Ruckus

Simply Better Wireless.

Ruckus Wireless™ SmartCell Gateway™ 200

Tunneling Interface Reference Guide for SmartZone 3.4.1

Part Number 800-71380-001 Rev A
Published July 2016

www.ruckuswireless.com

Copyright Notice and Proprietary Information

Destination Control Statement

Technical data contained in this publication may be subject to the export control laws of the United States of America. Disclosure to nationals of other countries contrary to United States law is prohibited. It is the reader’s responsibility to determine the applicable regulations and to comply with them.

Disclaimer

THIS DOCUMENTATION AND ALL INFORMATION CONTAINED HEREIN (“MATERIAL”) IS PROVIDED FOR GENERAL INFORMATION PURPOSES ONLY. RUCKUS AND ITS LICENSORS MAKE NO WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, WITH REGARD TO THE MATERIAL, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT AND FITNESS FOR A PARTICULAR PURPOSE, OR THAT THE MATERIAL IS ERROR-FREE, ACCURATE OR RELIABLE. RUCKUS RESERVES THE RIGHT TO MAKE CHANGES OR UPDATES TO THE MATERIAL AT ANY TIME.

Limitation of Liability

IN NO EVENT SHALL RUCKUS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGES, OR DAMAGES FOR LOSS OF PROFITS, REVENUE, DATA OR USE, INCURRED BY YOU OR ANY THIRD PARTY, WHETHER IN AN ACTION IN CONTRACT OR TORT, ARISING FROM YOUR ACCESS TO, OR USE OF, THE MATERIAL.

Trademarks

Ruckus Wireless, Ruckus, the bark logo, ZoneFlex, FlexMaster, ZoneDirector, SmartMesh, Channelfly, Smartcell, Dynamic PSK, and Simply Better Wireless are trademarks of Ruckus Wireless, Inc. in the United States and other countries. All other product or company names may be trademarks of their respective owners.

Contents

About This Guide

1 Core Network Protocols

2 3rd Party Access Network Protocol

3 Tunnel Combinations and DHCP Processing

About This Guide

This *Ruckus Wireless™ SmartCell Gateway™ (SCG) 200 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 Wireless devices. Consequently, it assumes a basic working knowledge of local area networks, wireless networking, and wireless devices. .

NOTE If release notes are shipped with your product and the information there differs from the information in this guide, follow the instructions in the release notes.

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

Document Conventions

Table 1 and Table 2 list the text and notice conventions that are used throughout this guide.

Table 1. Text conventions

Convention	Description	Example
`monospace`	Represents information as it appears on screen	`[Device name]>`
`monospace bold`	Represents information that you enter	`[Device name]>` **`set ipaddr 10.0.0.12`**
default font bold	Keyboard keys, software buttons, and field names	On the **Start** menu, click **All Programs**.
italics	Screen or page names	Click **Advanced Settings**. The *Advanced Settings* page appears.

Table 2. Notice conventions

Notice Type	Description
NOTE	Information that describes important features or instructions
CAUTION!	Information that alerts you to potential loss of data or potential damage to an application, system, or device
WARNING!	Information that alerts you to potential personal injury

Terminology

Table 3 lists the terms used in this guide.

Table 3. Terms used in this guide

Term	Description
BRI	Binding Revocation Indication
Control Plane	SCG Control Plane
CVLAN	Customer VLAN
Data Plane	SCG Data Plane
DHCP	Dynamic Host Configuration Protocol (DHCP)
DM	Disconnect Message

Table 3. Terms used in this guide

Term	Description
EPC	Evolved Packet Core
EPS	Evolved Packet System
fwd_policy	Forwarding policy to identify one of the supported network protocol types
G-PDU	GTP Packet Data Unit
GGSN	Gateway GPRS Support Node
GTP	GPRS Tunneling Protocol
ICMP	Internet Control Message Protocol
L2oGRE	Standard GRE (version 0 no options) of Ethernet packets
L2oGRE	Layer 2 over GRE
LBO	Local Breakout Traffic
LMA	Local Mobility Anchor
MAG	Mobile Access Gateway
MAG	Mobile Access Gateway
MN	Mobile Node
PDG	Packet Data Gateway
PDN	Packet Data Network
PGW	PDN Gateway
PMIPv6	Proxy Mobile IPv6
RADIUS	Remote Access Dial-Up User Service
SGW	Serving Gateway
SVLAN	Service VLAN
TEIDs	Tunnel End Point Identifiers
TTG	Tunnel Termination Gateway

References

Table 4 lists the specifications and standards that are referred to in this guide.

Table 4. References used

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

Impacted Systems

Table 5 lists the impacted systems.

Table 5. Impacted Systems

Term	Description
Controlplane	• 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 • ICD Message - Enhancements to support additional forwarding policy • AAA Proxy - Supports additional forward policy – L2oGRE and QinQ
Dataplane	• 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)	Host pad - New forward policy support for L2oGRE

Legend

Table 6 lists the legends used in this guide.

Table 6. Legend used

Legend	Description
M	Mandatory
O	Optional
C	Conditional

Related Documentation

For a complete list of documents that accompany this release, refer to the Release Notes.

Online Training Resources

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

Documentation Feedback

Ruckus Wireless is interested in improving its documentation and welcomes your comments and suggestions. You can email your comments to Ruckus Wireless at:

docs@ruckuswireless.com

When contacting us, please include the following information:

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

For example:

- SmartCell Gateway 200 Tunneling Interface Reference Guide for SmartZone 3.4.1
- Part number: 800-71380-001
- Page 280

Core Network Protocols

1

In this chapter:

Overview

This interface reference guide describes the enhancements that support additional protocols for 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).

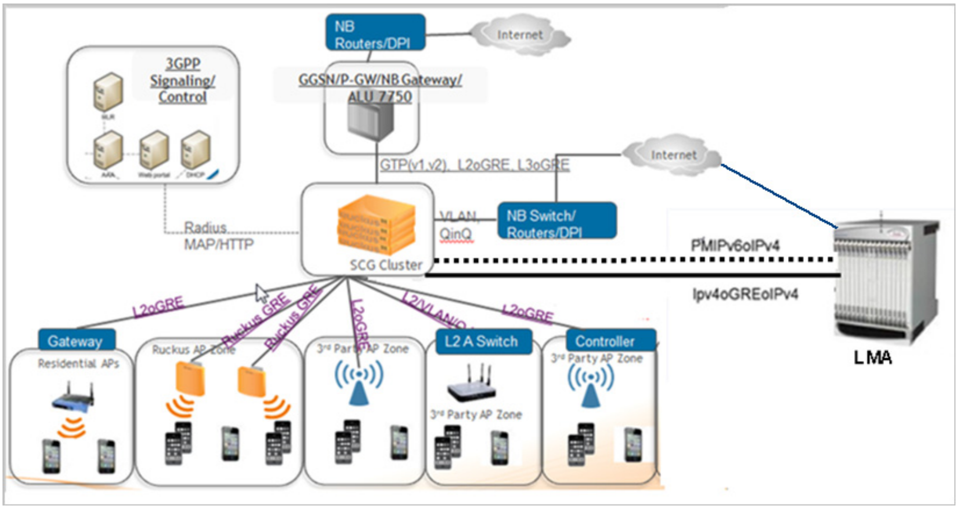
On the core network, UE traffic from APs along with next-hop destinations based on forwarding policy supports:

- 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. In addition, data plane supports in sending non-tunneled packets to the core network with optional VLAN or QinQ tags.
- PMIP tunneling is between the SCG (MAG) and LMA and is per session. The tunneling to carry the payload is IPv4 over GRE over IPv4 type.

On the access network, UE traffic from 3rd Party APs is sent to the data plane via an L2oGRE tunnel, or alternatively a QinQ tunnel configuration on the access network. This is in addition to QinQ packets on the access network. The configuration is per zone with specifications of the IP range of the connecting tunnel endpoint. The tunnel is accepted and the UE packet is accepted (based on per zone authentication settings) as long as the IP address of the GRE tunnel endpoint is within that range.

Figure 1 shows the tunneling interface and its various tunneling interfaces.

Figure 1. Tunneling interface for the SCG



NOTE: Refer to About This Guide for the conventions used in this guide.

Core Network Protocols

Each 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.

This section covers:

- L2oGRE
- L2oGRE with TTG PDG Profile with 802.1x Authentication
- Bridge Mode - (0-2 tags)
- GTP Tunnel with GGSN (GTPv1)
- GTP Tunnel with PGW (GTPv2)
- PMIPv6 Tunnelling

L2oGRE

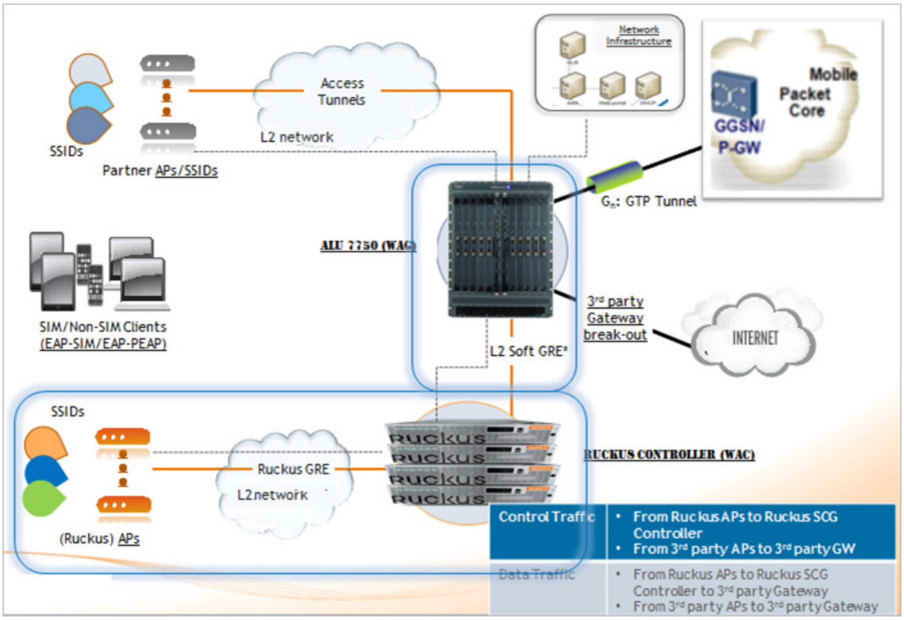
L2oGRE is a core network tunneling protocol, with the following features:

- 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 the 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. Figure 2 displays the L2oGRE traffic flow.

Figure 2. L2oGRE control and data traffic flow.


Network Infrastructure
Mobile Packet Core
GGSN/ P-GW
Access Tunnels
L2 network
SSIDs
Partner APs/SSIDs
ALU 7750 (WAG)
G_n: GTP Tunnel
SIM/Non-SIM Clients (EAP-SIM/EAP-PEAP)
3rd party Gateway break-out
INTERNET
L2 Soft GRE*
SSIDs
Ruckus GRE
L2 network
(Ruckus) APs
RUCKUS CONTROLLER (WAC)
Control Traffic
From Ruckus APs to Ruckus SCG Controller
From 3rd party APs to 3rd party GW
Data Traffic
From Ruckus APs to Ruckus SCG Controller to 3rd party Gateway
From 3rd party APs to 3rd party Gateway

NOTE: For information on how to configure L2oGRE, refer to the *SmartCell Gateway 200 Administrator Guide* (PDF) or the *SmartCell Gateway 200 Online Help*, which is accessible from the SCG Web interface.

L2oGRE with TTG PDG Profile with 802.1x Authentication

This network protocol supports authentication of UE tunnel traffic from 3rd party APs using 802.1X, via L2oGRE tunnels. 3rd party AP UE's using 802.1X authentication is already supported with QinQ access and LBO core forwarding by configuring the TTG+PDG profile.

The UE authentication is similar to QinQ and LBO expects that the UE packet is seen at the data plane from an L2oGRE tunnel. This means that the L2oGRE and LBO path is already supported for the parameter *auth_type*.

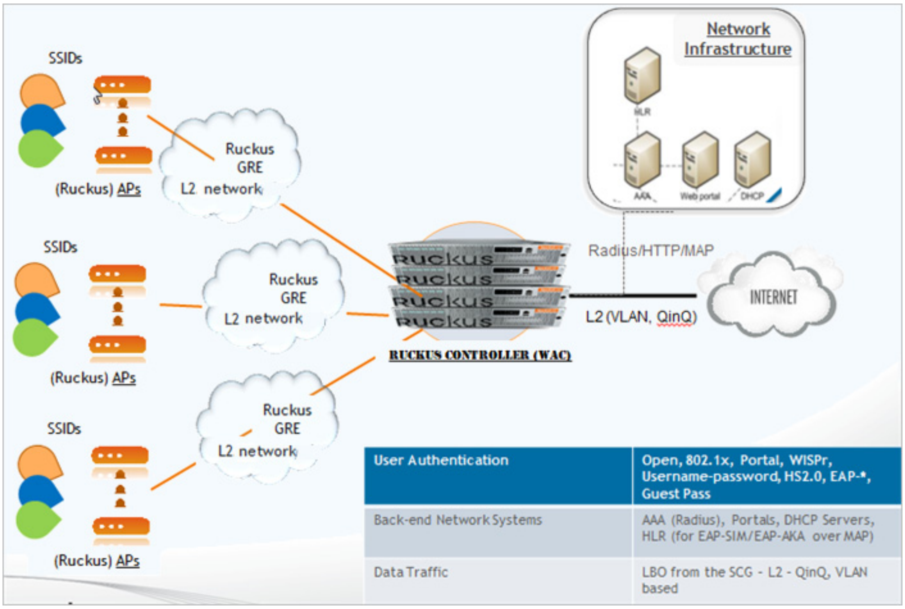
In this particular path, as long as the L2oGRE AP can be mapped to a configured zone (based on IP address range), the UE packet will be accepted and forwarded. The datacore verifies the unknown UE's coming from the AP in the L2oGRE LBO zone before forwarding the UE packets. The following are the UE packet processing steps.

1. UE associated with AP successfully is authenticated through 802.1X.
2. The authenticated UE traffic is sent to data plane through the L2oGRE tunnel.
3. The data blade receives the first UE packet (L2oGRE encapsulated). This could either be the DHCP packet or any other IP packet (roaming to another data plane)
4. If the UE entry is not found, a message to *GTpmgr* is sent about the unknown UE status.
5. *GTpmgr* sends an ICD message (*D-C-DATA-TRIG-MSG*) to the UE using the UE Mac address.
6. The AUT indicates the UE is authenticated with the message *C-D-DATA-TRIG-MSG* (status=22), The UE authentication state will be set to *UE_AUTH_NORMAL*.
7. Subsequent UE packets are bridged out, VLAN/QinQ tagging rules will be as per the configuration.
8. If the UE IP address is later identified, it is tracked through *DHCP ACK*. The AUT will receive a *D-C-NTFY-MSG*, which include the UE IP address.
9. If the UE exists, the data plane UE entry is timed-out and marked as inactive. The *GTpmgr* sends a *D-C-NTFY-MSG* (cause=1) to the AUT notifying the UE timed out event.
10. If the UE returns or moves to another datablade, the status query process for unknown UE is called again.

Bridge Mode - (0-2 tags)

Traffic from UE's are QinQ tagged and bridged out to the core network as seen in Figure 3. The core VLAN type can be either QinQ or preserve the 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



User Authentication	Open, 802.1x, Portal, WISPr, Username-password, HS2.0, EAP-*, Guest Pass
Back-end Network Systems	AAA (Radius), Portals, DHCP Servers, HLR (for EAP-SIM/EAP-AKA over MAP)
Data Traffic	LBO from the SCG - L2 - QinQ, VLAN based

NOTE: For information on how to configure QinQ, refer to the *SmartCell Gateway 200 Administrator Guide* (PDF) or the *SmartCell Gateway 200 Online Help*, which is accessible from the SCG Web 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.

GTP Tunnel with GGSN (GTPv1)

Gn interface is used in controlling the signal between the SCG and GGSN as well as for tunneling end user data payload within the backbone network between both the nodes.

GTP transmits user data packets and signaling between SCG and GGSN. GTP encapsulates traffic and creates GTP tunnels, which act as virtual data channels for transmission of packet data between SCG and GGSN. A GTP tunnel is established between SCG and GGSN through *create PDP context* procedure 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 the GGSN. TEID is a session identifier used by GTP protocol entities in the SGSN and in the GGSN.

The two TEID are defined each for GTP-C and GTP-U. GTP-U is a tunneling mechanism that provides a service for carrying user data packets. On both planes, a GTP header encapsulates the data package, called G-PDU, and a path implemented by UDP/IP is used as bearer of the GTP traffic. GTP-C is a tunnel control and management protocol and is used to create, modify and delete tunnels.

The SCG supports the following categories of GTP signaling traffic:

- Path management messages - The main purpose of these messages is to supervise an UDP/IP path to ensure that connectivity failure can be detected on time. This is managed by frequently sending GTP echo request or response packets between the SCG and the GGSN.
- Tunnel management messages - These contain messages that establish, modify and release GTP tunnels.

Figure 4 shows the message flow between the SCG and the GGSN for establishing a GTP tunnel. Figure 5 shows the Gn interface flow.

Figure 4. Message flow between the SCG and GGSN

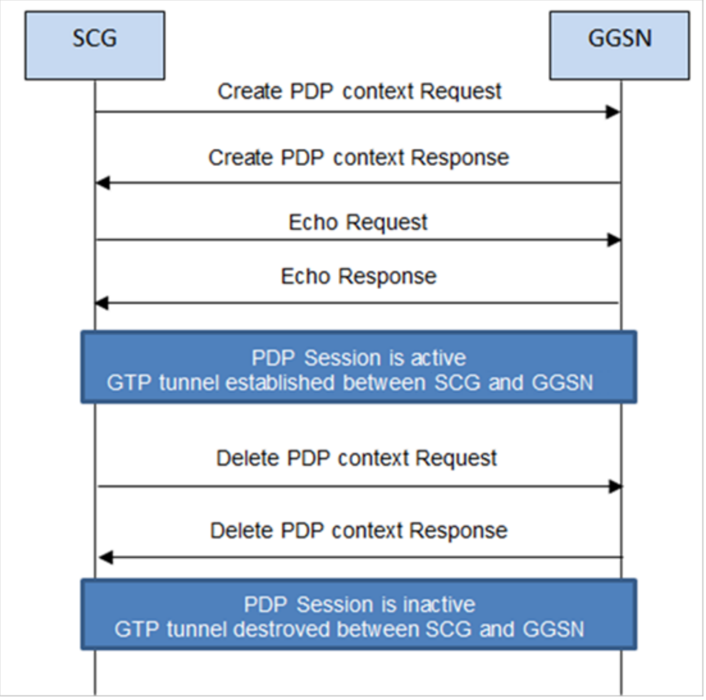
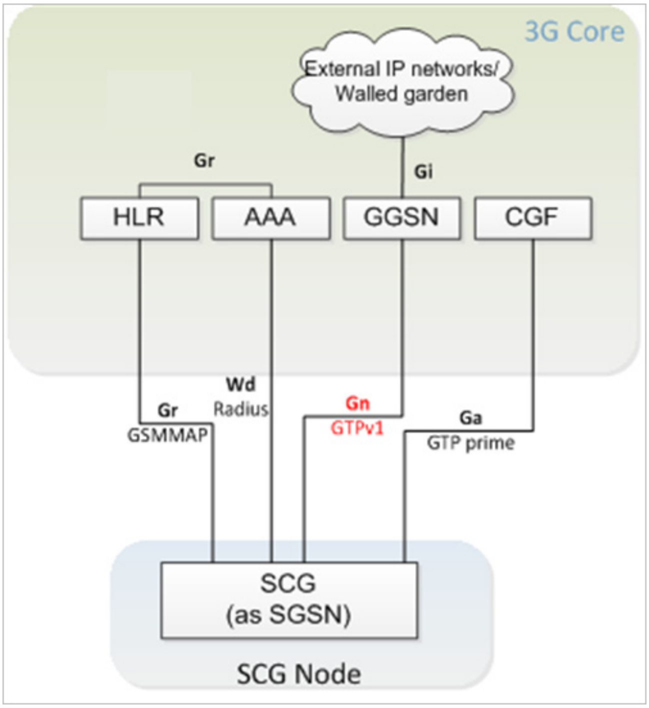

SCG
GGSN
Create PDP context Request
Create PDP context Response
Echo Request
Echo Response
PDP Session is active
GTP tunnel established between SCG and GGSN
Delete PDP context Request
Delete PDP context Response
PDP Session is inactive
GTP tunnel destroved between SCG and GGSN

Figure 5. Gn interface flow



NOTE: For information on tunnel and path messages, refer to the *SmartCell Gateway 200 Gn Interface Reference Guide* (PDF).

GTP Tunnel with PGW (GTPv2)

This is the interface between the SCG with PGW. It is the control plane GPRS tunneling protocol messages v2 for EPS interfaces (GTPv2-C) from the SCG and PGW.

The S2a interface is used in controlling the signal between the SCG and PGW. It also acts as a tunnel for end user data payload within the EPC network.

The GTP transmits user data packets and signaling messages between the SCG and PGW. GTP encapsulates traffic and creates GTP tunnels, which act as virtual data channels. A GTP tunnel is established between the SCG and PGW through *Create Session Request* procedure for a data session initiated from the UE.

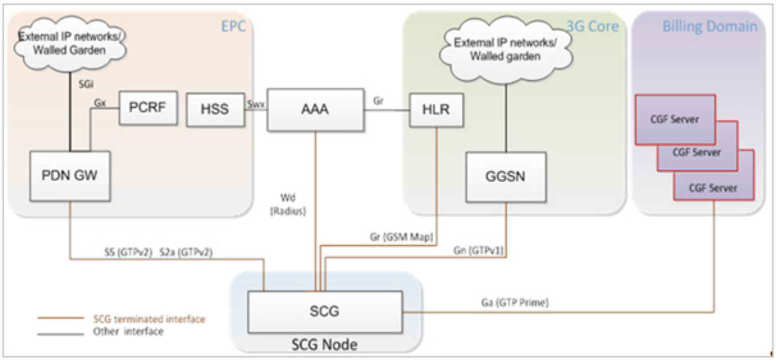
The SCG acts as trusted non-3GPP access network (TWAN) towards PGW with S2a (GTPv2) interface. In case the operator EPC network, does not support the S2a interface, the SCG can be statically configured to support S5 (GTPv2) interface, in which case the SCG acts as serving gateway.

A GTP tunnel is identified by a pair of IP addresses and a pair of GTP TEIDs, where one IP address and TEID is for the SCG (TWAN) and the other is for the PGW. The TEID is a session identifier used by GTP protocol entities in the SCG and in the PGW. 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, which provides a service for carrying user data packets. On both planes, a GTP header encapsulates the data package, called GPDU, and a path implemented by UDP/IP is used as bearer of the GTP traffic. The SCG supports the following categories of GTP signaling traffic:

- Path management messages - The main purpose of these messages is to supervise an UDP/IP path to ensure that connectivity failure can be detected on time. This is managed by frequently sending GTP echo request or response packets between the SCG and PGW.
- Tunnel management messages - These contain messages that establish, modify and release GTP tunnels.

Figure 6 shows the deployment of the SCG in operator networks with 3G and EPC.

Figure 6. Deployment of SCG with 3G and EPC

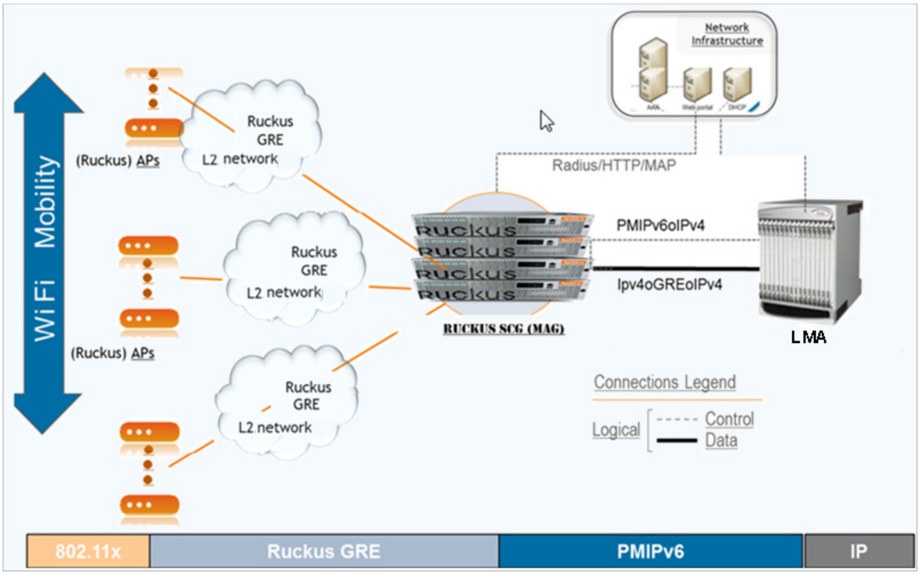


NOTE: For information on tunnel and path messages, refer to the *SmartCell Gateway 200 S2a Interface (GTPCv2, GTP-U v1) Reference Guide* (PDF).

PMIPv6 Tunnelling

Proxy mobile IPv6 is a network based mobility management protocol standardized by IETF and primarily specified in RFC5213. Each data plane in the SCG cluster along with control plane acts as MAG. The Ruckus GRE tunnel between the AP and the data plane is per AP. Figure 7 shows the deployment of the SCG as MAG.

Figure 7. SCG as MAG



Following are the considerations for PMIPv6 support on the SCG.

- The SCG acts as an integrated WLAN controller and MAG
- The signaling transport network between MAG and LMA is PMIPv6 over IPv4-only. The user plane is IPv4 over GRE over IPv4. Future versions of the SCG will support IPv6 or dual stack
- The service offered to mobile node is IPv4 whereby only IPv4 addresses are assigned to the MN
- It is assumed that the LMA supports binding revocation indication procedures. This is required for handling the inter MAG handover procedures
- The SCG maintains heartbeats in terms of Internet control message protocol towards the LMA
- The SCG supports all MN authentication procedures supported over Ruckus APs (for example, Portal, WISPr, 802.1x, EAP-SIM/EAP-AKA/EAP). The SCG setups the PMIP tunnel appropriately on the DHCP trigger and assigns it to the UE IPv4 address as seen in Figure 8 and Figure 9. It then forwards the packets to the LMA.

Figure 8. MN Attach Signalling Call Flow - Open SSID

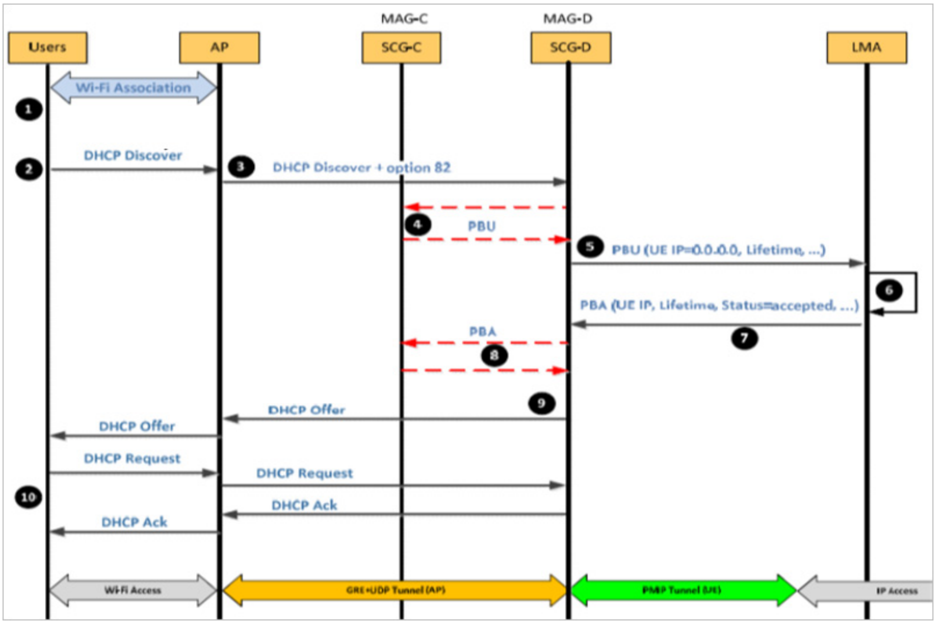
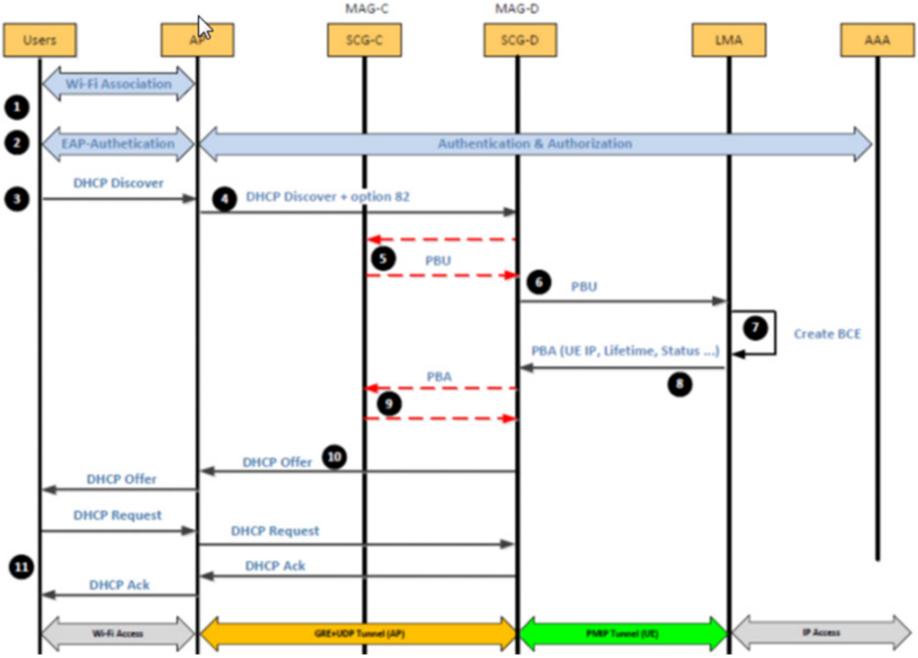


Figure 9. MN Attach Signalling Call Flow - 802.1x



3rd Party Access Network Protocol

2

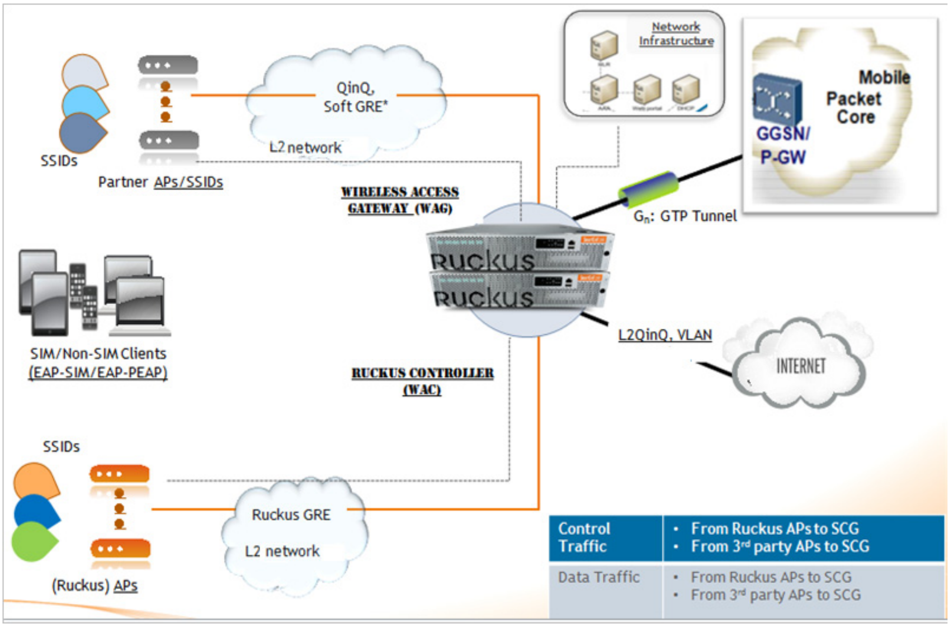
In this chapter:

- 3rd Party AP Zone
- L2oGRE
- QinQ (L2)
- 3rd Party Session Termination

Access Network

The SCG supports two types of access network for 3rd party, namely QinQ and L2oGRE. Figure 10 shows the 3rd party AP flow.

Figure 10. Data traffic from 3rd party AP to the SCG



3rd Party AP Zone

The SCG connects to 3rd party AP zones in the same way as that of Ruckus Wireless APs. The SCG receives RADIUS messages directly from 3rd party AP and supports multiple 3rd party AP zones. The SCG accepts UE data traffic from 3rd party APs from access networks via L2oGRE tunnels APs or QinQ tags. The UE MAC is available from the UE packet.

3rd party APs are managed by 3rd party AP controller, where the SCG acts as WAG. An access network protocol is defined for each 3rd party AP zone. The options are L2oGRE or QinQ. For 3rd party AP zones using L2oGRE access, traffic is accepted from the 3rd party APs using the access network provided to match a configured list of AP address range.

3rd party AP zones can also be configured with QinQ as the access network protocol. For traffic from these zones, the UE packets are QinQ tagged, and the SVLAN/CVLAN tags must match one of the defined ranges of SVLAN/CVLAN configured for that zone. 3rd party AP-Zone to data plane is a 1:1 mapping. No data plane redundancy is offered for 3rd party APs.

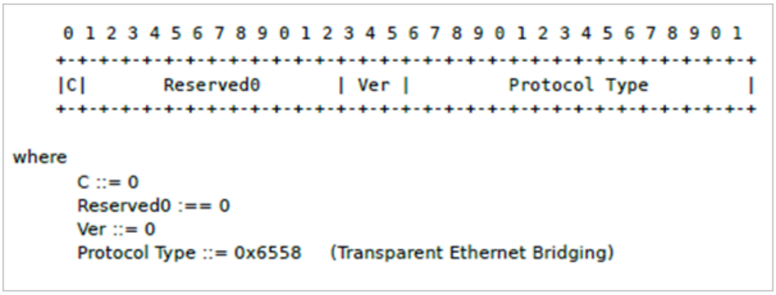
Each 3rd party AP Zone is identified by a list of IP addresses, range, and subnets used by the APs for sending RADIUS traffic to the SCG. A 3rd party AP Zone ID is generated internally for each zone. Authentication and accounting procedures supported are same as Ruckus Wireless APs.

3rd party AP Zone support different northbound tunnels for Ruckus WLAN.

L2oGRE

3rd party AP sends GRE encapsulated packet to the datablade, which has the header form as seen in Figure 11.

Figure 11. L2oGRE header



```
    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |C|       Reserved0       | Ver |         Protocol Type         |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

where
      C ::= 0
      Reserved0 :== 0
      Ver ::= 0
      Protocol Type ::= 0x6558    (Transparent Ethernet Bridging)
```

Ethernet 802.3 packet is the payload from the UE and includes UE MAC. On receiving the datacore, it first verifies if the packets are from the supported APs. An L2oGRE packet does not necessarily come directly from the AP. There could be one or more intermediate routers indicating that the MAC address may not be that of the AP. The IP address is used for identifying the AP.

The attribute *src_ip address* matches and identifies the 3rd party AP zone, which sends the packet and forwards it to the GRE input module for processing. The GRE packet header stores the appropriate information in the packet descriptor. For 3rd party AP packets, it includes AP Zone ID and/or the network traffic profile associated with the AP zone. The GRE input also maintains the AP table, including statistics.

For 3rd party APs, if the attribute, *src_ip address* is within the range, the tunnel is automatically created. It does not require a setup. The AP table is for 3rd party AP only and entries are timed-out periodically based on the in-activity. The complete UE Ethernet packet is passed to the forward packet module, which is responsible for forwarding the packet based on the rules and service policies.

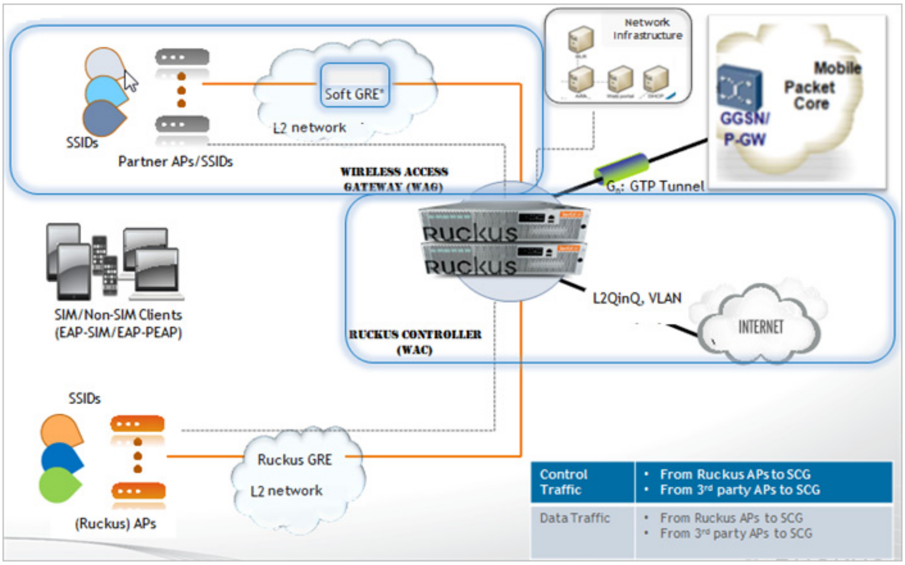
NOTE: For information on how to configure L2oGRE, refer to the *SmartCell Gateway 200 Administrator Guide* (PDF) or the *SmartCell Gateway 200 Online Help*, which is accessible from the SCG Web interface.

L2oGRE and Bridge

In the user interface, the administrator user configures the access network as *L2oGRE* and the core network as *Bridge.*

UE packets from the access network are sent to the data plane inside a layer 2 GRE tunnel. L2oGRE packets with outer source IP within the configured ranges are accepted. The *fwd_policy* in this configuration is to bridge the inner UE packet to the core-side network with 0, 1 or 2 VLAN tags as configured. See Figure 12 for the schematic flow of 3rd party APs using L2oGRE and Bridge.

Figure 12. 3rd party using L2oGRE and Bridge



Control Traffic	• From Ruckus APs to SCG • From 3rd party APs to SCG
Data Traffic	• From Ruckus APs to SCG • From 3rd party APs to SCG

QinQ (L2)

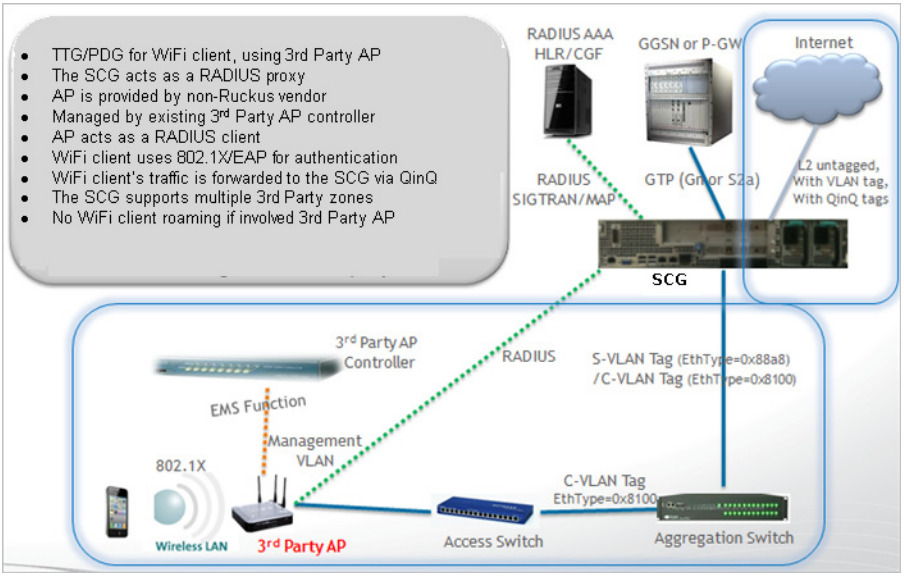
Wi-Fi clients associated with 3rd party AP zones using QinQ access can be configured to be bridged to the core network with 0, 1 or 2 VLAN tags. On the access network, UE traffic from 3rd party APs is sent to the data plane as QinQ tagged packets. The configuration is as per the zone specifying the accepted SVLAN and CVLAN ranges of QinQ tags. The UE packet is accepted (based on per zone authentication settings) provided the QinQ tags of the packet are within the configured range.

In the user interface, when the administrator user configures the *Access Network* as *QinQ* and the *Core Network* as *Bridge,* the SCG acts as the RADIUS proxy and is managed by the AP controller. The AP acts like a RADIUS client and uses 802.1X/ EAP for authentication. The client traffic is forwarded to the SCG via QinQ. The SCG support multiple 3rd party zones.

QinQ is configured per 3rd party AP zone, which accesses UE traffic arriving at the data plane as tagged packets (double VLAN). QinQ access packets are recognized by configuring SVLAN/ CVLAN range in 3rd party AP zone configuration as seen in Figure 13. SVLAN/CVLAN range does not overlap between the zones.

NOTE: The SCG does not support roaming for 3rd party APs.

Figure 13. 3rd party using QinQ and Bridge



- TTG/PDG for WiFi client, using 3rd Party AP
- The SCG acts as a RADIUS proxy
- AP is provided by non-Ruckus vendor
- Managed by existing 3rd Party AP controller
- AP acts as a RADIUS client
- WiFi client uses 802.1X/EAP for authentication
- WiFi client's traffic is forwarded to the SCG via QinQ
- The SCG supports multiple 3rd Party zones
- No WiFi client roaming if involved 3rd Party AP

NOTE: For information on how to configure QinQ, refer to the *SmartCell Gateway 200 Administrator Guide* (PDF) or the *SmartCell Gateway 200 Online Help*, which is accessible from the SCG Web interface.

QinQ and TTG+PDG

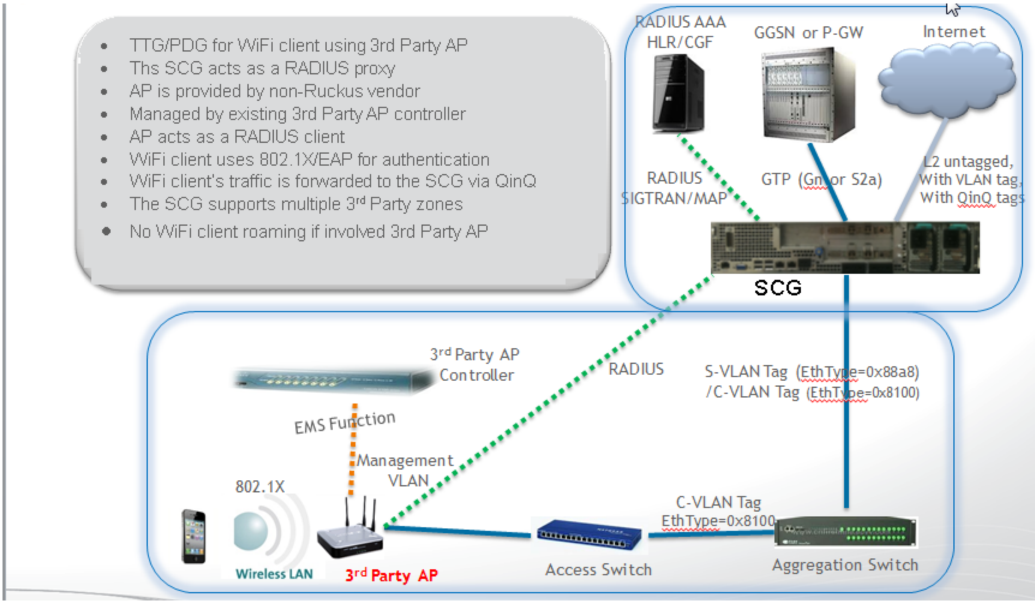
3rd party AP zones can be configured for Wi-Fi client traffic to be sent to the data plane as QinQ tagged packets, which is then forwarded to the core network as per the configuration in the TTG+PDG profile. Wi-Fi client's traffic is forwarded to the SCG using QinQ tags ensuring that UE MAC is present in frames coming from AP into data plane. With the TTG+PDG profile, the *fwd_policy* that will be applied for each UE session is determined during authentication. The *fwd_policy* choices are either TTG (forwarding to a GGSN) or PDG (local break out at the SCG).

In the user interface, when the administrator user configures the access network as *QinQ* and the core network as *TTG+PDG,* the SCG acts as the RADIUS proxy. 3rd party AP acts like a RADIUS client and uses 802.1X/EAP to perform authentication. The client traffic is forwarded to the SCG via QinQ. Figure 14 shows the access flows of 3rd party APs using QinQ and TTG+PDG.

3rd party APs are managed by the 3rd party AP controller. The SCG supports multiple 3rd party zones.

NOTE: The SCG does not support roaming for 3rd party APs.

Figure 14. 3rd party using QinQ and TTG+PDG



- TTG/PDG for WiFi client using 3rd Party AP
- Ths SCG acts as a RADIUS proxy
- AP is provided by non-Ruckus vendor
- Managed by existing 3rd Party AP controller
- AP acts as a RADIUS client
- WiFi client uses 802.1X/EAP for authentication
- WiFi client's traffic is forwarded to the SCG via QinQ
- The SCG supports multiple 3rd Party zones
- No WiFi client roaming if involved 3rd Party AP

3rd Party Session Termination

TTG session termination procedures for UEs associated to 3rd party AP differ from Ruckus APs call flows. In this case, the control plane sends the RADIUS DM message to the AP. When a session is to be terminated (GGSN/HLR/Admin initiated) control plane uses the 3rd party AP's IP address to build and send the RADIUS DM message to the AP.

It is possible that 3rd party AP does not support RADIUS DM or 3rd party APs residing behind a NAT device. During an IP address assignment, the control plane DHCP server provides a finite lease time (for TTG sessions). If the session is deleted in the SCG and the association still exists, all data packets coming from UE are discarded. When UE initiates DHCP renew/rebind procedure, the SCG denies the renewal/rebind. Once this is denied, it automatically disassociates itself and starts a new connection.

In case of PDG session termination, *an age out* event is sent to the control plane. The session also gets terminated, if the UE session ages out or when a session deletes a control plane or the data plane ages out the entry. Alternatively a user can build an API to delete the entry.

Tunnel Combinations and DHCP Processing

3

In this chapter:

Tunnel Combinations

Table 7 lists the tunnel combinations for Ruckus Wireless and 3rd Party APs.

Table 7. 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+PDG (0-2 tags)		X	X		
Ruckus	RGRE	Mixed Tunnel Mode			X		
3rd Party	QinQ	Bridge (0-2 tags)	X	X			
3rd Party	QinQ	TTG+PDG (0-2 tags)			X		
3rd Party	L2oGRE	Bridge (0-2 tags)	X	X			
3rd Party	L2oGRE	TTG+PDG (0-2 tags)			X		

DHCP Processing

DHCP relay processing is automatically enabled if the core forwarding profile is TTG+PDG, which means that user configuration is not required. DHCP server is always - control plane DHCP server.

The DHCP relay function data plane relays all UE packets to the SCG DHCP server. For Ruckus GRE packets, the outer Ethernet/IP/UDP/GRE headers are stripped to recover the UE packet. For 3rd Party AP QinQ access packets, the QinQ tags are removed before the UE DHCP packet is forwarded to the DHCP server.

Control plane verifies whether the UE has been authenticated and if the session is PDG or TTG. If the UE entry is not found, DHCP discover packet is silently dropped. For TTG configuration, the control plane establishes the GTP tunnel to GGSN and sends a DHCP offer with an assigned IP address back to the data plane.The DHCP relay function on the data plane forwards the DHCP reply packets from the DHCP server back to the UE. For UE from Ruckus APs, the DHCP reply packets are sent back via the Ruckus GRE tunnel. For UE from 3rd Party APs, the DHCP reply packet is tagged with the appropriate SVLAN/CVLAN and sent back to the UE.

If the control plane is unable to establish the GTP tunnel to GGSN or if the UE is not authenticated, the control plane silently drops the DHCP discover message.

For PDG configuration, the control plane responds with DHCP NAK including the northbound VLAN tag options used by the data plane, which is forwarded to the DHCP discover on the northbound interface to an external DHCP server. Option 82 conveys this information.

This section covers:

- DHCP Relay
- DHCP Option 82

DHCP Relay

DHCP relay supports GTP traffic and 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 SCG 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. Dataplane keeps track of the timestamps 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 SCG 2.1, 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 server used will always be control plane and does not require any configuration. Also, the DHCP NAK packet sent by the DHCP server indicates that the UE forward policy is PDG.

DHCP Option 82

By default, the DHCP Option 82 Circuit_ID is set with the following information:

- AP_IP:AP_Mac:SVLAN:VLAN:Zone_ID:SSID_string
- SSID_string stands for WLAN SSID
    - For QinQ(L2) access, the SVLAN/VLAN is included in the Circuit_ID sub-option. The AP_IP and AP_MAC fields are NULL.
    - For non-QinQ access, SVLAN field is null and VLAN field includes the VLAN_ID. If the UE packet is VLAN tagged, the AP IP address will always be included. AP MAC is included only for Ruckus APs.
    - The Zone ID field includes the 16-bit Zone ID from the zone config table in hex characters.
- Option 82 D-blade IP includes the data plane's IP and MAC address, which is e separated by a colon. This is the interface address required for sending it to the core GW.

Index

Ruckus®

Simply Better Wireless.

350 West Java Dr. Sunnyvale, CA 94089. USA
www.ruckuswireless.com