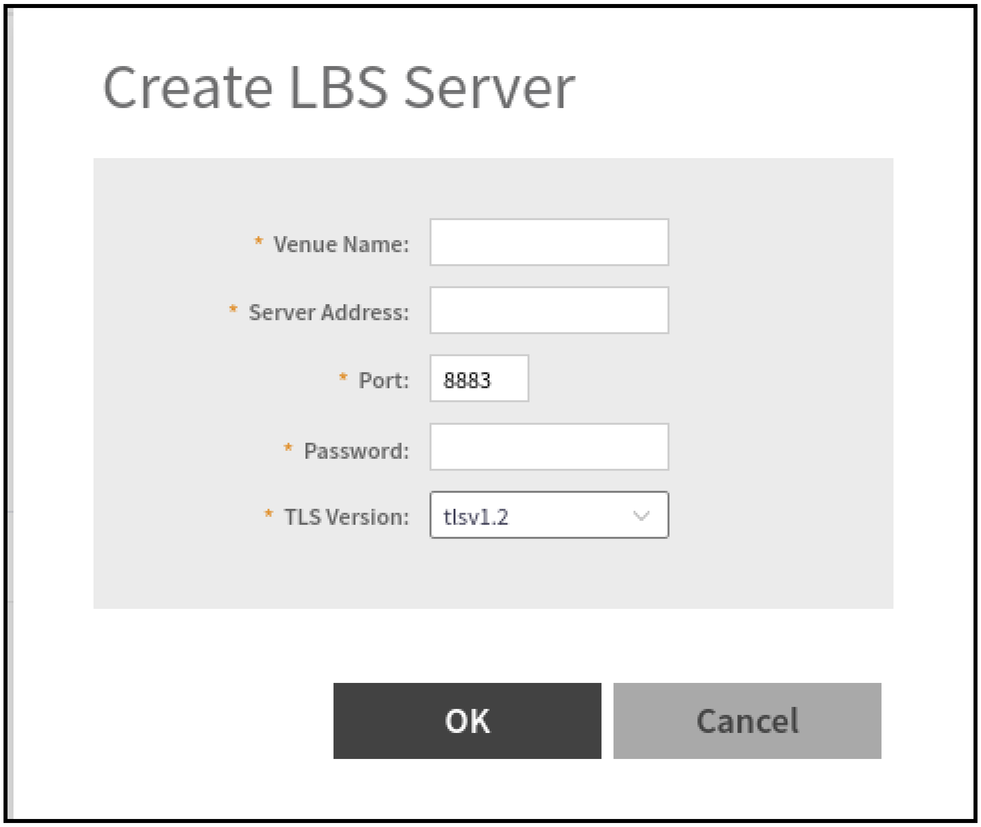
1. From the main menu, go to **Administration** > **External Services** > **Ruckus Service** > **Ruckus Location Services (SPoT)**.

   The **Ruckus Location Services (SPoT)** tab is displayed.

2. Click **Create**.

   The **Create LBS Server** dialog box is displayed.

   FIGURE 14 Creating a Location-Based Server



Create LBS Server

* Venue Name:	
* Server Address:	
* Port:	8883
* Password:	
* TLS Version:	tlsv1.2

3. In the **Venue Name** field, type the venue name for the server.
4. In the **Server Address** field, type the server IP address.

   NOTE
   The server address must be entered in IPv4 address format. The LBS server does not support configuration of IPv6 addresses.

5. In the **Port** field, type the port number to communicate with the server.

   NOTE
   The default port number is 8883.

6. In the **Password** field, type the password to access the server.
7. From the **TLS Version** list, select the TLS version.
8. Click **OK**.

   NOTE
   You can also edit, clone, and delete the location-based services by selecting the **Configure**,**Clone**, and **Delete** options respectively from the **Ruckus Location Services (SPoT)** tab.

   NOTE
   The connection between the controller and vSPoT is an outbound connection, so it depends on the destination IP address. If the destination IP address falls in the subnet of one interface, it is routed to that interface. Otherwise, it is routed through the default route.

Working with Tunnels and Ports

Creating a RUCKUS GRE Profile

Generic Routing Encapsulation (GRE) provides a way to encapsulate arbitrary packets (payload packet) inside of a transport protocol, and transmit them from one tunnel endpoint to another. You can configure the RUCKUS GRE tunnel profile of the controller to manage AP traffic.

To create a GRE profile follow the below steps.

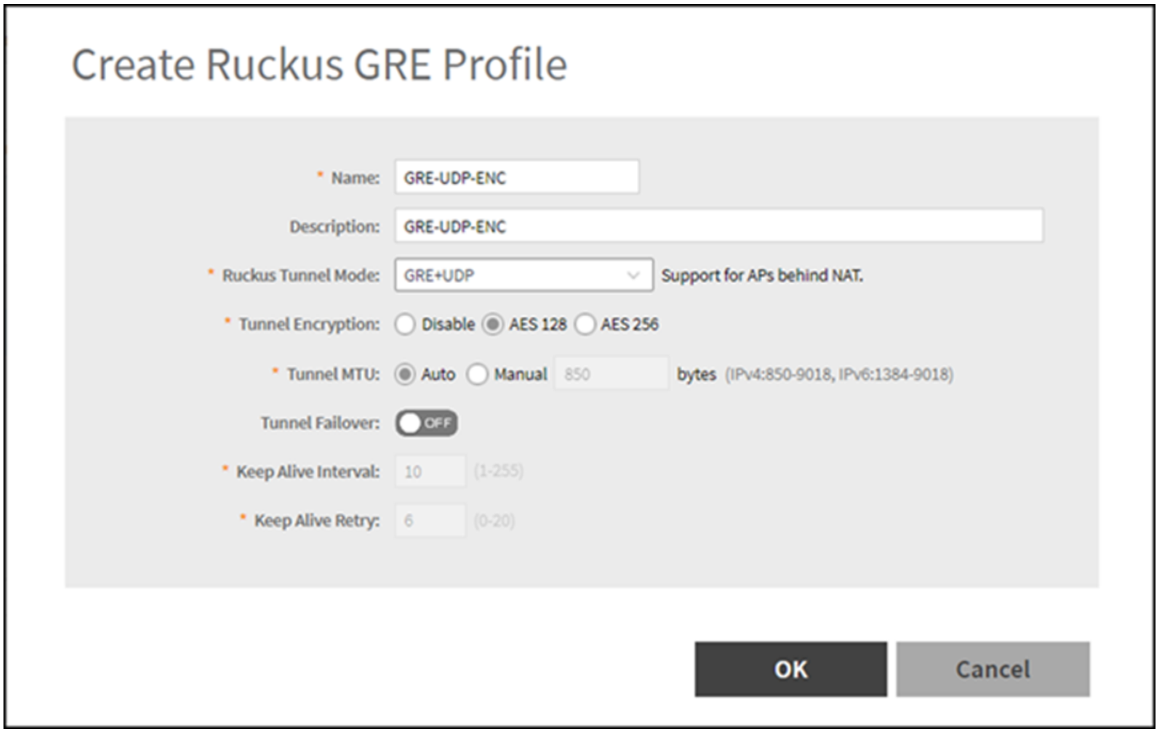
NOTE
You can also edit, clone and delete the profile by selecting the options **Configure**, **Clone** and **Delete** respectively, from the **Ruckus GRE** tab.

1. From the main menu go to **Services** > **Tunnels & Ports**.
2. Select the **Ruckus GRE** tab, and select the system to create the profile.

3. Click **Create**.

   The **Create Ruckus GRE Profile** page is displayed.

   FIGURE 15 Creating a Ruckus GRE Profile



Create Ruckus GRE Profile

* Name: GRE-UDP-ENC

Description: GRE-UDP-ENC

* Ruckus Tunnel Mode: GRE+UDP Support for APs behind NAT.

* Tunnel Encryption: ○ Disable ● AES 128 ○ AES 256

* Tunnel MTU: ● Auto ○ Manual 850 bytes (IPv4:850-9018, IPv6:1384-9018)

Tunnel Failover: OFF

* Keep Alive Interval: 10 (1-255)

* Keep Alive Retry: 6 (0-20)

4. Type a name for the profile in the **Name** box.
5. Type a description for the profile in the **Description** box.
6. Select a protocol to use for tunneling WLAN traffic back to the data plane by choosing one of the following after clicking the drop-down arrow in the **Ruckus Tunnel Mode** box:
   - **GRE + UDP**—Select this option to allow APs behind a NAT server to tunnel WLAN traffic back to the data plane.
   - **GRE**—Select this option to tunnel regular WLAN traffic only.
7. To allow managed APs to decrypt 802.11 packets, and then use an AES encrypted tunnel to send them to the data plane. Select one of the **Tunnel Encryption** options:
   - Click the **Disable** radio button to allow only the management traffic to be encrypted; data traffic is unencrypted. This is the default option.
   - Click the **AES 128** radio button to use an AES 128-byte encryption tunnel.
   - Click the **AES 256** radio button to use an AES 256-byte encryption tunnel.

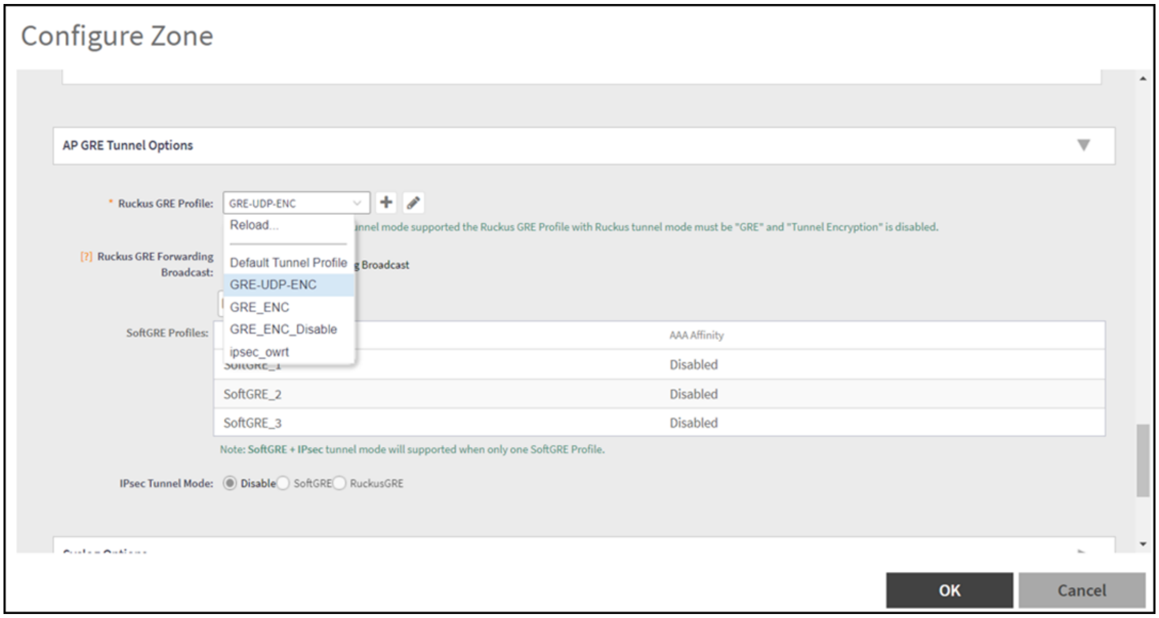
   MTU is the size of the largest protocol data unit that can be passed on the controller network.
8. Set the maximum transmission unit (MTU) for the tunnel using one of the **Tunnel MTU** options:
   - Click the **Auto** radio button. This is the default option.
   - Click the **Manual** radio button and enter the maximum number of bytes. For IPv4 traffic the range is from 850-1500 bytes, for IPv6 traffic the range is from 1384 to 1500 bytes.
9. Set the Tunnel failover option to either OFF or On. By default it is in OFF mode.

10. Enter the **Keep Alive Interval** value. By default the interval value is 10 and the range is between 1-255.
11. Enter the **Keep Alive Retry** value. By default the retry value is 06 and the range is between 0-20.
12. Click **OK**.

Using the created GRE profile in an AP Zone and WLAN

13. From the main menu go to **Network** > **Wireless** > **Access Points** > **Zone** profile to use the created GRE profile.
14. Select the GRE profile from the drop down list. Enable or disable the RUCKUS GRE forwarding broadcast. By default the option is turned OFF. Select the SoftGRE profiles and IPSec Tunnel Mode.

FIGURE 16 Applying the Ruckus GRE Profile



* Ruckus GRE Profile: GRE-UDP-ENC

…nnel mode supported the Ruckus GRE Profile with Ruckus tunnel mode must be "GRE" and "Tunnel Encryption" is disabled.

[?] Ruckus GRE Forwarding Broadcast: …g Broadcast

SoftGRE Profiles:

	AAA Affinity
SoftGRE_1	Disabled
SoftGRE_2	Disabled
SoftGRE_3	Disabled

Note: SoftGRE + IPsec tunnel mode will supported when only one SoftGRE Profile.

IPsec Tunnel Mode: ● Disable ○ SoftGRE ○ RuckusGRE

15. From the main menu go to **Network** > **Wireless LANs** > **WLAN** profile to use the created GRE profile.
16. Another option is navigate to the Zone level configuration and find **AP GRE Tunnel**.
17. Click + to create a new profile.
18. Go to the required WLAN to use the GRE profile.

Creating a Soft GRE Profile

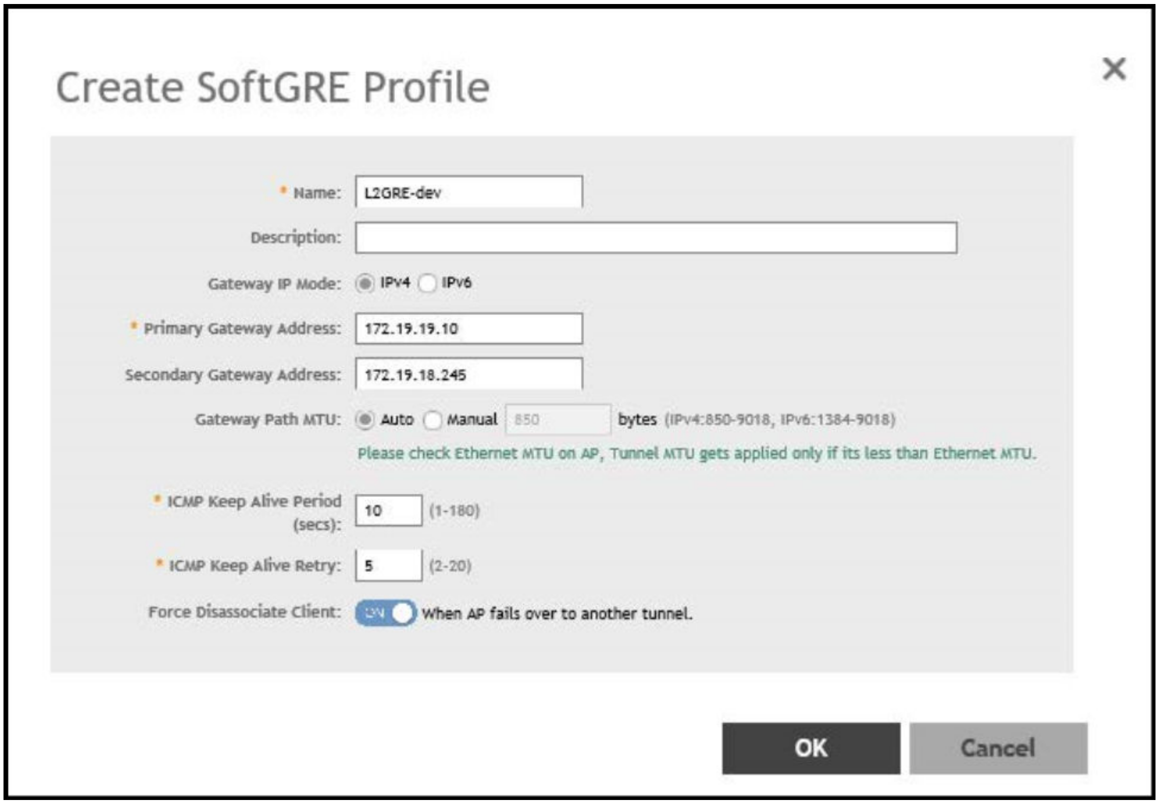
You can configure the Soft GRE tunnel profile of the controller to manage AP traffic.

1. From the main menu go to **Services** > **Tunnels and Ports**.

2. Select **SoftGRE** and click **Create**.

   The **Create SoftGRE Profile** page is displayed.

   FIGURE 17 Creating a SoftGRE Profile



Create SoftGRE Profile

* Name: L2GRE-dev
Description:
Gateway IP Mode: ● IPv4 ○ IPv6
* Primary Gateway Address: 172.19.19.10
Secondary Gateway Address: 172.19.18.245
Gateway Path MTU: ● Auto ○ Manual 850 bytes (IPv4:850-9018, IPv6:1384-9018)
Please check Ethernet MTU on AP, Tunnel MTU gets applied only if its less than Ethernet MTU.
* ICMP Keep Alive Period (secs): 10 (1-180)
* ICMP Keep Alive Retry: 5 (2-20)
Force Disassociate Client: ON When AP fails over to another tunnel.

3. Enter profile name and description.
4. Under **Gateway IP Mode**, select **IPv4** or **IPv6** addressing.
5. In the **Primary Gateway Address** field, enter the IP address or fully-qualified domain name (FQDN) of the primary gateway server.
6. In the **Secondary Gateway Address** field, enter the IP address or fully-qualified domain name (FQDN) of the secondary gateway server.

   NOTE
   If the controller is unable to reach the primary gateway server, the controller automatically attempts to reach the secondary gateway address at the IP address specified by you.

7. For **Gateway Path MTU**, set the maximum transmission unit (MTU) for the gateway path.

   Select one of the following options:

   - **Auto**: This is the default option.
   - **Manual**: The transmission range is from 850 through 1500 bytes.

8. In the **ICMP Keep Alive Period** field, enter the time interval in seconds.

   NOTE
   Time interval is the time taken by the APs to send a keep alive message to an active third party WLAN gateway. The range is from 1 through 180 seconds. The default value is 10 seconds.

9. In the **ICMP Keep Alive Retry** field, enter the number of keep alive attempts.

   NOTE
   Keep alive attempts are the number of attempts that the APs wait for a response from the active third party WLAN gateway before failing over to the standby WLAN gateway. The range is from 2 through 10 attempts. The default value is 5 attempts.

10. Under **Force Disassociate Client**, enable **Disassociate client when AP fails over to another tunnel** if you want to disassociate the client when AP fails over to another tunnel.

    NOTE
    You must select this option if you have enabled **AAA Affinity** while configuring the zone.

11. Click **OK**.

You have created the Soft GRE profile.

> **NOTE**
> You can also edit, clone, and delete the profile by selecting the options **Configure**, **Clone**, and **Delete** respectively from the **Soft GRE** tab.

Creating an IPsec Profile

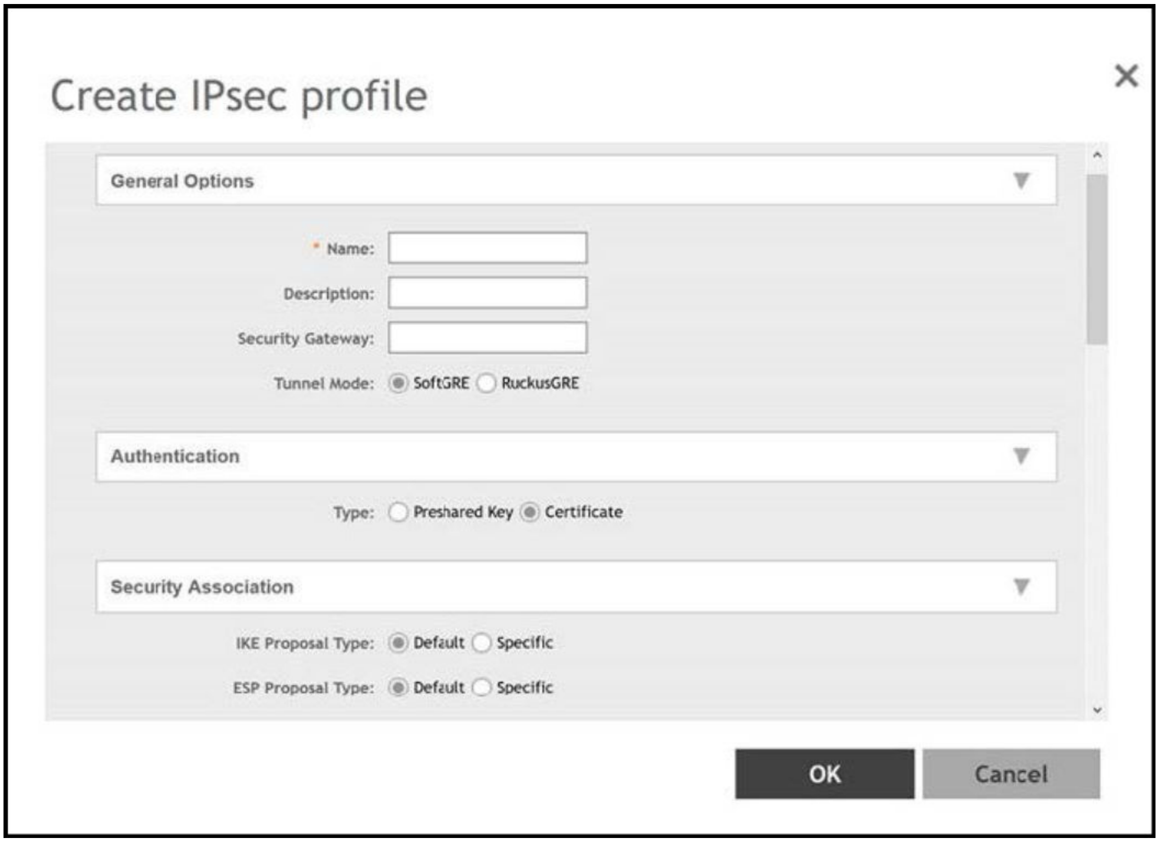
You can create an IPsec profile on 11ac and 11ax APs.

1. From the main menu, navigate to **Services** > **Tunnels & Ports**.
2. Select the **IPsec** tab, and then select the zone for which you want to create the profile.

3. Click **Create**.

   The **Create IPsec Profile** dialog box is displayed.

   FIGURE 18 Creating an IPsec Profile



Create IPsec profile

General Options

* Name:

Description:

Security Gateway:

Tunnel Mode: ● SoftGRE ○ RuckusGRE

Authentication

Type: ○ Preshared Key ● Certificate

Security Association

IKE Proposal Type: ● Default ○ Specific

ESP Proposal Type: ● Default ○ Specific

4. Under **General Options**, configure the following options:
   - **Name:** Enter a name for the profile.
   - **Description:** Enter a description for the profile.
   - **Security Gateway:** Enter the IP address or fully-qualified domain name (FQDN) of the IPsec server. If you use the IP address, the IP address format that you must enter will depend on the IP mode that is configured on the controller.
   - **Tunnel Mode:** Select **SoftGRE** or **RuckusGRE**.

     NOTE
     The **IP Mode** option is displayed only when **SoftGRE** is selected for **Tunnel Mode**.

   - **IP Mode:** Select **IPv4** or **IPv6**.
5. Under **Authentication**, configure the **Type** option.

   Select **Preshared Key** to use PSK for authentication or **Certificate** to use an X.509 certificate on the certificate authority (CA) or registration authority (RA) server. The controller uses the CMPv2 protocol to obtain the signed certificate from the **CA or RA** server. If you select **Preshared Key**, enter the **PSK**. The PSK must be 8 to 128 ASCII characters in length.

6. Under **Security Association**, configure the following options:
   - **IKE Proposal Type**: Select **Default** to use the default Internet Key Exchange (IKE) security association (SA) proposal type or select **Specific** to manually configure the IKE SA proposal. If you select **Specific**, you must configure the following settings:
     - **Encryption Algorithm:** Options include 3DES, AES128, AES192, and **AES256**.
     - **Integrity Algorithm:** Options include **MD5, SHA1, AES-XCBC, SHA256, SHA384**, and **SHA512**.
     - **Pseudo-Random Function:** Options include **Use integrity ALG, PRF-MD5, PRF-SHA1, PRF-AES-XCBC, PRF-AES-CMAC, PRF-SHA256,** and **PRF-SHA384**.
     - **DH Group:** Options for Diffie-Hellman (DH) groups for IKE include **modp768, modp1024, modp1536, modp2048, modp3072, modp4096, modp6144**, and **modp8192**.
   - **ESP Proposal Type:** Select **Default** to use the default Encapsulating Security Payload (ESP) SA proposal type or select **Specific** to manually configure the ESP proposal. If you select **Specific**, you must configure the following settings:
     - **Encryption Algorithm:** Options include **3DES, AES128, AES192, AES256**, and **NONE**.
     - **Integrity Algorithm:** Options include **MD5, SHA1, AES-XCBC, SHA256, SHA384**, and **SHA512**.
     - **DH Group:** Options for Diffie-Hellman (DH) groups for ESP include **None, modp768, modp1024, modp1536, modp2048, modp3072, modp4096, modp6144**, and **modp8192**.

     NOTE
     If you selected **RuckusGRE** for **Tunnel Mode**, the following IKE and ESP proposals are supported:

     - › AES128-SHA1-MODP2048
     - › AES256-SHA384-ECP384

       NOTE
       IKE encryption proposals should be greater than or equal to ESP encryption proposals. RuckusGRE over IPsec supports IKEv2 authentication by X.509 certificate only.

7. Under **Rekey Options**, configure the following options:
   - **Internet Key Exchange:** Select a time unit (day, hour, or minute) from the list, and enter a number to set the time interval at which the IKE key renews. Select the **Disable** check box to disable the IKE rekey.
   - **Encapsulating Security Payload:** Select a time unit (day, hour, or minute) from the list, and enter a number to set the time interval at which the ESP key renews. Select the **Disable** check box to disable the ESP rekey.
8. Under **Certificate Management Protocol**, configure the following options:
   - **DHCP Option 43 Sub Code for CA/RA Address:** Set the DHCP Option 43 subcode that will be used to discover the address of the CA or RA server on the network. The default subcode is 8.
   - **Server Path:** Enter the path to the X.509 certificate on the CA or RA server.
   - **DHCP Option 43 Sub Code for Subject Name of CA/RA**: Set the DHCP Option 43 subcode that will be used to discover the subject name of the CA or RA server on the network. The default subcode is 5.
   - **Subject Name of CA/RA:** Enter an ASCII string that represents the subject name of the CA or RA server.

9. Under **Advanced Options**, configure the following options:
   - **DHCP Option 43 Sub Code for Security Gateway**: Set the DHCP Option 43 subcode that will be used to discover the address of the security gateway on the network. The default subcode is 7.
   - **Retry Limit:** Set the number of times that the controller will attempt to discover the address of the security gateway. The default retry count is 5. Accepted values are 0 (disable) through 16.
   - **Replay Window:** Set the ESP replay window (in packets). The default size is 32 packets. Accepted values are 0 (disable) through 32 packets.
   - **IP Compression:** Click **Enable** to enable IP Payload Compression Protocol (IPComp) compression before encryption. The default value is Disable.
   - **Force NAT-T:** Click Enable to enforce UDP encapsulation of ESP packets. The default value is Disable.
   - **Dead Peer Detection:** By default, the IKE protocol runs a health check with the remote peer to ensure that it is alive. Click **Disable** to disable the health check.
   - **NAT-T Keep Alive Interval:** Enter a value (in seconds) to set the keepalive interval for NAT traversal. The default keep alive interval is 20 seconds. Accepted values are 1 to 65536. To disable the keep alive interval, click Disable.
   - **FailOver Options:** To configure the failover settings when APs are unable to connect, configure the following options:
     - **Retry Period:** Set the number of days (minimum 3 days) during which APs will keep attempting to connect. Select the **Forever** check box to keep trying indefinitely.
     - **Retry Interval:** Set the interval (in minutes) between each retry attempt. The default retry interval is 1 minute. Accepted values are from 1 through 30 minutes.
     - **Retry Mode:** Click **Revertive** if you want APs to fall back to the specified primary security gateway. Click **Non-revertive** if you want APs to maintain connectivity with the security gateway to which they are currently connected.
10. Click **OK**.

    NOTE
    You can also edit, clone, and delete the profile by selecting the Configure, Clone, and Delete options respectively from the IPsec tab.

Creating an Ethernet Port Profile

An Ethernet port profile contains settings that define how an AP will handle VLAN packets when its port is designated as a trunk, access, or general port. By default, three Ethernet port profiles exist: General Port, Access Port, and Trunk Port.

Follow the below steps to create an **Ethernet Port** profile.

1. From the main menu go to **Services** > **Tunnels and Ports**.
2. Select the **Ethernet Port** tab, and then select the zone for which you want to create the profile.
3. Click **Create**.

   The **Create Ethernet Port** page is displayed.

4. Configure the following options:
   - General Options
     - Name: Enter a name for the Ethernet port profile that you are creating.
     - Description: Enter a short description about the profile.
     - Type: The Ethernet port type defines how the AP will manage VLAN frames. You can set Ethernet ports on an AP to one of the following types: Trunk Port, Access Port, or General Port. By selecting the appropriate port type, authentication method, and 802.1X role, you can configure the Ethernet ports to be used for the wired client. If you select a non-user port, there is no restriction on the number of clients supported. If the User Side Port is selected, the maximum number of supported clients is 32 and this number is configurable.
   - Ethernet Port Usage
     - Access Network:
       - Default WAN: Enables default WAN configuration
       - Local Subnet(LAN): Enables DHCP service on ethernet ports. In the **VLAN Options**, select the **VLAN Untag ID** in the ethernet profile which is similar to the DHCP NAT VLAN ID.
       - Tunnel Ethernet Port Profile: Enables tunneling on the ethernet port
     - Anti-spoofing: Prevents attacks on genuine clients from rogue clients that could lead to service disruption, data loss, and so on. This is achieved by matching the MAC address or IP address (IPv4) of the client with the address in the RUCKUS database. If the addresses do not match, the packet is dropped. These checks are also performed on ingress data packets to catch spoofed data packets early.
       - ARP request rate limit: The Address Resolution Protocol (ARP) limits the rate of ARP requests from the connected clients to prevent ARP flooding. Enter the number of packets to be reviewed for ARP attacks per minute. In ARP attacks, a rogue client sends messages to a genuine client to establish connection over the network.
       - DHCP request rate limit: The DHCP request limits the rate of DHCP requests from the connected clients to prevent DHCP flooding. Enter the number of packets to be reviewed for DHCP pool exhaustion, per minute. When rogue clients send a DHCP request with a spoofed address, an IP address from the DHCP pool is assigned to it. If this happens repeatedly, the IP addresses in the DHCP pool are exhausted, and genuine clients may miss out on obtaining the IP addresses.

         NOTE
         When you enable anti-spoofing, an ARP request rate limiter and a DHCP request rate limiter are automatically enabled with default values (in packets per minute) which are applied per client; implying that each client connected to an interface enabled with anti-spoofing is allowed to send a maximum of "X" ARP and DHCP request packets per minute (ppm). The "X" value is configured on the interface to which the client is connected.
     - User Side Port: User Side Port is by default enabled when 802.1x is enabled.
       - Number of clients allowed to be connected: Enter the number of clients that can be connected to the User Side Port. The maximum number of clients that can be connected is 32.
   - Wired Client Isolation
     - Client Isolation: Prevents wired clients from communicating with each other. This option isolates wired client traffic from all hosts on the same VLAN/subnet. By default, this option is disabled. Enable the following options as approriate:
       - Isolate unicast packets: Isolates only unicast packets between a wired client enabled with client isolation and other clients of the AP. By default, this option is enabled.
       - Isolate multicast/broadcast packets: Isolates only multicast/broadcast packets between a wired client enabled with client isolation and other clients of the AP. By default, this option is disabled.
       - Automatic support for VRRP: Isolates packets in Virtual Router Redundancy Protocol (VRRP) deployment. By default, this option is disabled indicating the AP is not in VRRP deployment.
     - Isolation Whitelist: Defines wired destinations on the local subnet that can be reached, even if client isolation is enabled. This option is available only if you enable Wired Client Isolation.

- Authentication Options
  - 802.1X: Select to enable 802.1X authentication.
  - 802.1X Role: Select the authenticator role from the menu.
    - Supplicant: You can customize the user name and password to authenticate as a supplicant role or use the credentials of the AP MAC address.
    - MAC-based Authenticator: Each MAC address host is individually authenticated. Each newly learned MAC address triggers an Extensible Authentication Protocol over LAN (EAPoL) request-identify frame.
    - Port-based Authenticator: Only a single MAC address host must be authenticated for all hosts to be granted access to the network.
  - Enable client visibility regardless of 802.1X authentication: If client visibility is enabled, you can view connected wired client information. Client visibility is enabled by default if the 802.1x authentication method is selected. For the open authentication method, you must enable client visibility based on your requirements.

    NOTE
    You can view statistical information about wired clients without enabling 802.1X authentication.

- Supplicant: Select the authentication type
  - MAC Address: Select this option to use the AP MAC address as the username and password.
  - Custom: Enter customized Username and Password to authenticate.
- VLAN Options
  - VLAN Untag ID: Enter the ID of the native VLAN (typically 1), which is the VLAN into which untagged ingress packets are placed upon arrival. If your network uses a different VLAN as the native VLAN, configure the VLAN Untag ID of the AP Trunk port with the native VLAN used throughout your network. If **Local Subnet** option is selected in **Ethernet Port Usage**, then VLAN ID configured should be the same as one of DHCP NAT VLANs.
  - VLAN Members: Enter the VLAN IDs that you want to use to tag WLAN traffic that will use this profile. You can enter a single VLAN ID or a VLAN ID range (or a combination of both). The valid VLAN ID range is from 1 through 4094. If **Local Subnet** option is selected in **Ethernet Port Usage**, then only DHCP NAT VLANs are allowed on trunk port.
  - Enable Dynamic VLAN: Select this check box if you want the controller to assign VLAN IDs on a per-user basis. Before enabling dynamic VLAN, you must define on the RADIUS server the VLAN IDs that you want to assign to users.

    NOTE
    The Enable Dynamic VLAN option is only available when the Type is set to Access Port and 802.1X authentication is set to MAC-based Authenticator.

    NOTE
    If you enable client visibility, a maximum of 16 clients can be connected to a port regardless of the 802.1X authentication. The same limitation applies when 802.1X authentication is enabled and client visibility is not enabled.

  - Guest VLAN: Select this option if you want to limit the device access to internal network resources only.
  - QinQ VLAN: Select the check box and update the ranges:
    - QinQ SVLAN Range: Enter a SVLAN range. The range is 2 through 4095.
    - QinQ CVLAN Range: Enter a CVLAN range. The range is 2 through 4095.

    NOTE
    For QinQ VLAN to work:

    - Port Type: Must be Access Port
    - Access Network: Must be Tunnel Ethernet Port traffic
    - 802.1x Role: Enabled with Mac Based
    - DVLAN: Enabled

        - Q in Q (Client Visibility and User Side Port are by default enabled): Enabled

- Authentication and Accounting Services
  - Authentication Server: Select the check box and a controller from the menu to use the controller as a proxy authentication server.
  - Accounting Server: Select the check box and a controller from the menu to use the controller as a proxy accounting server.
  - Enable MAC authentication bypass: Select this check box if you want to use the device MAC address as access credentials (user name and password).
- RADIUS Options
  - NAS ID: Set the NAS ID for the AP to communicate with the RADIUS server. Options include using the AP MAC address or any user-defined address.
  - Delimiter: If the AP MAC address is selected to configure the NAS ID, then you can choose between Dash or Colon as delimiters to separate.
- Firewall Options

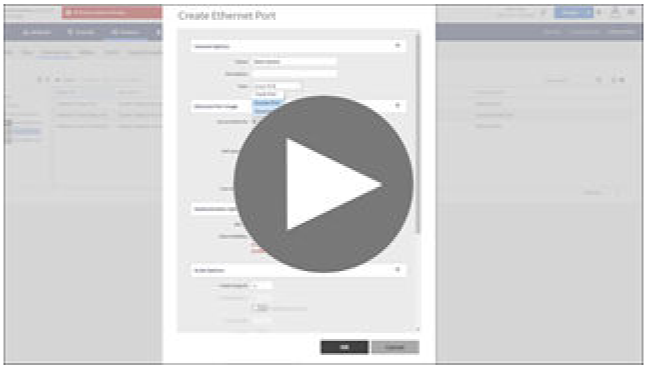
  NOTE
  The User Side Port must be enabled to configure the Firewall Profile, Application Recognition and Control, and URL Filtering Policy.

  NOTE
  While mapping group attribute values to the user role, avoid special characters or duplicate entries regardless of the order.

  - Firewall Profile: Select the firewall profile for wired ports.
  - Application Recognition and Control: Enable the option for the wired clients.
  - URL Filtering Policy: Enable the option for wired clients.
  - L2 Access Control Policy: Select the Layer 2 policy for wired ports. When the User Side Port is not enabled, a Layer 2 Access Control wired support policy can be mapped directly to the wired port. If the User Side Port is enabled, the Layer 2 Access Control wired support policy can be mapped to the wired port of the firewall profile. Click + to create a new policy. Refer to the **Creating a L2 Access Control Service** section of the *SmartZone Security Guide (SZ300/vSZ-H)* for more information.
- Click **OK**.

NOTE
You can edit, copy, or delete the profile by selecting the options **Configure**, **Clone**, or **Delete**, respectively, from the **Ethernet Port** tab.

VIDEO
Creating Ethernet Port Profiles. Creating an Ethernet port profile (securing secondary wired port), port types explained



Click to play video in full screen mode.

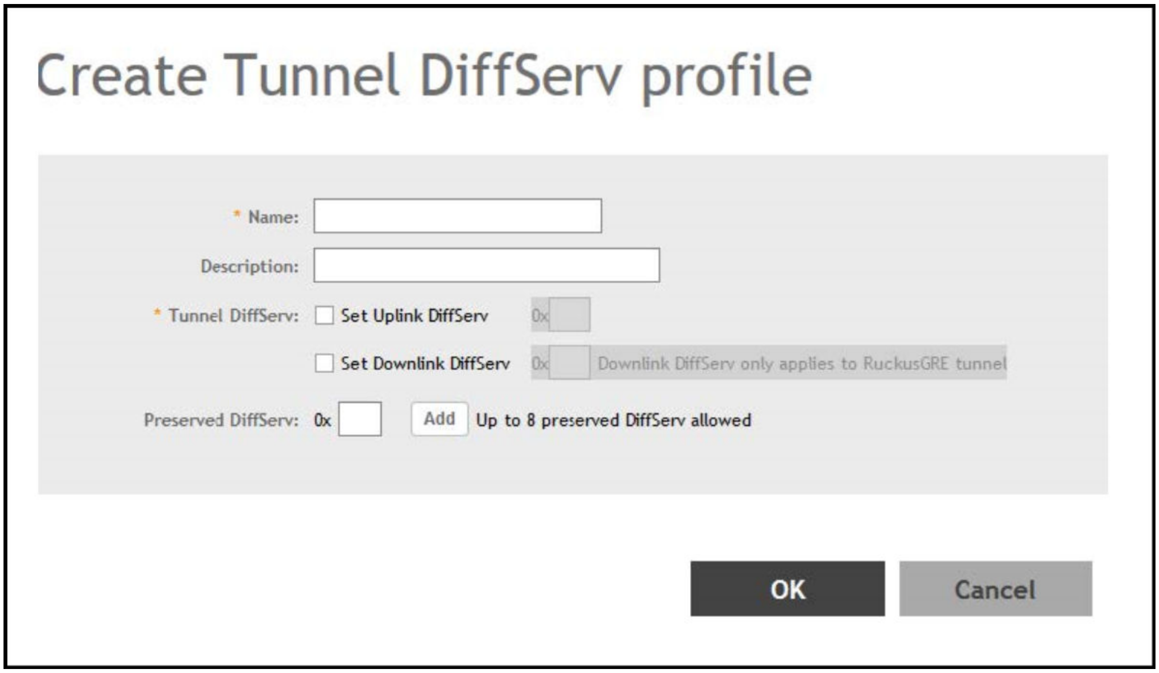
Creating a Tunnel DiffServ Profile

If you want to configure the type of service (ToS) bit settings for the access-side traffic from RUCKUS APs, complete the following steps to create a Differentiated Services (DiffServ) profile. This profile can only be applied to RuckusGRE and SoftGRE traffic.

1. From the main menu, go to **Services** > **Tunnels and Ports**.
2. Select the **DiffServ** tab, and then select the zone for which you want to create the profile.
3. Click **Create**.

   The **Create Tunnel DiffServ Profile** dialog box is displayed.

   FIGURE 19 Creating a Tunnel DiffServ Profile

   Downlink DiffServ only applies to RuckusGRE tunnel

   Up to 8 preserved DiffServ allowed

4. Configure the following options:
   - **Name:** Enter a name for the DiffServ profile that you are creating.
   - **Description:** Enter a brief description for the DiffServ profile.
   - **Tunnel DiffServ:** Configure the following options.
     - **Set Uplink DiffServ:** Select the check box if you want to set the **Differentiated Services** field for uplink user traffic from RUCKUS APs towards either the controller or a third-party gateway using SoftGRE, and enter the desired value to be set by the RUCKUS AP.
     - **Set Downlink DiffServ:** Select the check box if you want to set the **Differentiated Services** field for downlink user traffic from the controller towards the AP, and enter the desired value to be set by the RUCKUS AP.
   - **Preserved DiffServ:** Configure up to eight entries in the preserved DiffServ list. The Preserved DiffServ list allows the preservation of values that have been already marked in incoming packets either in uplink or downlink traffic.

5. Click **OK**.

   NOTE
   You can also edit, clone, and delete the profile by selecting the **Configure**, **Clone**, and **Delete** options respectively from the **DiffServ** tab.

Applying Communications Assistance for Law Enforcement Act

The Communications Assistance for Law Enforcement Act (CALEA) is a law passed by the United States. This is to enhance the ability of law enforcement agencies to conduct electronic surveillance by requiring that telecommunications carriers and manufacturers of telecommunications equipment, to modify and design their equipment, facilities, and services to ensure that they have built-in surveillance capabilities.

NOTE
CALEA applies only to the virtual SmartZone (vSZ-H) platform.

1. From the main menu, go to **Services** > **Tunnels and Ports**.
2. Select the **CALEA** tab.
3. For **Server IP**, enter the CALEA server IP address, and click **OK**.
4. Click **Create**.

   The **Create UE MAC** dialog box is displayed.

   NOTE
   Only the health of top 100 clients are displayed.

5. For **MAC Address**, enter the MAC address of the client or user equipment for which CALEA mirroring is required. The MAC address is sent by the controller to the vSZ-D.
6. Click **OK**.

Enabling Tunnel Encryption

You can use tunnel encryption to encrypt data for a private network through a public network. Tunnel encryption is available in virtual controller vSZ-H and vSZ-E platforms.

1. From the main menu, go to **Services** > **Tunnels and Ports**.
2. Select the **Tunnel Encryption(DP)** tab.

   The **Tunnel Encryption(DP)** tab is displayed.

3. Set **Enable Tunnel Encryption** to **ON**. By default the encryption is turned OFF.
4. Click **OK**.

Forwarding Multicast Packets

In multicast forwarding, a group of hosts is typically grouped under a multicast IP address. Data can then be transmitted from the source to the IP address, which in turn transmits data to the various hosts assigned to the multicast IP address. This is point-to-multipoint data transmission. Forwarding multicast packets is only available for the SZ100.

1. From the main menu, navigate to **Services** > **Tunnels and Ports**.
2. Select the **Multicast Forwarding** tab.

   The **Multicast Forwarding** tab is displayed.
3. Under **Global Setting**, set **Enable forwarding multicast packet on tunnel mode** to **ON**. By default the setting is set to OFF.
4. Click **OK**.

Split Tunnel Profile

A Split Tunnel Profile can be created to manage corporate and local traffic by sending only corporate traffic to the controller. A split tunnel ensures that local traffic does not incur the overhead of the round trip to the controller, which decreases traffic on the WAN link and minimizes latency for local application traffic. Using a split tunnel, a remote user is associated with a single SSID (rather than multiple SSIDs) to access corporate resources, such as a mail server, and local resources (for example, a local printer).

Split Tunnel Profile Limitations

Before enabling the Split Tunnel Profile, consider the following limitations:

- The Split Tunnel Profile does not support a zone where Mesh-enabled APs are present.
- The Split Tunnel Profile and Express Wi-Fi are not supported together on the same WLAN.
- For the Split Tunnel Profile and Express Wi-Fi to work properly, the configured IP rules for a split tunnel and a walled garden must be different.
- The Split Tunnel Profile does not support DHCP server or NAT router.
- The Split Tunnel Profile does not support wired clients.
- The limitations applicable to DHCP or NAT also apply to the Split Tunnel Profile.
- WISPr-related (web-authentication) WLANs are not supported on a split tunnel WLAN.
- ICMP is not supported towards a line buildout (LBO) split path where Source Network Address Translation (SNAT) occurs.
- IPv6 addresses are not supported in the Split Tunnel Profile.
- Multicast discovery of Bonjour devices will not occur over the LBO.
- As the data traffic is established from the server side, TFTP is not supported.
- As the server rejects the data connection that does not have the NAT IP address sent by the client, the FTP active mode is not supported with a split tunnel.

Creating a Split Tunnel Profile

A Split Tunnel profile is created to manage corporate and local traffic by sending only corporate traffic to the controller.

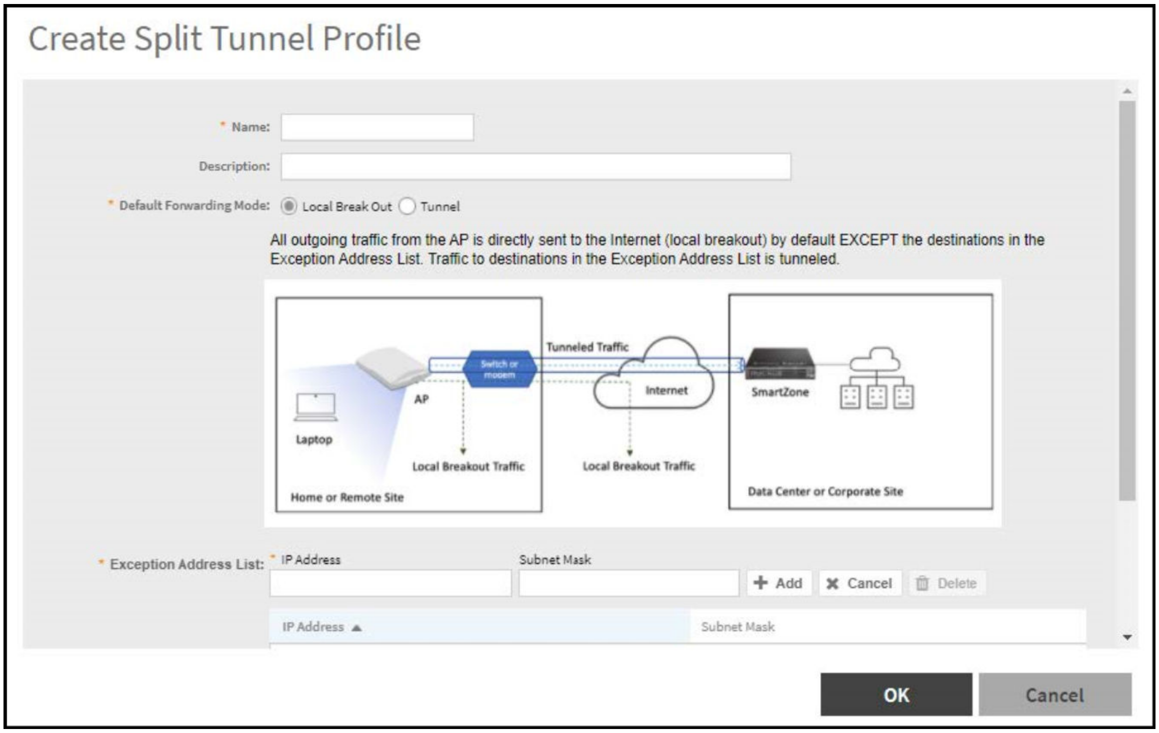
Complete the following steps to configure a split tunnel profile.

1. From the main menu go to **Services** > **Tunnels and Ports** > **Split Tunnel**.

2. Select the zone for which you want to create the profile and click **Create**.

   The **Create Split Tunnel Profile** window is displayed.

   FIGURE 20 Creating a Split Tunnel Profile



Create Split Tunnel Profile

* Name:

Description:

* Default Forwarding Mode: ● Local Break Out ○ Tunnel

All outgoing traffic from the AP is directly sent to the Internet (local breakout) by default EXCEPT the destinations in the Exception Address List. Traffic to destinations in the Exception Address List is tunneled.

* Exception Address List: * IP Address | Subnet Mask

3. Enter the split tunnel profile information:

   NOTE
   RuckusGRE or SoftGRE must be enabled on the WLAN before mapping it to a Split Tunnel Profile.

   a. In the **Name** field, type a name for the split tunnel profile.
   b. In the **Description** field, type a short description for the split tunnel profile.
   c. In **Default Forwarding Mode** field, select one of the following option:
      - **Local Break Out**: All outgoing traffic from the AP is by default sent to the Internet (local breakout) except for the destinations in the Exception Address List. Traffic to destinations in the Exception Address List is tunneled.
      - **Tunnel**: All outgoing traffic from the AP is tunneled except for the destinations in the Exception Address List. Traffic to destinations in the Exception Address List is directly sent to the Internet (local breakout).
   d. In the **IP Address** field, enter the destination IP address.
   e. In the **Subnet Mask** field, enter the destination IP subnet mask.
   f. Click **Add** to add the destination IP details.
   g. Click **OK**.

   NOTE
   You can also edit, clone or delete the profile by selecting the options **Configure**, **Clone**, and **Delete** respectively from the **Split Tunnel** tab.

Creating a Bond Port Profile

A Bond port profile aggregates multiple network interfaces into a single logical interface. Existing Ethernet configurations must be removed before forming a bonding interface. As both Ethernet links should operate at the same speed, the link speed must be downgraded and should be set to 1 Gbps.

Following default configurations are chosen when the bond is formed on the AP:

```
Mode: 8023AD
LACP-rate: slow
MII-Mon: 100 (ms)
Xmit-Hash: layer2+3
```

To create a bond-port profile follow these steps.

1. From the main menu go to **Services** > **Tunnels & Ports** > **Bond Port**.
2. Select the zone or AP Group and click **Create**.

   The **Create Bond Profile** page is displayed.
3. Configure the following options:
   a. **General Options**
      1. **Name**: Enter a name for the Bond port profile that you are creating.
      2. **Description**: Enter a short description about the profile.
      3. **Type**: The Ethernet port type configuration. You can set the Ethernet ports on an AP to one of the following types: **Trunk Port**, **Access Port**, or **General Port**.

   b. **VLAN Options**
      1. **VLAN Untag ID**:
      2. **VLAN Members**:
4. Click **OK**.

Managing Core Network Tunnels

Tunneling protocols allows users to access or provide a network service that the network does not support or provide directly.

Creating Bridge Forwarding Profiles

An Bridge forwarding profile defines the DHCP configuration for the core network.

Follow the below steps to create a Bridge Forwarding Profile.

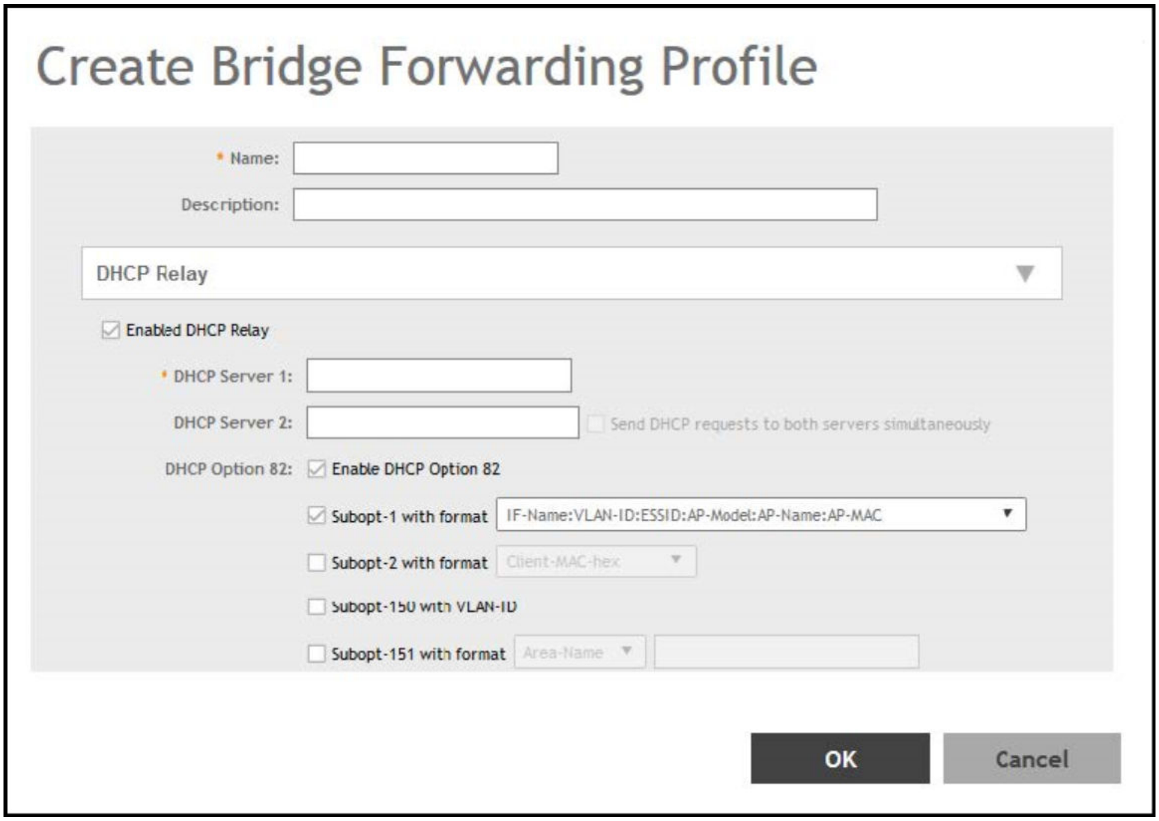
NOTE
This feature is applicable only for SZ300 and vSZ-H platforms.

1. From the main menu go to **Services** > **Tunnels and Ports** > **Core Network Tunnel** > **Bridge**.
2. Select the zone for which you want to create the profile.

3. Click **Create**.

   The **Create Bridge Forwarding Profile** page is displayed.

FIGURE 21 Creating a Bridge Forwarding Profile



Create Bridge Forwarding Profile

* Name:

Description:

DHCP Relay ▼

☑ Enabled DHCP Relay

* DHCP Server 1:

DHCP Server 2: □ Send DHCP requests to both servers simultaneously

DHCP Option 82: ☑ Enable DHCP Option 82

☑ Subopt-1 with format: IF-Name:VLAN-ID:ESSID:AP-Model:AP-Name:AP-MAC ▼

□ Subopt-2 with format: Client-MAC-hex ▼

□ Subopt-150 with VLAN-ID

□ Subopt-151 with format: Area-Name ▼

4. Configure the following:
   a. Name: Type a name for the profile that you are creating.
   b. Description: Type a brief description for the profile.
   c. DHCP Relay: Select the **Enable DHCP Relay**check-box and configure the DHCP server IP address and DHCP option 82 settings.
      1. DHCP Server 1: Type the IPv4 address of the DHCP server that will allocate IP addresses to DHCP clients.
      2. DHCP Server 2: If a secondary DHCP server exists on the network, type the IPv4 address of the secondary server.
      3. DHCP Option 82: Select this check box if you want the DHCP relay agent (in this case, the controller) to insert specific identification information into requests that are forwarded to the DHCP server. If you enabled DHCP Option 82, you can configure the following Option 82 sub-options by selecting the corresponding check boxes:
         - Subopt-1 with format: You can customize sub-option 1 (Circuit ID) to send only the AP’s MAC address in hexadecimal format or the MAC address and ESSID. The default format is: IFName:VLAN-ID:ESSID:AP-Model:AP-Name:AP-MAC.
         - Subopt 2 with format: You can customize sub-option 2 (Remote ID), which sends the client’s MAC address by default, to send the AP’s MAC address, or the client MAC plus ESSID or AP MAC plus ESSID.
         - Subopt-150 with VLAN ID: This sub-option encapsulates the VLAN ID.
         - Subopt-151 with format: This sub-option can encapsulate either the ESSID or a configurable Area Name.
   d. Click **OK**.

You have created the Bridge forwarding profile.

> **NOTE**
> You can also edit and delete the profile by selecting the options **Configure** and **Delete** respectively, from the **Bridge** tab.

Creating L2oGRE Forwarding Profiles

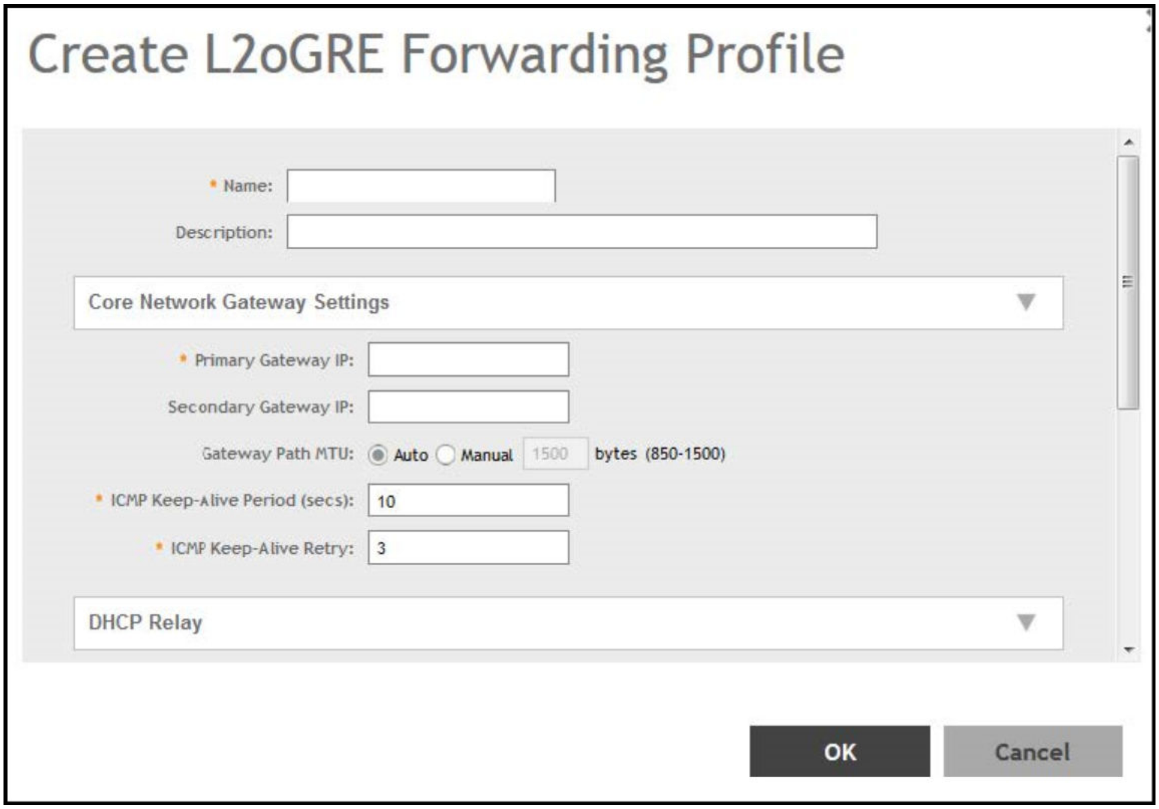
An L2oGRE forwarding profile defines the gateway and tunnel configuration for the core network of L2oGRE tunnels. This feature is applicable only for SZ300 and vSZ-H platforms.

Follow the below steps to create a L2oGRE Forwarding Profile.

1. From the main menu go to **Services** > **Core Network Tunnel** > **L2oGRE**.
2. Select the zone for which you want to create the profile.
3. Click **Create**.

   The **Create L2oGRE Forwarding Profile** page is displayed.

FIGURE 22 Creating a L2oGRE Forwarding Profile



Create L2oGRE Forwarding Profile

* Name:

Description:

Core Network Gateway Settings

* Primary Gateway IP:

Secondary Gateway IP:

Gateway Path MTU: ● Auto ○ Manual 1500 bytes (850-1500)

* ICMP Keep-Alive Period (secs): 10

* ICMP Keep-Alive Retry: 3

DHCP Relay

4. Configure the following:

   a. Name: Type a name for the profile that you are creating.

   b. Description: Type a brief description for the profile.

   c. Core Network Gateway Settings

      1. Primary Gateway IP: Type the IP address of the primary gateway for the L2oGRE tunnel.
      2. Secondary Gateway IP: Type the IP address of the secondary gateway for the L2oGRE tunnel. If the primary gateway is unreachable, this gateway will be used for the L2oGRE tunnel.
      3. Gateway Path MTU: Set it the MTU manually or use Auto (default). MTU is the size of the largest protocol data unit (in bytes) that can be passed on the controller network.
      4. ICMP Keep-Alive Period (secs): Set the time in seconds between sending retry messages to the keep alive IP address. Enter an integer between 2 and 255. The default is 10 seconds.
      5. ICMP Keep-Alive Retry: Set the retry period to send messages to the keep alive IP address. The default value is 3 retries.

   d. DHCP Relay: Select the **Enable DHCP Relay**check-box and configure the DHCP server IP address and DHCP option 82 settings.

      1. DHCP Server 1: Type the IPv4 address of the DHCP server that will allocate IP addresses to DHCP clients.
      2. DHCP Server 2: If a secondary DHCP server exists on the network, type the IPv4 address of the secondary server.
      3. DHCP Option 82: Select this check box if you want the DHCP relay agent (in this case, the controller) to insert specific identification information into requests that are forwarded to the DHCP server. If you enabled DHCP Option 82, you can configure the following Option 82 sub-options by selecting the corresponding check boxes:
         - Subopt-1 with format: You can customize sub-option 1 (Circuit ID) to send only the AP’s MAC address in hexadecimal format or the MAC address and ESSID. The default format is: IFName:VLAN-ID:ESSID:AP-Model:AP-Name:AP-MAC.
         - Subopt 2 with format: You can customize sub-option 2 (Remote ID), which sends the client’s MAC address by default, to send the AP’s MAC address, or the client MAC plus ESSID or AP MAC plus ESSID.
         - Subopt-150 with VLAN ID: This sub-option encapsulates the VLAN ID.
         - Subopt-151 with format: This sub-option can encapsulate either the ESSID or a configurable Area Name.

   e. Click **OK**.

You have created the L2oGRE forwarding profile.

> **NOTE**
> You can also edit and delete the profile by selecting the options **Configure** and **Delete** respectively, from the **L2oGRE** tab.

SoftGRE Support

This section describes the SoftGRE support that the controller provides and the supported deployment topology.

Overview of SoftGRE Support

There are numerous equipment vendors serving the service provider market today. Among these vendors, the more prominent ones include Alcatel-Lucent (ALU), Ericsson, NSN, Huawei and Cisco. Most of these vendors support different tunneling and mobility management protocols at their packet gateways.

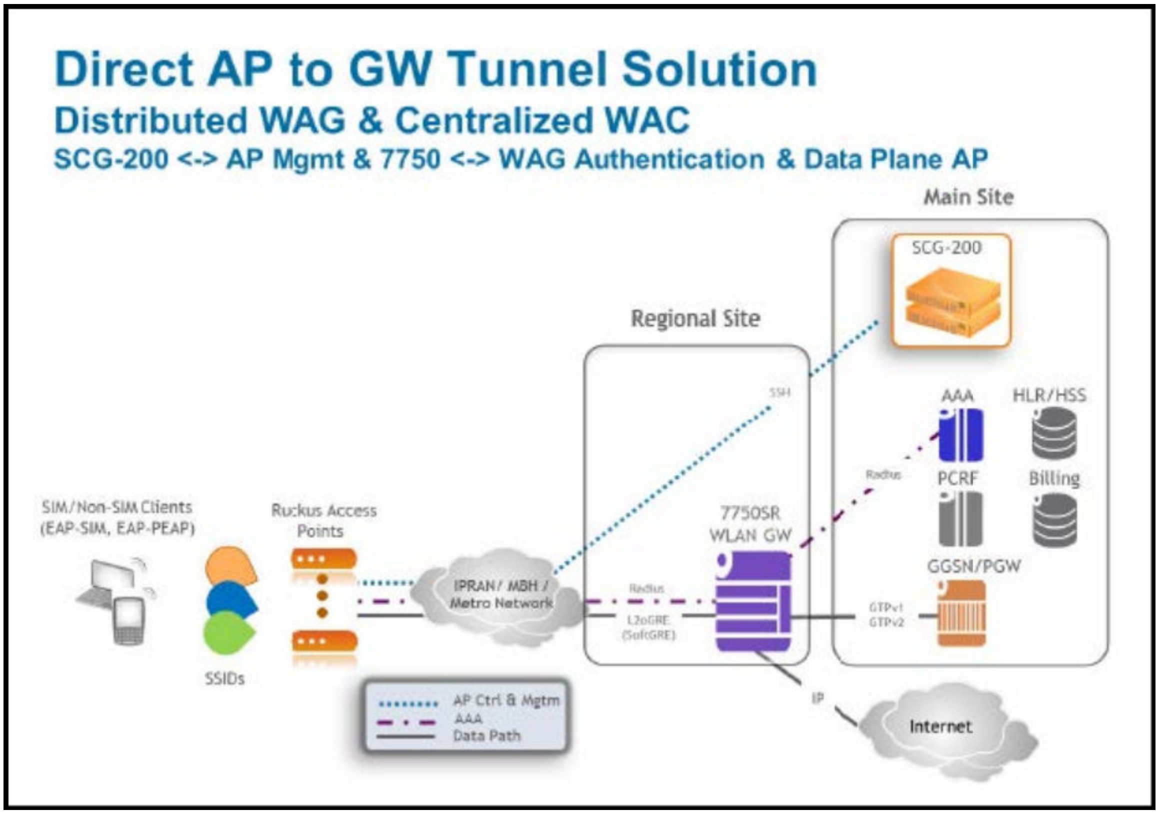
Since most (if not all) of these equipment vendors do not develop access points themselves, they are publishing SoftGRE specifications to enable access point vendors (such as RUCKUS) to support SoftGRE on their devices.

Supported Deployment Scenario

The controller supports SoftGRE in the deployment scenario wherein the controller functions purely as an AP controller. In this deployment topology, the controller only manages the RUCKUS APs and does not perform other functions. All control paths (RADIUS Authentication or Accounting) and data paths (SoftGRE tunnel) terminate on the third party WLAN gateway.

If 802.1x authentication is used, the RADIUS server will be outside of the SoftGRE tunnel. If open, WISPr-based authentication is used, the portal or redirect function will be on the edge router or northbound of the edge router. The controller does not play any role in the control and data path functions.

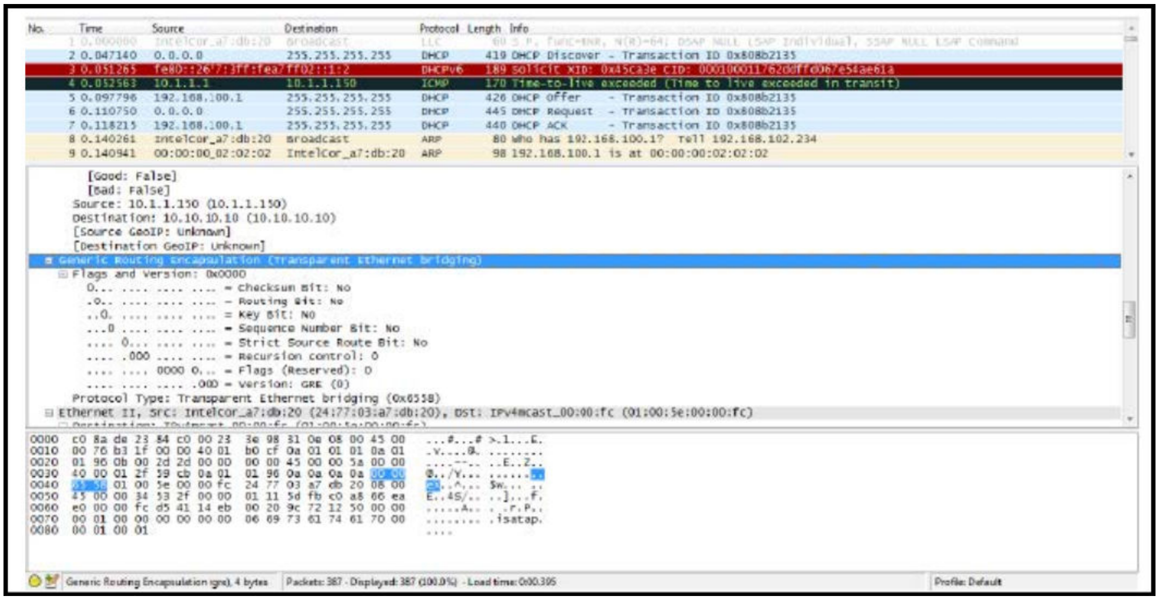
FIGURE 23 Controller as a pure AP controller



SoftGRE Packet Format

The following figure displays a screen shot of SoftGRE packet capture data.

FIGURE 24 Example of SoftGRE Packet Format



```
No.  Time      Source                 Destination          Protocol Length Info
   1 0.000000  Intelcor_a7:db:20      Broadcast            LLC         60 S, P, func=RNR, N(R)=64; DSAP NULL LSAP Individual, SSAP NULL LSAP Command
   2 0.047140  0.0.0.0                255.255.255.255      DHCP       419 DHCP Discover - Transaction ID 0x808b2135
   3 0.051265  fe80::2677:3ff:fea7    ff02::1:2            DHCPv6     189 Solicit XID: 0x45ca3e CID: 000100011762ddffd067e54ae61a
   4 0.052563  10.1.1.1               10.1.1.150           ICMP       170 Time-to-live exceeded (Time to live exceeded in transit)
   5 0.097796  192.168.100.1          255.255.255.255      DHCP       426 DHCP Offer    - Transaction ID 0x808b2135
   6 0.110750  0.0.0.0                255.255.255.255      DHCP       445 DHCP Request  - Transaction ID 0x808b2135
   7 0.118215  192.168.100.1          255.255.255.255      DHCP       440 DHCP ACK      - Transaction ID 0x808b2135
   8 0.140261  Intelcor_a7:db:20      Broadcast            ARP         80 Who has 192.168.100.1?  Tell 192.168.102.234
   9 0.140941  00:00:00_02:02:02      Intelcor_a7:db:20    ARP         98 192.168.100.1 is at 00:00:00:02:02:02
```

```
      [Good: False]
      [Bad: False]
    Source: 10.1.1.150 (10.1.1.150)
    Destination: 10.10.10.10 (10.10.10.10)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
⊟ Generic Routing Encapsulation (Transparent Ethernet bridging)
  ⊟ Flags and Version: 0x0000
      0... .... .... .... = Checksum Bit: No
      .0.. .... .... .... = Routing Bit: No
      ..0. .... .... .... = Key Bit: No
      ...0 .... .... .... = Sequence Number Bit: No
      .... 0... .... .... = Strict Source Route Bit: No
      .... .000 .... .... = Recursion control: 0
      .... .... 0000 0... = Flags (Reserved): 0
      .... .... .... .000 = Version: GRE (0)
    Protocol Type: Transparent Ethernet bridging (0x6558)
⊟ Ethernet II, Src: Intelcor_a7:db:20 (24:77:03:a7:db:20), Dst: IPv4mcast_00:00:fc (01:00:5e:00:00:fc)
```

```
0000  c0 8a de 23 84 c0 00 23  3e 98 31 0e 08 00 45 00   ...#...# >.1...E.
0010  00 76 b3 1f 00 00 40 01  b0 cf 0a 01 01 01 0a 01   .v....@. ........
0020  01 96 0b 00 2d 2d 00 00  00 00 45 00 00 5a 00 00   ....--.. ..E..Z..
0030  40 00 01 2f 59 cb 0a 01  01 96 0a 0a 0a 0a 00 00   @../Y... ........
0040  65 58 01 00 5e 00 00 fc  24 77 03 a7 db 20 08 00   eX..^... $w... ..
0050  45 00 00 34 53 2f 00 00  01 11 5d fb c0 a8 66 ea   E..4S/.. ..]...f.
0060  e0 00 00 fc d5 41 14 eb  00 20 9c 72 12 50 00 00   .....A.. . .r.P..
0070  00 01 00 00 00 00 00 00  06 69 73 61 74 61 70 00   ........ .isatap.
0080  00 01 00 01                                        ....
```

Generic Routing Encapsulation (gre), 4 bytes | Packets: 387 · Displayed: 387 (100.0%) · Load time: 0:00.395 | Profile: Default

Configuring And Monitoring AP Zones

If no tunneled WLANs exist in the zone, you can change the tunnel type from SoftGRE to GRE or GRE + UDP.

MVNO accounts are currently unsupported by SoftGRE tunnels. If you create an MVNO account and assign an AP zone that is using a SoftGRE tunnel, an error message appears.

1. Follow the steps as described in *Creating an AP Zone* in *RUCKUS SmartZone AP Management Guide* to change the tunnel type from SoftGRE.
2. Scroll down to the **AP GRE Tunnel Options** section and select the **Ruckus GRE Profile** or click **Add** to create a new profile.
3. From the Create Ruckus GRE Profile window, select the **Ruckus Tunnel Mode** to change from SoftGRE.

   If you attempt to change the tunnel type when a tunneled WLAN exists within the zone, the following error message appears:

   ```
   Unable to update the configuration of the AP zone. Reason: It is disallowed to change the
   tunnel type, because it
   has tunneled WLAN.
   ```
4. Click **OK**.

   The zone configuration information is displayed.

SoftGRE SNMP MIBs

The following table lists the SoftGRE OIDs.

TABLE 5 OIDs related to SoftGRE

Parent Node	Node Name	OID
ruckusWLANAPInfo	ruckusSCGWLANAPMacAddr	1.3.6.1.4.1.25053.1.3.2.1.1.2.3.1.1
	ruckusSCGWLANAPSoftGREServer	1.3.6.1.4.1.25053.1.3.2.1.1.2.3.1.2
	ruckusSCGWLANAPSoftGREGWAddr	1.3.6.1.4.1.25053.1.3.2.1.1.2.3.1.3
	ruckusSCGWLANAPSoftGREActive	1.3.6.1.4.1.25053.1.3.2.1.1.2.3.1.4

TABLE 5 OIDs related to SoftGRE (continued)

Parent Node	Node Name	OID
	ruckusSCGWLANAPSoftGRETxPkts	1.3.6.1.4.1.25053.1.3.2.1.1.2.3.1.5
	ruckusSCGWLANAPSoftGRETxBytes	1.3.6.1.4.1.25053.1.3.2.1.1.2.3.1.6
	ruckusSCGWLANAPSoftGRERxPkts	1.3.6.1.4.1.25053.1.3.2.1.1.2.3.1.7
	ruckusSCGWLANAPSoftGRERxBytes	1.3.6.1.4.1.25053.1.3.2.1.1.2.3.1.8
	ruckusSCGWLANAPSoftGRETxPktsErr	1.3.6.1.4.1.25053.1.3.2.1.1.2.3.1.9
	ruckusSCGWLANAPSoftGRERxPktsErr	1.3.6.1.4.1.25053.1.3.2.1.1.2.3.1.10
	ruckusSCGWLANAPSoftGRETxPktsDropped	1.3.6.1.4.1.25053.1.3.2.1.1.2.3.1.11
	ruckusSCGWLANAPSoftGRERxPktsDropped	1.3.6.1.4.1.25053.1.3.2.1.1.2.3.1.12
	ruckusSCGWLANAPSoftGRETxPktsFrag	1.3.6.1.4.1.25053.1.3.2.1.1.2.3.1.13
	ruckusSCGWLANAPSoftGREICMPTotal	1.3.6.1.4.1.25053.1.3.2.1.1.2.3.1.14
	ruckusSCGWLANAPSoftGREICMPNoReply	1.3.6.1.4.1.25053.1.3.2.1.1.2.3.1.15
	ruckusSCGWLANAPSoftGREDisconnect	1.3.6.1.4.1.25053.1.3.2.1.1.2.3.1.16

SoftGRE Events and Alarms

If there is no downstream traffic in the tunnel, APs that belong to the zone configured for SoftGRE send out-of-band ICMP keep-alive messages (interval is configurable) to the active third party WLAN gateway. If an AP does not receive a response from the active WLAN gateway, it triggers an alarm and it automatically creates a SoftGRE tunnel to the standby WLAN gateway.

If the AP does not receive a response from the standby WLAN gateway either, the AP disconnects all tunneled WLAN services. It continues to send keep-alive messages to both the active WLAN gateway (primary GRE remote peer) and standby WLAN gateway (secondary GRE remote peer). If it receives a response from either WLAN gateway, the AP restores all tunneled WLAN services automatically.

There are four types of events that APs send to the controller:

- Failover from primary GRE remote peer to secondary GRE remote peer
- Failover from secondary GRE remote peer to primary GRE remote peer.
- Tunnel disconnected because both primary and secondary GRE remote peers are unreachable
- Tunnel restored because either primary or secondary GRE remote peer is reachable

For the list of alarms and events related to SoftGRE that APs generate, refer to SoftGRE Events on page 58 and SoftGRE Alarms.

SoftGRE Events

SoftGRE related events that APs send to the controller.

Following are the events related to SoftGRE that AP generates.

apSoftGRETunnelFailoverPtoS AP [{apname@apMac}] fails over from primaryGRE [{address}] to secondaryGRE [{address}].

Code: 611

Severity:

Attributes:

- "apMac"="xx:xx:xx:xx:xx:xx"
- "primaryGRE"="xxx.xxx.xxx.xxx"
- "secondaryGRE"="xxx.xxx.xxx.xxx"

apSoftGRETunnelFailoverStoP AP [{apname@apMac}] fails over from secondaryGRE [{address }] to primaryGRE [{address}].

Code: 612

	Severity: Warning Attributes: ● "apMac"="xx:xx:xx:xx:xx:xx" ● "secondaryGRE"="xxx.xxx.xxx.xxx" ● "primaryGRE"="xxx,xxx.xxx.xxx"
apSoftGREGatewayReachable	AP [{apname@apMac}] is able to reach [{softgreGW}] [{softgreGWAddress}] successfully. Code: 613 Severity: Informational Attributes: ● "apMac"="xx:xx:xx:xx:xx:xx" ● "softgreGW"="primaryGRE" ● "softgreGWAddress" = "xxx.xxx.xxx.xxx"
apSoftGREGatewayNotReachable	AP [{apname@apMac}] is able to reach [{softgreGW}] [{softgreGWAddress}] successfully. Code: 614 Severity: Critical Attributes: ● apMac"="xx:xx:xx:xx:xx:xx" ● "softGREGatewayList"="xxx.xxx.xxx.xxx, yyy,yyy.yyy.yyy"

URL Filtering

Administrators can use the URL filtering feature to block access to inappropriate websites. The Web pages available on the internet are classified into different categories, and those identified to be blocked can be configured based on available categories. Administrators can also create policies based on these categories, to allow or deny user access.

After categorizing websites accessed by the clients connected to the AP, a third-party cloud-hosted URL categorization service is used to categorize the live web traffic generated from the client devices. By default, traffic which is not categorized is allowed. The packets from the client device are dropped only after the URL is successfully categorized, and DENY is configured for the client in the policy.

The AP periodically generates statistics such as the Top 10 Denied URLs/categories, Top 10 URLs/categories by traffic and sends them to controller which collects this information and maintains it based on the filters applied per zone and WLAN.

URLs are typically classified by third-party applications to enhance internet security and usage. To categorize the web page or URL, the network packets must be analyzed. In HTTP packets, the complete URL value is extracted and in HTTPS packets, the domain name of the URL is extracted for URL web page categorization. The AP remembers the signature of the packet it forwards and when the packet is identified as HTTP or HTTPS, it receives the domain name/URL from the packet and sends it to the third-party URL categorization engine to verify the Web category. If the retrieved category is blocked as per the configured policy, packets with the same signature are blocked. Blocked HTTP browser traffic redirects the user to a web page that provides information on why the access to the website was denied. This feature is not applicable to HTTPS traffic and mobile application traffic.

The AP maintains a cache of up to 98304 URL entries and attempts to find the URL category from the local cache. It contacts the third-party URL categorization server only when the URL is not available in the local cache.

Viewing a Summary of URL Filters

The **Summary** page provides administrators with a view to analyze URL traffic based on the user activity over the network.

You can view the top ten URLs by:

- Traffic - displays all URLs accessed (including blocked URLs) the most
- Categories Traffic - displays all categories accessed (including blocked categories) the most
- Clients Traffic - displays all clients accessed (including blocked clients) the most
- Blocked URLs - displays the URLs that have been denied access the most
- Blocked Categorize - displays the URL categories that have been denied the most
- Blocked Clients - displays the clients that have been denied access the most

Enabling URL Filtering on the WLAN

Administrators can create URL filtering policies and reuse them across WLAN controllers. You can define the policy based on the web page categorization, whitelist, blacklist, and web search.

Policies can also be created based on the role assigned to the user. Users can be allowed or denied access to a particular URL based on the role assigned, and the SSID login details for that role.

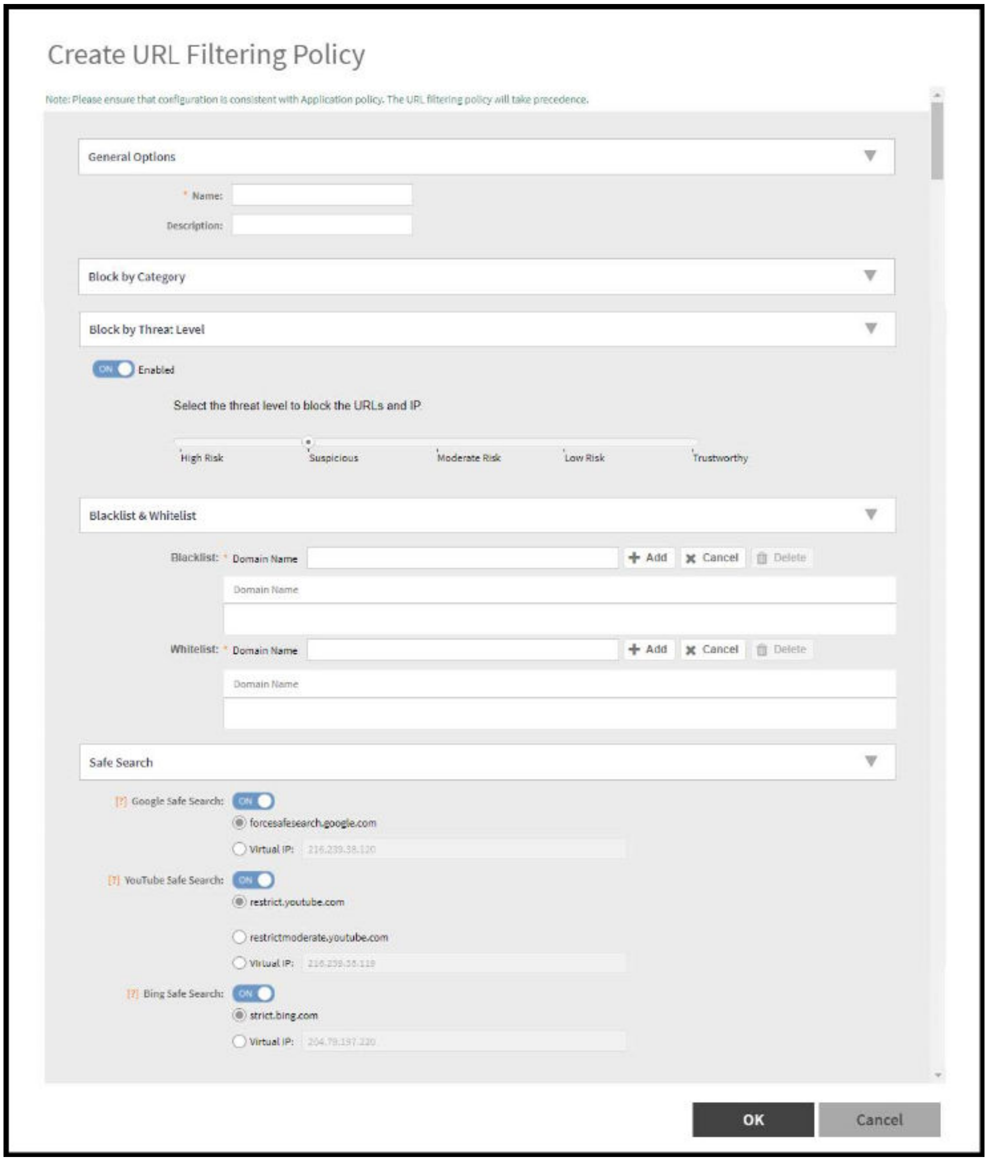
Complete the following steps to create a URL filtering policy.

1. From the main menu go to **Security** > **Access Control** > **URL Filtering** > **Profiles**.

2. Select the **Profiles** tab, and then click **Create**.

   The **Create URL Filtering Policy** page is displayed.

   FIGURE 25 Creating URL Filtering Policy



Create URL Filtering Policy

Note: Please ensure that configuration is consistent with Application policy. The URL filtering policy will take precedence.

General Options

* Name:

Description:

Block by Category

Block by Threat Level

ON Enabled

Select the threat level to block the URLs and IP

High Risk ● Suspicious Moderate Risk Low Risk Trustworthy

Blacklist & Whitelist

Blacklist: * Domain Name

Domain Name

Whitelist: * Domain Name

Domain Name

Safe Search

[?] Google Safe Search: ON

● forcesafesearch.google.com

○ Virtual IP: 216.239.38.120

[?] YouTube Safe Search: ON

● restrict.youtube.com

○ restrictmoderate.youtube.com

○ Virtual IP: 216.239.38.119

[?] Bing Safe Search: ON

● strict.bing.com

○ Virtual IP: 204.79.197.220

Configure the following options:

- General Options

  Name:: Enter the name of the policy you want to create.

  Description: Enter a brief description to identify the policy.

- **Blocked Categories**: Select one of the categories to block. Selecting the **Custom** option allows the administrator to customize the list of categories to block for the user. You can also use **Select All** to choose all of the categories listed, or **None** to set no filters for the user to access (the user can access any URL in this case because no web page is blocked).

- **Block by Threat Level**: Enable this option and set the slider bar to a threat level. The web reputation score, from1 through 100, gives the reputation index or threat level of a URL being browsed by a user. The reputation score can be used to categorize the threat level of URLs according to the following levels:
  - **Trustworthy**: The web reputation score is in the range of 81 through 100. These are well known sites with strong security characteristics.
  - **Low-Risk**: The web reputation score is in the range of 61 through 80. These are generally benign sites and rarely exhibit the characteristics that expose the user to security risks.
  - **Moderate-Risk**: The web reputation score is in the range of 41 through 60. These are benign sites but have exhibited some characteristics that suggest a security risk.
  - **Suspicious**: The web reputation score is in the range of 21 through 40. These are suspicious sites.
  - **High-Risk**: The web reputation score is in the range of 1 through 20. These are high risk sites.
- **Blacklist & Whitelist**: If web content categorization, is unable to classify URLs that the user, organization or institution needs, then Whitelist and Blacklist profiles can be created by the administrator. The URLs listed by the administrator under Blacklist are blocked and those listed under Whitelist are allowed access. The domain names under Blacklist and Whitelist take precedence over the default allow or deny action of the URL filter.

  The AP matches the URL pattern against all the configured Whitelist and Blacklist profiles through the Extended Global Regular Expressions Print (egrep) program which performs a line-by-line scan of the file and returns lines that contain a pattern matching the given expression. Currently, the exact URL name or a wildcard at the beginning of the URL is used to match the pattern. From R5.2 onwards, the wildcard (*) character is supported in middle and on either start or end, for example, "*.ruckus*.com", www.ruckus*.co*). This only allows a maximum of two wildcards (*).

  Administrators can also add specific IP addresses or wildcard domain names under Whitelist and Blacklist.

  In **Domain Name**: Enter the domain name of the web page which you want to deny user access to in the **Blacklist** tab, and enter the domain name of the web page to which you want to provide user access on the **Whitelist** tab. You can define up to 16 domains.

  Click **Add**. The domain name or web page is listed in the corresponding tab.

  Click **Cancel** to remove the domain name you have entered in the field.

  If you want to delete the domain name from the **Blacklist** or **Whitelist** tab, select the URL and click **Delete**.
- Safe Search: Administrators can configure the policy to include a safe search option when users access Google, YouTube, or Bing to search on the internet. Select the respective enable option for Google, YouTube, and Bing. Enabling the option will mandate all users using the policy on the network to use safe search on Google, YouTube, and Bing. By default, FQDN-based safe search is enabled. This option provides a secure connection through HTTPS while allowing access to the internet. To use virtual IP (IPv4 and IPv6) address, select the **Virtual IP** option and enter the IP address. If safe search is enabled before uprading to release 6.1, the old configuration or virtual IP-based safe search will be retained.

3. Click **OK**.

   The **URL Filtering Policy** form is submitted with the specified configuration settings.

You have created the URL filtering policy. The newly created policy is displayed on the **Profiles** page.

If you click the policy, the following information is displayed:

- Name
- Managed By
- Description
- Filtering Level
- # of Blocked Categorize
- # of Blacklist

- # of Whitelist
- Threat Level

Click **Configure** to edit the policy. Click **Clone** to create a duplicate of the policy, or to make modifications to the existing settings of the clone.

Click **Delete** to delete the policy from the URL Filtering Profile.

Enabling URL Filtering on the Controller

You can enable the URL filtering feature on the WLAN controller to block or allow access to specific web sites or web pages.

By configuring the controller, administrator can create a wireless network SSID and allow or deny access to a category of websites for all users that join this SSID.

Follow these steps to enable URL filtering on the controller for an available WLAN.

1. From the main menu go to **Network** > **Wireless LANs** to select a domain or zone.
2. Choose a WLAN from the system tree hierarchy to **Enable URL Filtering** option.

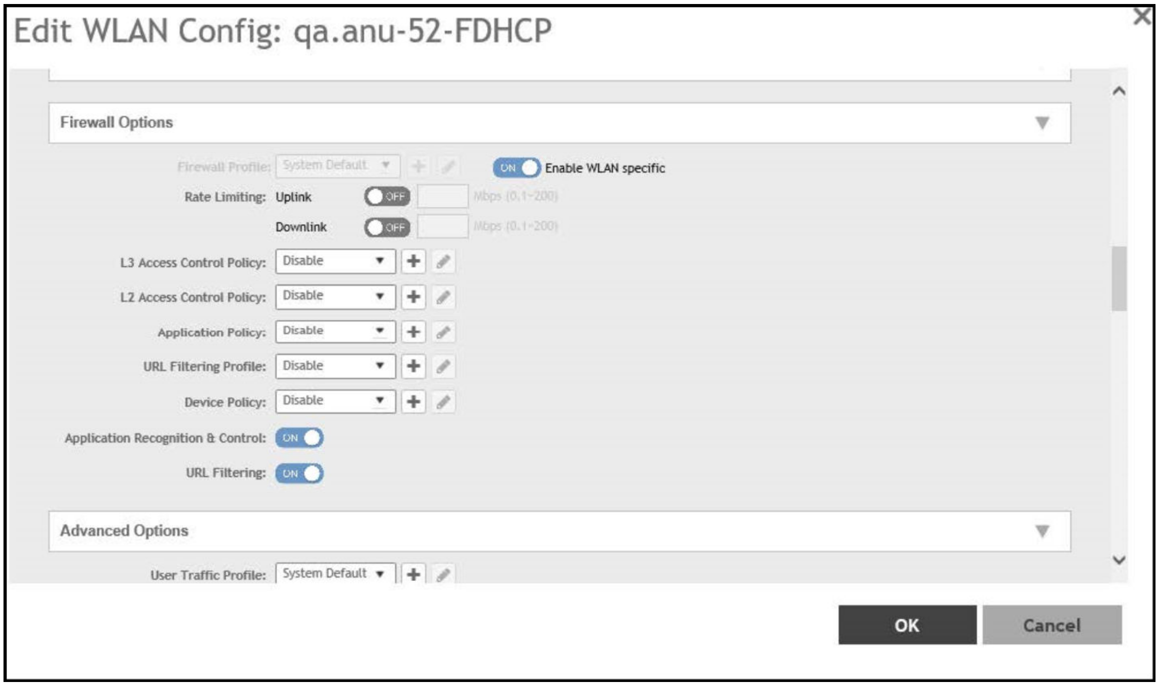
   This displays **Edit WLAN Config** page.

   > **NOTE**
   > To enable URL Filtering for a new WLAN, follow the steps to create a new WLAN.

3. Scroll down to **Firewall Options**, click **URL Filtering Policy** option.

   The **URL Filtering Profile** field appears. Select a URL filtering profile from the drop-down menu. To create a new URL filtering policy, refer Enabling URL Filtering on the WLAN on page 61.

   FIGURE 26 Enabling URL Filtering



Edit WLAN Config: qa.anu-52-FDHCP

Firewall Options

Firewall Profile: System Default
ON Enable WLAN specific
Rate Limiting: Uplink OFF Mbps (0.1-200)
Downlink OFF Mbps (0.1-200)
L3 Access Control Policy: Disable
L2 Access Control Policy: Disable
Application Policy: Disable
URL Filtering Profile: Disable
Device Policy: Disable
Application Recognition & Control: ON
URL Filtering: ON

Advanced Options

User Traffic Profile: System Default

NOTE
Application rules are applied based on the following priority:

a. User defined Access Control Profile

b. URL Filtering

c. Application Control Policy

User defined rules take precedence over URL filtering.

You have enabled URL filtering on the controller.

Managing URL Filtering Licenses

URL Filtering license for the selected partners-to use the content database is issued for a duration of one year for an AP. Dashboard warnings are issued thirty days before the end of the license term.

You can add licenses over time. For example, you can purchase 100 one-year licenses on January 1st and add another 200 one-year licenses in May. The controller receives a new expiry date for the combined license count of 300 APs.

- To view license details such as start date, end date, and capacity, navigate to **Administration** > **Administration** > **Licenses** > **Installed Licenses**.
- For R5.2.1 or earlier releases, navigate to **Administration** > **Licenses** > **Installed Licenses** tab.

For more information on importing installed licenses, synchronizing the controller with the license server, and downloading license files, refer *RUCKUS SmartZone Software Licensing Guide*.

When the license capacity is exhausted, event code 1281 is triggered. When the license period expires, alarm code 8003 is generated, indicating that the URL filtering server is unreachable. For more information, refer *RUCKUS SmartZone Alarms and Events Guide*.

NOTE
A permissive license similar to the BSD 2-Clause License, but with a 3rd clause that prohibits others from using the name of the project or its contributors to promote derived products without written consent.
Copyright (c) 2005, Google Inc. All rights reserved.
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of Google Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

ATTENTION
THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

URL filtering feature is supported only on APs that have a minimum of 256MB RAM.

NOTE
The R730 AP is supported on Zones running R6.1.0.

TABLE 6 List of APs that have a RAM size of 256MB or more

E510	T811-CM	T310c/d/n/s	H320
R720	T610/T610s	C110	R610
R500e	H510	T710 / T710s	R510
R310	T504	R710	R600
T300	T301n	T301s	T300e
FZM300 & FZP300	R500	R700	R730
R750	R650	R550	R850
H550	T750	T750SE	

Understanding Wi-Fi Calling

Mobile service providers offer services where you can make voice calls or send and receive text messages from their mobile phones using a Wi-Fi network, without changing the mobile number.

Built-in software applications on smart phones provide seamless authentication of the device when on the Wi-Fi network with the mobile carrier network. When Wi-Fi calling is enabled by the mobile carrier, an IPsec tunnel is established between the phone and the mobile network through which calls are routed.

Due to increasing use of Wi-Fi for device connections, Wi-Fi Calling is seeing high demand by many service providers worldwide, which allows them to differentiate their Wi-Fi access. Though the end-user device and Mobile Packet Core communicate directly over encrypted tunnels, it is important for the Wi-Fi network to detect and prioritize this type of traffic for an optimal application experience.

Wi-Fi calling supports Wi-Fi calling traffic recognition and prioritization above other network traffic, with visibility for Wi-Fi calling statistics for the network operator.

Analyzing Wi-Fi Calling Statistics

Wi-Fi calls are tunneled to the carrier’s Evolved Packet Data Gateway (EPDG), which eliminates dropped calls when switching from Wi-Fi to LTE and vice versa. Multiple carriers’ EPDGs can be supported on a single WLAN. Wi-Fi Calling coexists seamlessly with RUCKUS CBRS (Citizens Band Radio Service) APs.

Follow the below steps to view Wi-Fi Calling Summary to view statistics, client details and quality chart.

From the main menu, go to **Services** > **Others** > **Wi-Fi Calling** > **Summary**.

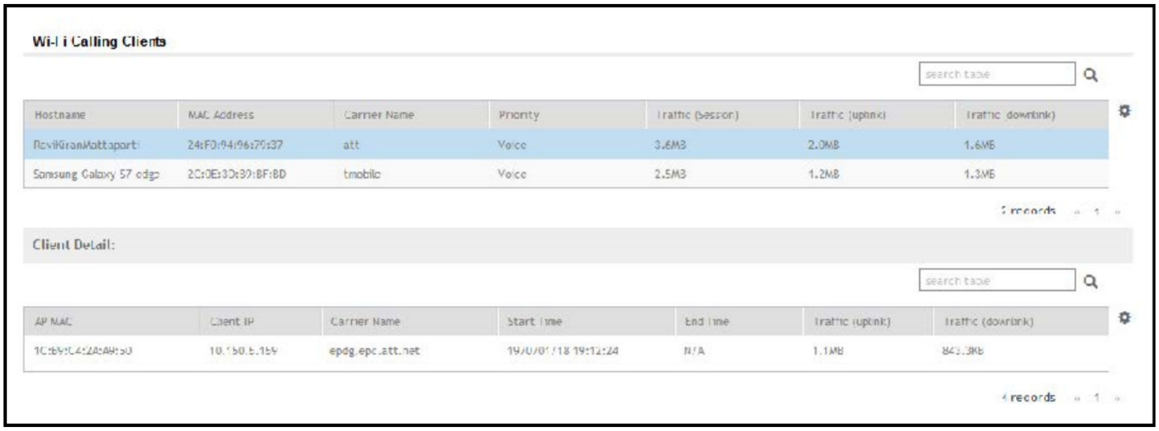
The summary displays statistics of the top ten SSIDs (Service Set Identifier) and Evolved Packet Data Gateway (ePDGs) by traffic in the last one or twenty four hour interval. Choose the Zone or Domain and the corresponding WLAN to view the relevant statistics.

The **Wi-Fi Calling Clients** provides the following information.

- **Hostname**: The name of the user equipment or device that is connected to Wi-Fi.
- **MAC Address**: The MAC address of the user equipment.
- **Carrier Name**: The name of the carrier network or service provider used by the user equipment, such as Verizon, AT&T, Sprint, T-Mobile, and so on.
- **Priority**: The priority set for the Wi-Fi call through this device, such as voice, video, best effort, and background.
- **Traffic Session**: Data that is transmitted during the Wi-Fi call.

- **Traffic (uplink/downlink)**: The speed with which data is transmitted during the Wi-Fi call.

FIGURE 27 Wi-Fi Calling Client Details



Wi-I i Calling Clients

search table

Hostname	MAC Address	Carrier Name	Priority	Traffic (session)	Traffic (uplink)	Traffic downlink)
RaviKiranMattaparti	24:F0:94:96:79:37	att	Voice	3.6MB	2.0MB	1.6MB
Samsung Galaxy S7 edge	2C:0E:3D:30:BF:BD	tmobile	Voice	2.5MB	1.2MB	1.3MB

2 records « 1 »

Client Detail:

search table

AP MAC	Client IP	Carrier Name	Start Time	End Time	Traffic (uplink)	Traffic (downlink)
1C:B9:C4:2A:A9:50	10.150.5.159	epdg.epc.att.net	1970/01/18 19:12:24	N/A	1.1MB	843.3KB

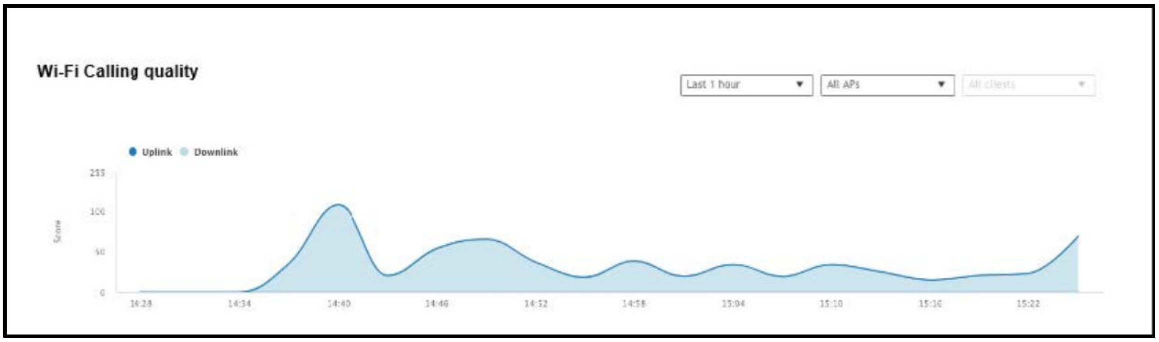
1 records « 1 »

The **Clients Detail** provides the following information.

- **AP MAC:** The MAC address of the AP.
- **Client IP:** The IP address of the client.
- **Carrier Name:** The name of the carrier, such as Verizon, AT&T, Sprint, T-Mobile.
- **Start Time:** The time when the client initiated the Wi-Fi call.
- **End Time:** The time when the client completed the Wi-Fi call.
- **Traffic (uplink/downlink):** The speed with which the data is transmitted during the Wi-Fi call session.

The **Wi-Fi Calling quality** chart displays the uplink and downlink quality. Call quality can be filtered based on time, the AP list, and the client MAC address list.

FIGURE 28 Wi-Fi Calling Quality Chart



Creating a Wi-Fi Calling Profile

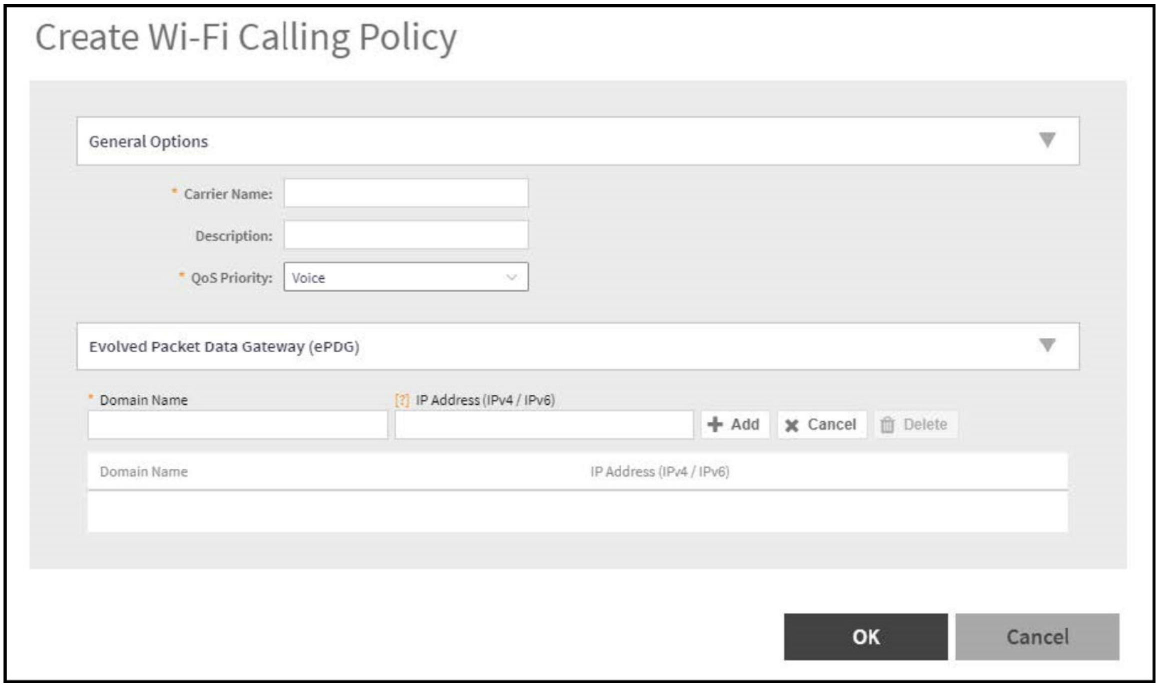
You can classify the voice packets in a Wi-Fi call based on the carrier by creating a Wi-Fi calling profile.

Follow the below steps to create a **Wi-Fi Calling** profile.

1. From the main menu go to **Services** > **Others** > **Wi-Fi Calling** > **Profiles**.
2. Click **Create**.

   The **Create Wi-Fi Calling Policy** dialog box is displayed.

   FIGURE 29 Creating a Wi-Fi Calling Policy



* QoS Priority: Voice

3. Under **General Options**, configure the following options:
   - **Carrier Name**: Enter the name of the carrier based on which you want to create a rule to prioritize the voice calls.
   - **Description**: Enter a brief description o the profile.
   - **QoS Priority**: Select the prioritization for the calls from the list such as Voice, Video, Best Effort and Background.
4. Under **Evolved Packet Data Gateway (ePDG)**, configure the following options:
   - **Domain Name**: Enter the domain name, for example, epdg.epc.att.net.
   - (Optional) **IP Address (IPv4/IPv6)**: Enter the IP address for the domain. Providing the IP address enables better Wi-Fi calling QoS during roaming.
5. Click **Add** to include the domain.

   The AP verifies the domain IP address before qualifying the Wi-Fi call.
6. Click **OK** .

The Wi-Fi calling profile is created and displayed with its name, QoS priority, number of ePDGs associated, and management domain.

NOTE
You can edit,clone, and delete the profile by selecting **Configure**, **Clone**, and **Delete** options respectively.

Configuring Wi-Fi Calling in a WLAN

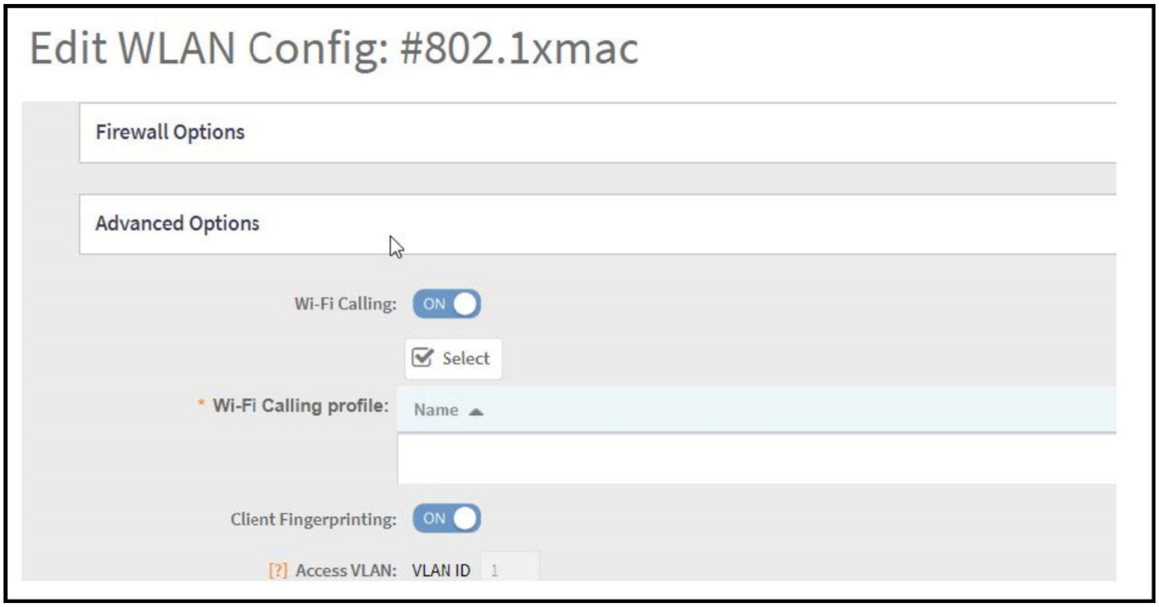
Use the configuration option to create the Wi-Fi policies.

Follow the steps below to edit the WLAN configuration for selecting a Wi-Fi calling profile.

1. From the main menu navigate to **Network** > **Wireless LANS**.
2. Select the WLAN to enable Wi-Fi calling and click **Configure**.

   The **Edit WLAN Configuration** dialog box is displayed. You can also enable Wi-Fi calling when you create a fresh WLAN configuration, by clicking **Create**.

   FIGURE 30 Configuring Wi-Fi Calling in a WLAN



Edit WLAN Config: #802.1xmac

Firewall Options

Advanced Options

Wi-Fi Calling: ON

☑ Select

* Wi-Fi Calling profile: Name ▲

Client Fingerprinting: ON

[?] Access VLAN: VLAN ID 1

3. Under **Advanced Options**, set **Wi-Fi Calling** to **ON**.
4. Click **Select**.

   The **Wi-Fi Calling Policies** dialog box is displayed.
5. From the **Available Profiles** list, identify the profiles you want and click the **->** icon. The profiles move to **Selected Profiles**. You can use the **<-** icon to remove the profile for the WLAN.
6. Click **OK**.

   The profiles selected are displayed in the **Wi-Fi Calling Profile** page.

350 West Java Dr., Sunnyvale, CA 94089 USA
https://www.commscope.com