API REFERENCE GUIDE

Ruckus SmartZone 300 Tunneling Interface Reference Guide

Supporting SmartZone 5.1

Part Number: 800-71939-001 Rev A
Publication Date: November 2018

Copyright, Trademark and Proprietary Rights Information

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, ARRIS 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. ARRIS 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. ARRIS 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 ARRIS 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 ARRIS, ARRIS 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 ARRIS 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

ARRIS, the ARRIS logo, Ruckus, Ruckus Wireless, Ruckus Networks, Ruckus logo, the Big Dog design, BeamFlex, ChannelFly, EdgeIron, FastIron, HyperEdge, ICX, IronPoint, OPENG, SmartCell, Unleashed, Xclaim, ZoneFlex are trademarks of ARRIS International plc and/or its affiliates. Wi-Fi Alliance, Wi-Fi, the Wi-Fi logo, the Wi-Fi CERTIFIED logo, Wi-Fi Protected Access (WPA), the Wi-Fi Protected Setup logo, and WMM are registered trademarks of Wi-Fi Alliance. Wi-Fi Protected Setup™, Wi-Fi Multimedia™, and WPA2™ are trademarks of Wi-Fi Alliance. All other trademarks are the property of their respective owners.

Contents

Preface

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 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.

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@arris.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.ruckuswireless.com.

Online Training Resources

To access a variety of online Ruckus training modules, including free introductory courses to wireless networking essentials, site surveys, and Ruckus products, visit the Ruckus Training Portal at https://training.ruckuswireless.com.

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.ruckuswireless.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://forums.ruckuswireless.com/ruckuswireless/categories
- 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.

About This Guide

Overview

This Ruckus SmartZone (SZ) 300 Tunneling Interface Reference Guide describes the AP networking protocols supported in the access and core networks.

This guide is written for service operators and system administrators who are responsible for managing, configuring, and troubleshooting Ruckus devices. Consequently, it assumes a basic working knowledge of local area networks, wireless networking, and wireless devices.

> **NOTE**
> Refer to the upgrade guide shipped with your product to be aware of certain challenges when upgrading to the latest version of SmartZone.

Most user guides and release notes are available in Adobe Acrobat Reader Portable Document Format (PDF) or HTML on the Ruckus Support Web site at https://support.ruckuswireless.com/contact-us.

Terminology

The table lists the terms used in this guide.

TABLE 2 Terms used in this guide

Terminology	Description
3GPP	3rd Generation Partnership Project
BRI	Binding Revocation Indication
Control Plane	Control Plane
CVLAN	Customer VLAN
DHCP	Dynamic Host Configuration Protocol (DHCP)
DM	Disconnect Message
EPC	Evolved Packet Core
EPS	Evolved Packet System
fwd_policy	Forwarding policy to identify one of the supported network protocol types
GGSN	Gateway GPRS Support Node
GTP	GPRS Tunneling Protocol
ICMP	Internet Control Message Protocol
L2oGRE	Layer 2 over GRE
LBO	Local Breakout Traffic

TABLE 2 Terms used in this guide (continued)

Terminology	Description
PDG	Packet Data Gateway
PDN	Packet Data Network
PGW	PDN Gateway
RADIUS	Remote Access Dial-Up User Service
SGW	Serving Gateway
SVLAN	Service VLAN
TEIDs	Tunnel End Point Identifiers
TTG	Tunnel Terminating Gateway
TWAG	Trusted Wireless Access Gateway

References

The table lists the specifications and standards that are referred to in this guide.

TABLE 3 References used

No.	Reference	Description
1	RFC 2784	Generic Routing Encapsulation (GRE)
2	IEEE 802.1ad	Provider Bridges

Legend

The table lists the legend/presence code used in this guide.

TABLE 4 Legend used

Legend	Description
M	Mandatory
O	Optional
C	Conditional

Impacted Systems

The table lists the impacted systems.

TABLE 5 Impacted Systems

Term	Description
Control plane	• User Interface – Configuration and statistics reporting • Configuration - For core network tunnel destinations • New access - Network type configuration for 3rd Party AP Zones • Session Manager – Supports additional core network tunnel types

TABLE 5 Impacted Systems (continued)

Term	Description
	• ICD Message - Enhancements to support additional forwarding policy • AAA Proxy - Supports additional forward policy – L2oGRE and QinQ
Data plane	• Statistics reporting per: – User per forward policy – Access network type – Core network type • Datacore for: – New forward policy – I/O modules for L2oGRE (both access and core) – QinQ for core network side traffic
Access Point (AP)	Hostpad - New forward policy support for L2oGRE

Core Network Protocols

Overview

This interface reference guide describes the supported protocols for user equipment (UE) access and core network traffic.

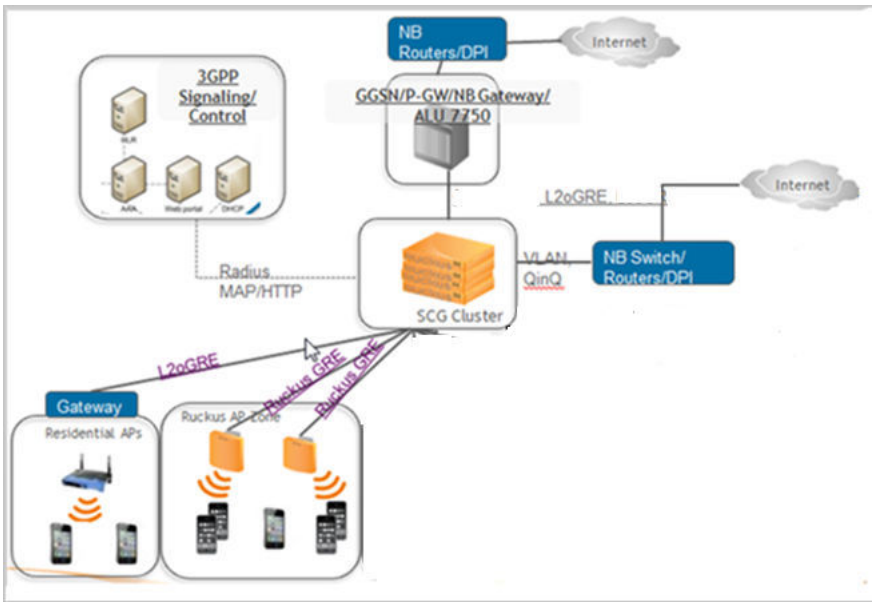
This includes supporting additional tunnel types (both access and core), core network forwarding rules and new networking protocols (both access and core).

On the core network, UE traffic from APs along with next-hop destinations based on forwarding policy supports:

- L2oGRE, which establishes a GRE tunnel to the core network forwarding gateway along with an Ethernet payload. That is, the client's MAC is available to the next hop gateway.
- TTG acts as the gateway where the UE traffic is encapsulated in GTP tunnel and forwarded to GGSN.
- In addition, data plane supports in sending non-tunneled packets to the core network with optional VLAN or QinQ tags.

The figure below shows the tunneling interface and its various tunneling interfaces.

FIGURE 1 Tunneling Interface



Core Network Protocols

Each user equipment (UE) is mapped to one single core network protocol type.

A maximum of 64 core gateways is supported, which translates to supporting 32 GGSNs and 64 GRE core gateways including L2oGRE in any combination.

L2oGRE

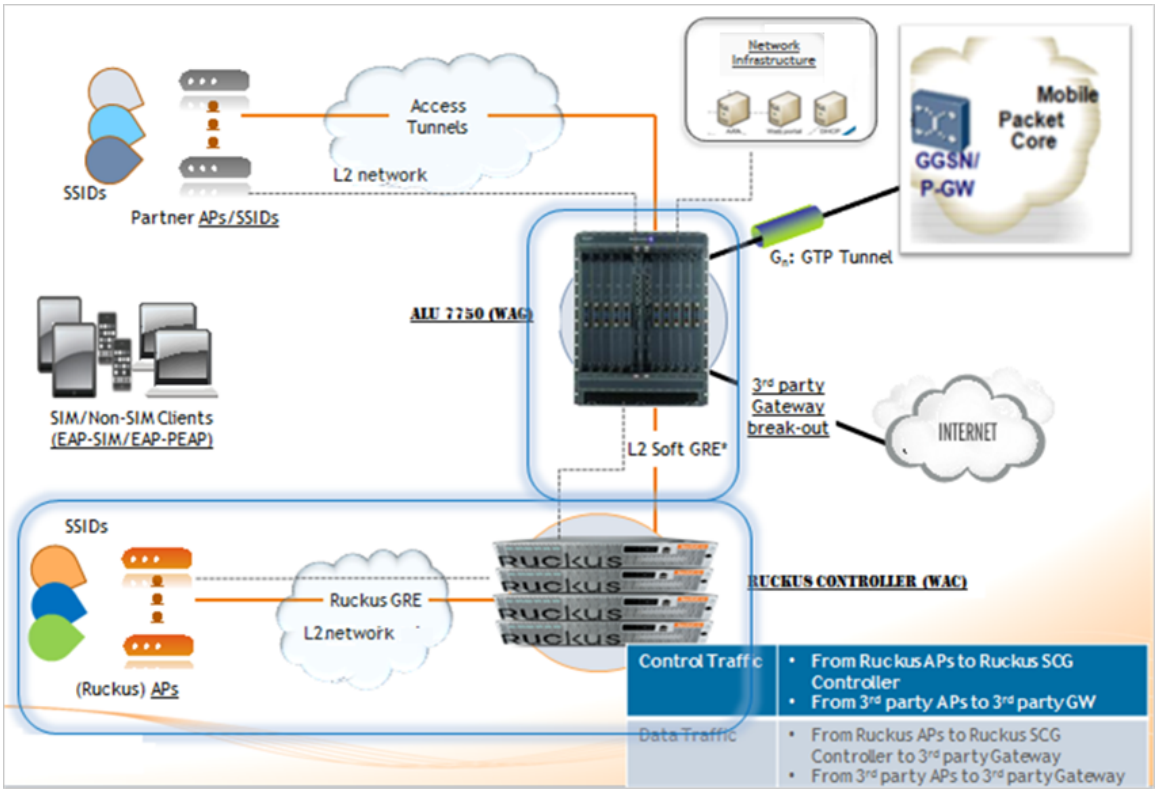
L2oGRE is a core network tunneling protocol, with the following features:

- The GRE header protocol type is 0x6558
- The GRE payload includes Ethernet header for the UE.
- The only supported combination of access network protocol type is L2, which includes Ruckus GRE and L2oGRE.
- ARPs are forwarded to the L2oGRE tunnel.
- DHCP relay function is optionally configured. If it is not configured, the DHCP packets are forwarded in the L2oGRE tunnel.

KeepAlive can be configured to L2oGRE gateway. The only KeepAlive mechanism supported is ICMP echo/reply messages, which are sent or received from L2oGRE gateway. The period for sending KeepAlive is *m* seconds (default = 10 seconds) and the total number of retries is *n* (default counter is 3). The values for *m* and *n* are configurable from command-line interface (CLI).

KeepAlive will always be answered, if it is received from the L2oGRE gateway. The data plane sends a KeepAlive packet only if no user traffic is received from the L2oGRE gateway within the KeepAlive period. An event is generated indicating that the L2oGRE gateway is unreachable when the maximum number of retries exceeds. This event occurs when L2oGRE does not receive an ICMP reply to an ICMP request sent from the datablade. The figure below displays the L2oGRE traffic flow.

FIGURE 2 L2oGRE control and data traffic flow



When redundant L2oGRE gateways are configured, the KeepAlive will be enabled by default. At init time, the first configured gateway will be active. The KeepAlive failures will trigger a switchover to the backup gateway. After the switchover, though the first gateway becomes available, the switchover will not revert until the current active gateway is alive.

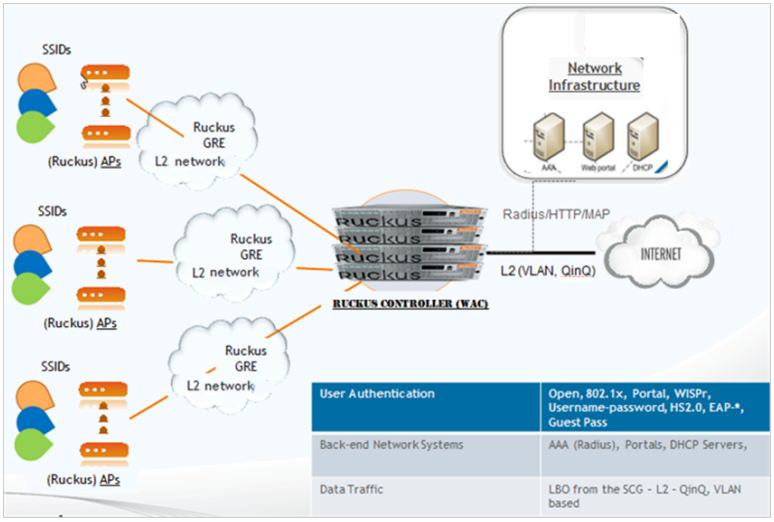
NOTE
For information on how to configure L2oGRE, refer to the Administrator Guide (PDF) or the Online Help, which is accessible from the controller web user interface.

Bridge Mode - (0-2 tags)

Traffic from user equipments (UE) are QinQ tagged and bridged out to the core network.

The core VLAN type can be either QinQ or access VLAN (1 tag). For core network traffic, the QinQ traffic is considered as a type of LBO traffic or VLAN (single) or untagged traffic.

FIGURE 3 QinQ Core Network



NOTE
For information on how to configure QinQ, refer to the SmartZone Administrator Guide (PDF) or the Online Help, which is accessible from the user interface.

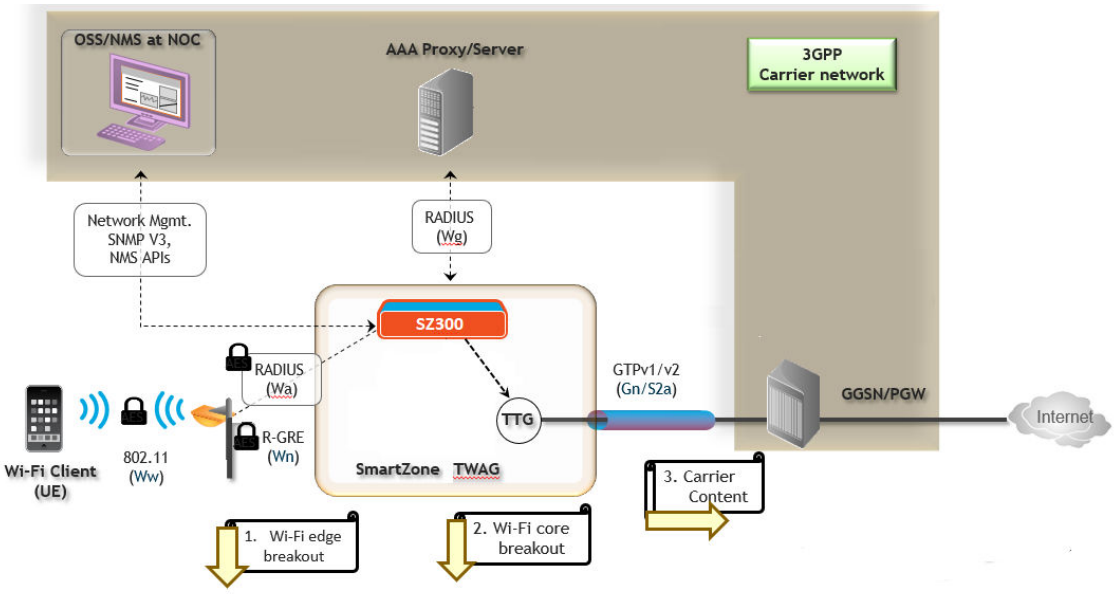
The bridge mode now supports optional DHCP relay function. If it is enabled the user equipment's DHCP packets are relayed to a configured DHCP server. Option 82 sub-option configurations are the same as before.

TTG

The TTG/PDG functionality defines the gateway and tunnel configurations for core network GTP tunnels and LBO configurations.

The controller has 3GPP-defined Tunnel Terminating Gateway (TTG) functionality, which enables it to act as a gateway between the UE and the telecom core to tunnel traffic between the UE (User Equipment, such as mobile phones) and controller gateway terminates the tunnel, and then transfers the data over to GGSN (Gateway GPRS Serving Node) implementing the Gn interface via GTPv1 (Release 6). The Gn interface is used in controlling the signal between controller and GGSN as well as for tunneling end user data payload within the backbone network between both the nodes.

FIGURE 4 Tunnel Terminating Gateway



GPRS Tunneling Protocol (GTP) transmits user data packets and signaling between controller and GGSN. GTP encapsulates traffic and creates GTP tunnels, which act as virtual data channels for transmission of packet data between controller and GGSN. A GTP tunnel is established between controller and GGSN for a data session initiated from UE.

A GTP tunnel is identified by a pair of IP addresses and a pair of GTP Tunnel End Point Identifiers (TEIDs), where one IP address and TEID is for the SGSN and the other is for GGSN. TEID is a session identifier used by GTP protocol entities in SGSN and GGSN.

GTP separates signaling from payload. Traffic is sorted onto a control plane (GTP-C) for signaling and a user plane (GTP-U) for user data. GTP-C is a tunnel control and management protocol and is used to create, modify and delete tunnels. GTP-U is a tunneling mechanism that provides a service for carrying user data packets.

Tunnel Combinations and DHCP Processing

Overview

The table below lists the tunnel combinations for Ruckus and 3rd Party APs.

TABLE 6 Tunnel combinations

AP Type	Access	Core	Authentication				
			Open	Hotspot (WISPr)	802.1X EAP	MAC Address	Hotspot 2.0
Ruckus	RGRE	Bridge (0-2 tags)	X	X	X	X	X
Ruckus	RGRE	L2oGRE	X	X	X	X	X
Ruckus	RGRE	TTG			X		

DHCP Processing

The DHCP relay function data plane relays all UE packets to the controller DHCP server. For Ruckus GRE packets, the outer Ethernet/IP/UDP/GRE headers are stripped to recover the UE packet.

DHCP Relay

DHCP relay is supported for all core network protocol types, when configured. For access network, the DHCP relay supports only L2 access traffic, which includes RuckusGRE, QinQ (L2).

The DHCP relay function is configurable on a per AP zone basis. The controller supports configuration of two DHCP servers per DHCP relay setting where one is in active mode and the other is in standby mode. All DHCP relay traffic will be forwarded to the active DHCP server. Data plane keeps track of the time stamps for DHCP packets sent to or received from the active DHCP server. If the user is unable to see any packets from the DHCP server in the configured time interval, the server is considered as unreachable and subsequent DHCP packets are sent to the standby server. An event is generated to notify the control plane.

For sending to DHCP servers, the DHCP relay agent's IP address is the interface IP address based on the routing table settings. It is the operator's responsibility to set the routes to allow the DHCP server to be reachable. In the controller, a secondary IP address is configurable on the data plane to support sending to DHCP servers, which could be in a private network.

For TTG+PDG traffic, the DHCP function in the data plane will always be active and does not require any configuration.

DHCP Option 82

The following suboptions are configurable:

Suboption 1

Select any one of the following values.

1. IF-Name:VLAN-ID:ESSID:AP-Model:AP-Name:AP-MAC
   where:
   ESSSID is the WLAN SSID
   AP-Model, AP-Name, AP-MAC are included only for Ruckus APs
2. AP-MAC-hex
3. AP-MAC-hex ESSID
4. IF-Name:VLAN-ID:ESSID:AP-Model:AP-Name:AP-MAC:Location
   where AP-Model, AP-Name, AP-MAC, location are included only for Ruckus APs

Suboption 2

Select any of the following values.

1. Client-MAC-hex
2. Client-MAC-hex ESSID
3. AP-MAC-hex
4. AP-MAC-hex ESSID

Suboption -150

This option is with VLAN-ID.

Suboption-151 with format

Select any of the following values.

1. Area name (string as configured by the user)
2. ESSID

Ruckus Wireless, Inc., a wholly owned subsidiary of ARRIS International plc.
350 West Java Dr., Sunnyvale, CA 94089 USA
www.ruckuswireless.com