Ruckus Wireless™ SmartCell Gateway200/SmartZone 300

KPI and Report Reference Guide for SmartZone 3.5.1

Part Number: 800-71528-001 Rev A
Published: 16 June 2017

www.ruckuswireless.com

Contents

1 Key Performance Indicators

2 Reports

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.

About this Guide

This *SmartCell Gateway™ 200* (SCG200) / *SmartZone™ 300 (SZ300)KPI and Report Reference Guide* provides a number of statistics, graphs, and reports that you can use to establish key performance indicators (KPIs) for the network.

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   This guide assumes that the SmartCell Gateway has already been installed as described in the *Getting Started Guide*.

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: Text conventions on page 5 and Table 2: Notice conventions on page 6 list the text and notice conventions that are used throughout this guide.

Table 1: Text conventions

Convention	Description	Example
`message phrase`	Represents information as it appears on screen	`[Device Name] >`

`user input`	Represents information that you enter	`[Device Name] >`
		`set ipaddr 10.0.0.12`

user interface controls	Keyboard keys, software buttons, and field names	Click **Start** > **All Programs**
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

The table lists the terms used in this guide.

Table 3: Terms used in this guide

Terminology	Description
AAA	Authentication, Authorization, and Accounting
AAR	AA Request
AP	Access Point
APN	Access Point Name
ASA	Abort Session Answer
ASR	Abort Session Request
BRA	Binding Revocation Acknowledgment
BRI	Binding Revocation Indicator
CEA	Capability-Exchange Answer
CER	Capacity Exchange Request
CGF	Charging Gateway Function
COA	Change of Authorization
DEA	Diameter EAP Answer
DER	Diameter EAP Request
DHCP	Dynamic Host Configuration Protocol
DM	Dynamic Multipoint
DP	Data Plane

Terminology	Description
DPA	Disconnect Peer Answer
DPR	Disconnect Peer Request
DRT	Data Record Transfer
GGSN	Gateway GPRS Support Node
GRE	Generic Route Encapsulation
GSN	GPRS Support Node
GTP-C	GPRS Tunneling Protocol – Control Plane
HLR	Home Location Register
KPI	Key Performance Indicators
LMA	Local Mobility Anchor
NAS	Network Access Server
PBA	Proxy Binding Acknowledgment
PBU	Proxy Binding Update
PDG	Packet Data Gateway
PDP	Packet Data Protocol
PGW	Packet Data Network Gateway
PMIP	Proxy Mobile IPv6
RADIUS	Remote Authentication Dial-In User Service
RAR	Re-Auth Request
SCG	Smart Cell Gateway
SCG-CBlade	SCG Controller Blade
SCG-DBlade	SCG Data Blade
SG	Service Gateway
SNMP	Simple Management Network Protocol
SSID	Service Set Identifiers
STA	Session Termination Answer
STR	Session Termination Request
TCP	Transmission Control Protocol
TTG	Tunnel Termination Gateway
UE	User Equipment

Terminology	Description
UE-IP	User Equipment - IP Address
UE-MAC	User Equipment - MAC Address
VLAN	Virtual LAN
WLAN	Wireless LAN

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:
  - KPI and Report Reference Guide for SmartZone 3.5.1
  - Part number: 800-71528-001
  - Page 88

Key Performance Indicators 1

Overview

The SCG200 / SZ300 (referred as controller in this guide) provides a number of statistics, graphs, and reports that you can use to establish Key Performance Indicators (KPIs) for the network. You can use these KPIs to determine, among others, the quality of wireless service that users are getting, the overall health of the controller system, and any issues that may impact the controller managed devices and, consequently, the network.

NOTE Refer to About this Guide on page 5 chapter for terminologies used in this guide.

KPIs under the Access Points Tab

The following sections describe the various key performance indicators that the controller provides in the **Access Points** tab.

NOTE For information on *Rogue Access Points Alarms and Events* refer to the *Administrator Guide for SmartZone* (PDF) or the *SmartZone* Online Help, which is accessible from the controller web interface.

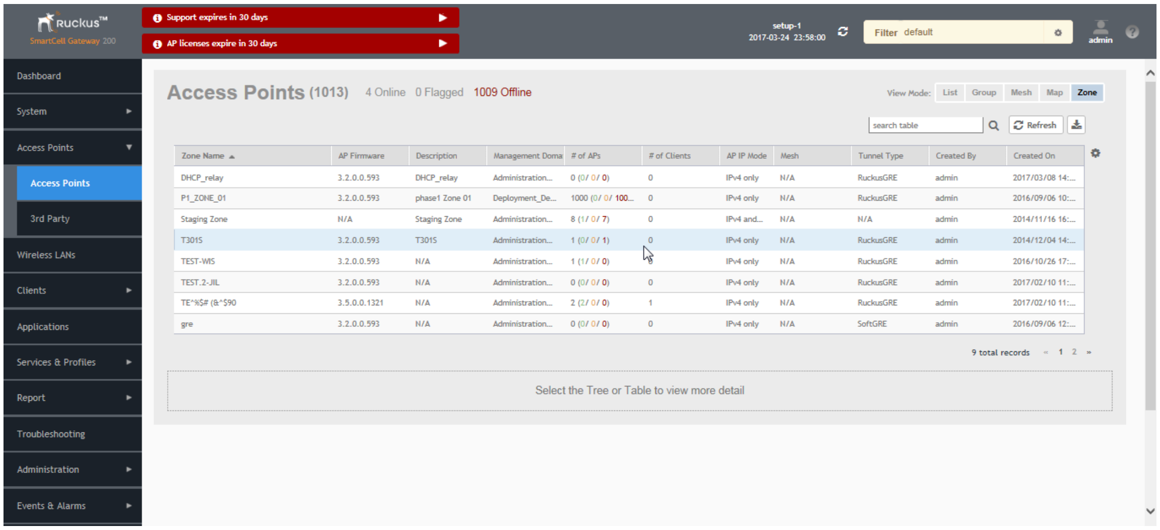
Access Point Zone

An AP zone functions as a way of grouping Ruckus Wireless APs and applying a particular set of settings (including WLANs and their settings) to these groups of Ruckus Wireless APs. By default, an AP zone named *staging zone* exists. Any AP that registers with the controllerr that is not assigned a specific zone is automatically assigned to the staging zone. Each AP zone can include up to 2048 WLAN services.

Navigate to **Access Points** > **Access Points** > **View Mode** > **Zone** to view the access point zone KPIs. The below table lists the key performance indicators for statistics related to the AP zones.

NOTE For information on configuring AP Zone, refer to the *SmartCell Gateway 200 Administrator Guide* (PDF) or the *SmartCell Gateway 200 Online Help*, which is accessible from the controller web interface.

Figure 1: KPIs for AP Zone



Support expires in 30 days

AP licenses expire in 30 days

Access Points (1013) 4 Online 0 Flagged 1009 Offline

Zone Name ▲	AP Firmware	Description	Management Doma	# of APs	# of Clients	AP IP Mode	Mesh	Tunnel Type	Created By	Created On
DHCP_relay	3.2.0.0.593	DHCP_relay	Administration...	0 (0/ 0/ 0)	0	IPv4 only	N/A	RuckusGRE	admin	2017/03/08 14:...
P1_ZONE_01	3.2.0.0.593	phase1 Zone 01	Deployment_De...	1000 (0/ 0/ 100...	0	IPv4 only	N/A	RuckusGRE	admin	2016/09/06 10:...
Staging Zone	N/A	Staging Zone	Administration...	8 (1/ 0/ 7)	0	IPv4 and...	N/A	N/A	admin	2014/11/16 16:...
T301S	3.2.0.0.593	T301S	Administration...	1 (0/ 0/ 1)	0	IPv4 only	N/A	RuckusGRE	admin	2014/12/04 14:...
TEST-WIS	3.2.0.0.593	N/A	Administration...	1 (1/ 0/ 0)	0	IPv4 only	N/A	RuckusGRE	admin	2016/10/26 17:...
TEST.2-JIL	3.2.0.0.593	N/A	Administration...	0 (0/ 0/ 0)	0	IPv4 only	N/A	RuckusGRE	admin	2017/02/10 11:...
TE^%$# (&^$90	3.5.0.0.1321	N/A	Administration...	2 (2/ 0/ 0)	1	IPv4 only	N/A	RuckusGRE	admin	2017/02/10 11:...
gre	3.2.0.0.593	N/A	Administration...	0 (0/ 0/ 0)	0	IPv4 only	N/A	SoftGRE	admin	2016/09/06 12:...

9 total records « 1 2 »

Select the Tree or Table to view more detail

Table 4: KPIs for AP zone

KPI	Description
Zone Name	Indicates the name of the zone.
AP Firmware	Indicates the firmware version that is installed on the access point.
Description	Indicates a short note of the AP zone.
Management Domain	Indicates the management domain to which the zone belongs.
# of APs	Total number of APs that belong to each AP zone.
# of Clients	Total number of clients that belong to each AP zone.
AP IP Mode	Indicates the IP version.
Mesh	Total number of APs per mesh role. Mesh roles include Root AP, Mesh AP, and eMesh AP.
Tunnel Type	Indicates the tunnel type used.
Created By	Indicates the role that created the entry.
Created On	Indicates the date and time when the entry was created.

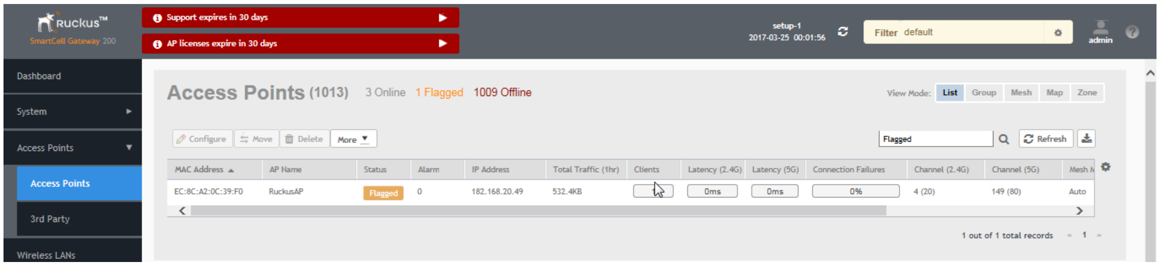
Access Point

Once you have created registration rules and the AP zones, APs can be assigned automatically. APs will be able to join or register with the controller automatically.

To view the KPIs, navigate to **Access Points** > **Access Point** > **View Mode** > **List**. The below table lists the key performance indicators for statistics related to access points.

NOTE For information on configuring Access Points, refer to the *Administrator Guide for SmartZone* (PDF) or the *SmartZone Online Help*, which is accessible from the controller web interface.

Figure 2: KPIs for Access Points



MAC Address	AP Name	Status	Alarm	IP Address	Total Traffic (1hr)	Clients	Latency (2.4G)	Latency (5G)	Connection Failures	Channel (2.4G)	Channel (5G)	Mesh M
EC:8C:A2:0C:39:F0	RuckusAP	Flagged	0	182.168.20.49	532.4KB		0ms	0ms	0%	4 (20)	149 (80)	Auto

Table 5: KPIs for access points

KPI	Description
MAC Address	Indicates the MAC address of the access point.
AP Name	Indicates the access point name.
Description	Indicates a short note of the AP.
Status	Indicates whether the access point is currently connected (online), disconnected (offline) or flagged.
Alarm	Indicates the total number of alarms generated on managed APs.
IP Address	Indicates the IP address of the access point.
Total Traffic (1hr)	Indicates the volume of traffic for the last 1 hour.
Clients	Indicates the number of clients connected to the access point.
Clients (2.4G)	Indicates the number of clients connected to the access point with 2.4G radio channel frequency.
Clients (5G)	Indicates the number of clients connected to the access point with 5G radio channel frequency.

KPI	Description
Latency (2.4G)	Indicates the average delay required to successfully deliver a Wi-Fi with 2.4G radio channel frequency.
Latency (5G)	Indicates the average delay required to successfully deliver a Wi-Fi with 5G radio channel frequency.
Airtime Utilization (2.4G)	Indicates airtime availability, which measures the total amount of airtime currently being used by tx, rx, or non-Wi-Fi interference.
Airtime Utilization (5G)	Indicates airtime availability, which measures the total amount of airtime currently being used by tx, rx, or non-Wi-Fi interference.
Connection failures	Indicates the percentage of AP-client connection attempts that failed.
Model	Indicates the AP model.
Channel (2.4G)	Indicates the 2.4G radio channel frequency.
Channel (5G)	Indicates the 5G radio channel frequency.
Mesh Mode	Indicates the mesh mode type.
Mesh Role	Indicates if the role is enabled or disabled.
Zone	Indicates the zone to which the access point belongs.
AP Group	Indicates the AP group to which the access point belongs.
External IP:Port	Indicates the external IP address.
AP Firmware	Indicates the firmware version installed on the access point.
Serial	Indicates the serial number.
Configuration Status	Indicates the status of configuration settings.
Last Seen	Indicates the date and time.
Traffic (uplink)	Indicates the uplink traffic.
Traffic (downlink)	Indicates the downlink traffic.
Location	Indicates the location of the AP.
WLAN Group (2.4G)	Indicates the 2.4G WLAN group.
WLAN Group (5G)	Indicates the 5G WLAN group.
Bonjour Gateway	Indicates if bonjour gateway service is enabled or disabled.
Control Plane	Indicates the control plane.
Data Plane	Indicates the data plane.

KPI	Description
LBS Status	Indicates location-based service support.
Administrative State	Indicates if the administrative state.
Registration State	Indicates if the registration is approved.
Provision Method	Indicates if the AP is discovered.
Provision Stage	Indicates the state of provision.
Registered On	Indicates the date and time the AP is registered.
Management VLAN	Indicates the number of VLANs.

KPI under the Clients Tab

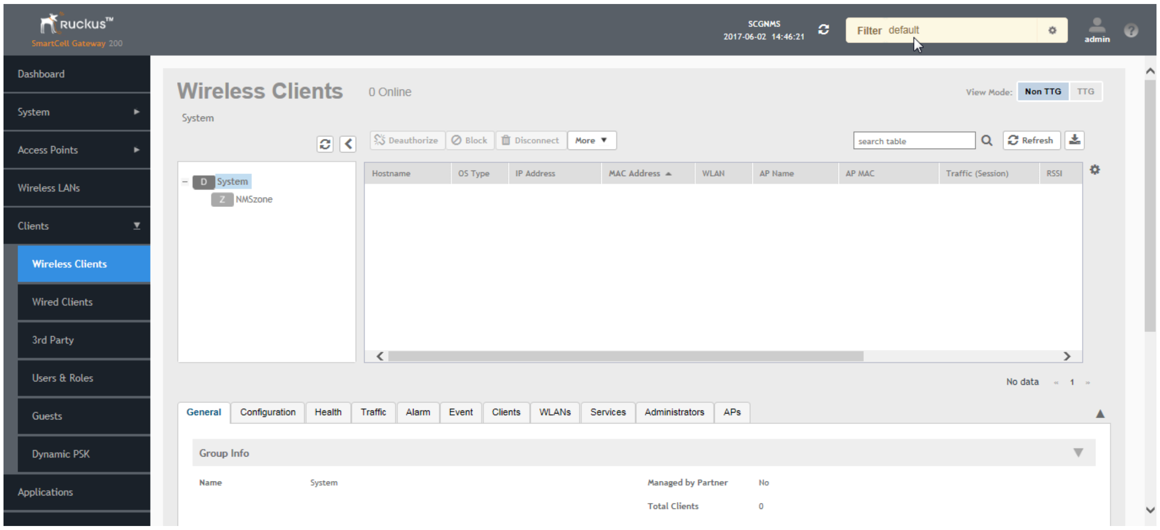
The following section describes the various key performance indicators that the controller provides in the **Clients** tab.

Wireless Clients KPI

To view the KPIs, navigate to **Clients** > **Wireless Clients**. See Table 6: KPIs for Wireless Clients on page 14 that lists the key performance indicator for statistics related to wireless clients.

NOTE For information on configuring Clients, refer to the *Administrator Guide for SmartZone* (PDF) or the *SmartZone Online Help*, which is accessible from the controller's web interface.

Figure 3: KPIs for Wireless Clients



Name: System
Managed by Partner: No
Total Clients: 0

The following table lists the wireless client details that are shown in the table.

Table 6: KPIs for Wireless Clients

KPI	Description
Host Name	Displays the hostname of the wireless client
OS Type	Displays the operating system that the wireless client is using
IP Address	Displays the operating system that the wireless client is using
MAC Address	Displays the MAC address of the wireless client
WLAN	Displays the name of the WLAN with which the client is associated
AP Name	Displays the name assigned to the access point
AP MAC	Displays the MAC address of the AP
Traffic (Session)	Displays the total traffic (in KB/MB/GB/TB) for this client in this session
Traffic (uplink)	Displays the total uplink traffic (in KB/MB/GB/TB) for this client in this session
Traffic (downlink)	Displays the total downlink traffic (in KB/MB/GB/TB) for this client in this session

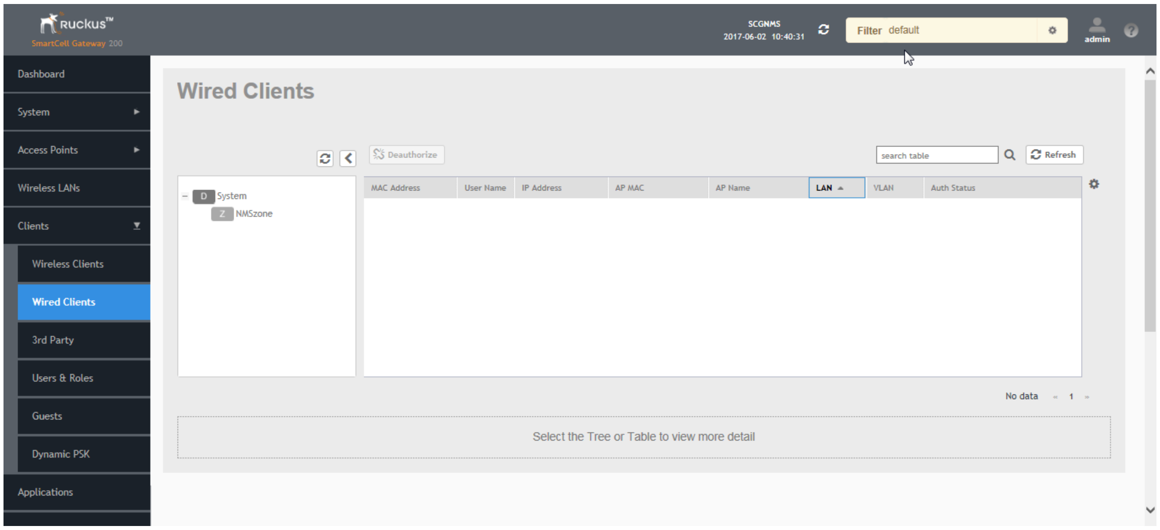
KPI	Description
RSSI	Displays the Received Signal Strength Indicator (RSSI), which indicates how well a wireless client can receive a signal from an AP. The RSSI value is shown in decibels (dB) and displayed as either the real-time value or the average value over the past 90 seconds.
SNR	Displays the Signal-to-Noise Ratio (SNR), which indicates the signal strength relative to background noise. The SNR value is shown in decibels (dB) and displayed as either the real-time value or the average value over the past 90 seconds.
Radio Type	Displays the type of wireless radio that the client supports. Possible values include 11b, 11g, 11g/n, 11a, 11a/g/n, and 11ac.
VLAN	Displays the VLAN ID assigned to the wireless client
Channel	Displays the wireless channel (and channel width) that the wireless client is using
User Name	Displays the name of the user logged on to the wireless client
Data Rate (up)	Displays the rate at which data is transmitted from the wireless client to the AP
Data rate (down)	Displays the rate at which data is transmitted from the AP to the wireless client
Auth Method	Displays the authentication method used by the AP to authenticate the wireless client
Auth Status	Indicates whether the wireless client is authorized or unauthorized to access the WLAN service
Encryption	Displays the encryption method used by the AP
Control Plane	Displays the name of SmartZone node to which the AP's control plane is connected
Packets To	Displays the downlink packet count for this session
Packets from	Displays the uplink packet count for this session
Packets dropped	Displays the downlink packet count for this client that have been dropped
Session start time	Displays the session start date and time.

Wired Clients KPI

To view the KPIs, navigate to **Clients** > **Wired Clients**. See Table 7: KPIs for Wired Clients on page 16 that lists the key performance indicator for statistics related to wired clients.

NOTE For information on configuring Clients, refer to the *Administrator Guide for SmartZone* (PDF) or the *SmartZone Online Help*, which is accessible from the controller's web interface.

Figure 4: KPIs for Wired Clients



The following table lists the wired client details that are shown in the table.

Table 7: KPIs for Wired Clients

KPI	Description
MAC Address	Displays the MAC address of the wired client
User Name	Displays the name of the user logged on to the wire client
IP Address	Displays the IP address assigned to the wired client
AP MAC	Displays the MAC address of the AP
AP Name	Displays the name assigned to the access point
LAN	Displays the LAN ID assigned to the wired client
VLAN	Displays the VLAN ID assigned to the wired client

KPI	Description
Auth Status	Indicates whether the wired client is authorized or unauthorized to access the WLAN service

KPI under the System Tab

The following section describes the various key performance indicators that the controller provides in the **System** tab.

System KPIs

The System KPI status or usage can be viewed for time period (8 hours to 30 days). The system includes CPU, memory, tunnel statistics and disk usage.

To view the KPIs, navigate to **System** > **Cluster** > **Control Plane** > **Traffic & Health**. Table 8: KPIs for the system on page 18 lists the key performance indicators for statistics related to the system.

Figure 5: KPIs for System

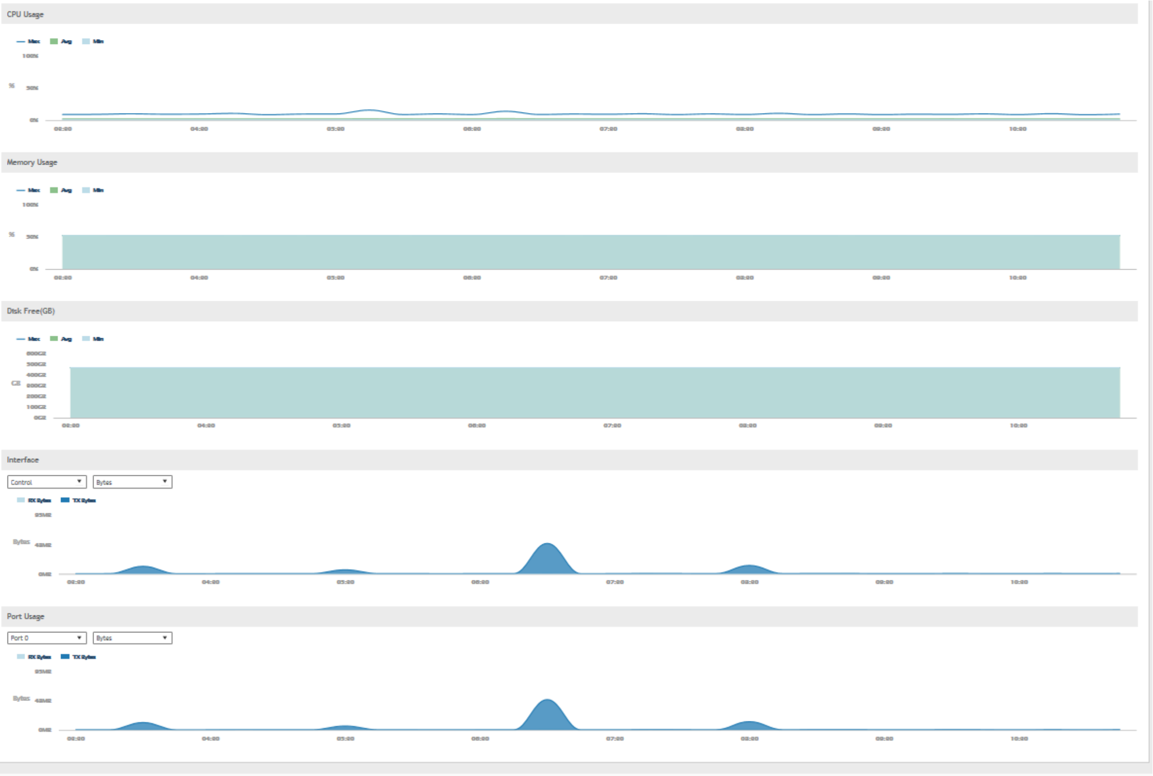


Table 8: KPIs for the system

KPI	Description
CPU status	CPU/memory/disk free usage/interface usage/ are available for 8 hours, 24 hours, 7days and 30 days.
Memory status	CPU/memory/disk free usage/interface usage/ are available for 8 hours, 24 hours, 7days and 30 days.
Disk Free (GB)	Indicates the percentage of free disk space on the controller's web interface.
Interface usage	Indicates • The Tx and Rx bytes on the control, cluster, and management interfaces for the last 15 minutes, hourly, daily or monthly. • The amount of packets (including Tx, Rx, Tx dropped, and Rx dropped) on the control, cluster, and management interfaces for the last 15 minutes, hourly, daily or monthly. • The amount of Tx and Rx bits on the control, cluster, and management interfaces per second.
Port usage	Indicates • The Tx and Rx bytes on the port 0 - port 5 for the last 8 hours to 30 days. • The amount of packets (including Tx, Rx, Tx dropped, and Rx dropped) on the port0 - port5 for the last 8 hours to 30 days. • The amount of Tx and Rx bits on the control, cluster, and management interfaces per second.

KPIs under the Diagnostics Tab

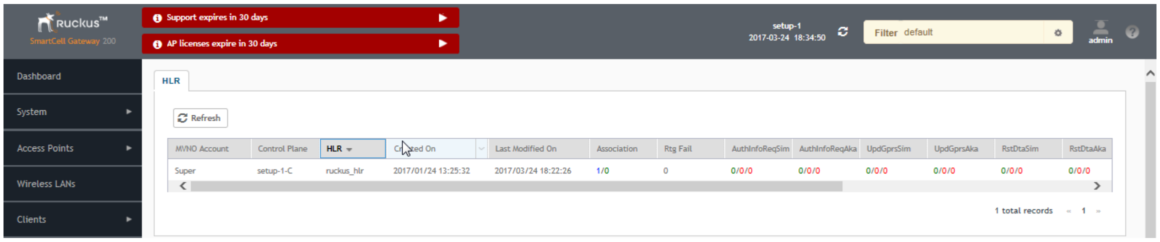
HLR Statistics

The controller and multiple HLRs manage wireless services gateway for authentication/ authorization and for unsolicited change of authorization. To view the KPIs, navigate to **Diagnostics** > **HLR**.

The following table lists the key performance indicators based on the statistics received or sent from the HLR.

NOTE For information on configuring HLR Service, refer to the Administrator Guide for SmartZone (PDF) or the SmartZone Online Help, which is accessible from the controller's web interface.

Figure 6: HLR statistic



Support expires in 30 days

AP licenses expire in 30 days

setup-1
2017-03-24 18:34:50

MVNO Account	Control Plane	HLR	Created On	Last Modified On	Association	Rtg Fail	AuthInfoReqSim	AuthInfoReqAka	UpdGprsSim	UpdGprsAka	RstDtaSim	RstDtaAka
Super	setup-1-C	ruckus_hlr	2017/01/24 13:25:32	2017/03/24 18:22:26	1/0	0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0

1 total records « 1 »

Table 9: KPIs for HLR

KPI	Description
MVNO Account	Indicates the mobile virtual network operator account..
Control Plane	Indicates the control plane name.
HLR	Indicates the Home Location Register.
Created On	Indicates created date and time.
Last Modified On	Indicates last modified date and time.
Association	Indicates the number of associations configured / number of active associations.
Rtg Fail	Indicates the reported routing failure on outbound MAP messages (*TC_Notice*).

KPI	Description
AuthInfoReqSim	Indicates the *MAP-SEND-AUTH-INFO-REQ SIM* (successful / error response from HLR / no response from HLR).
AuthInfoReqAka	Indicates the *MAP-SEND-AUTH-INFO-REQ AKA* (successful / error response from HLR / no response from HLR).
UpdGprsSim	Indicates the *MAP-GPRS-UPDATE-LOCATION-REQ SIM* (successful / error response from HLR / no response from HLR).
UpdGprsAka	Indicates the *MAP-GPRS-UPDATE-LOCATION-REQ AKA* (successful / error response from HLR / no response from HLR).
RstDtaSim	Indicates the *MAP-RESTORE-DATA SIM* (successful / error response from HLR / no response from HLR).
RstDtaAka	Indicates the *MAP-RESTORE-DATA AKA* (successful / error response from HLR / no response from HLR).
InsrtDtaSim	Indicates the *MAP-INSERT-SUBSCRIBER-DATA SIM* (successful / failed).
InsrtDtaAka	Indicates the *MAP-INSERT-SUBSCRIBER-DATA AKA* (successful / failed).
SaInsrtDta	Indicates the *MAP-INSERT-SUBSCRIBER-DATA* (received / unknown subscriber / decode failure or any other error).
RemoteDelSubsData	Indicates the *MAP-DEL-SUBS-DATA-REQ* (successful / failed).
RemoteCanLoc	Indicates the *MAP-CANCEL-LOC-REQ* (successful / failed).

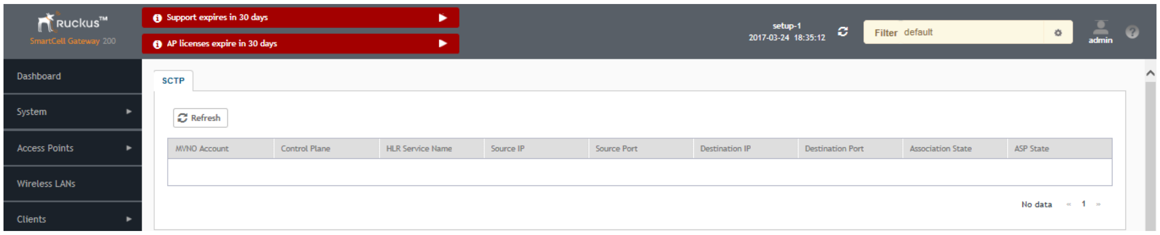
SCTP Associations

An HLR instance can be accessed via one or more SCTP association. One SCTP association can have a connection to one or more HLRs. To view the KPIs, navigate to **Diagnostics** > **SCTP**.

The below table lists the key performance indicators based on the statistics received or sent from the SCTP to the HLR.

NOTE For information on configuring SCTP, refer to the *Administrator Guide for SmartZone* (PDF) or the *SmartZone Online Help*, which is accessible from the controller's web interface.

Figure 7: SCTP association



Support expires in 30 days

AP licenses expire in 30 days

setup-1
2017-03-24 18:35:12

MVNO Account	Control Plane	HLR Service Name	Source IP	Source Port	Destination IP	Destination Port	Association State	ASP State

No data « 1 »

Table 10: SCTP association

KPI	Description
MVNO Account	Indicates the mobile virtual network operator account.
Control Plane	Indicates the control plane name.
HLR Service Name	Indicates the Home Location Register service name.
Source IP	Indicates the SCTP sender's port number.
Source Port	Indicates the SCTP sender’s source port.
Destination IP	Indicates the destination IP address for identifying the association, to which the packet belongs.
Destination Port	Indicates the SCTP destination port.
Association State	Indicates the state of the SCTP association. Value 1 indicates it as established and value 2 indicates closure.
ASP State	Indicates the ASP state. Value 1 indicates active mode, value 2 indicates inactive mode and value 3 indicates a downlink.

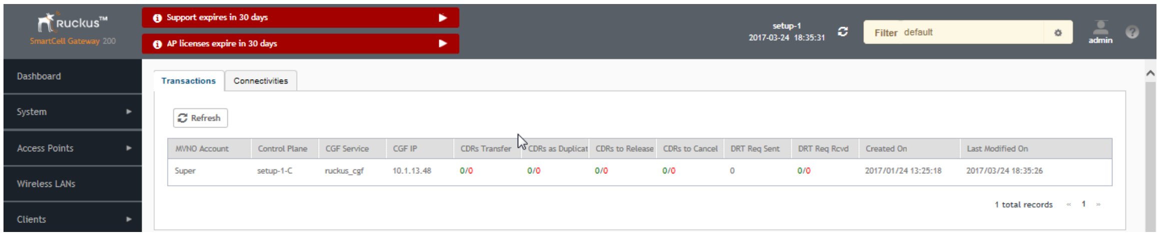
CGF Transactions

The controller plays the CTF role of collecting the chargeable event information for TTG sessions (that is, sessions toward GGSN/PGW). The CGF (Charging Data Functions) service receives the CDR generated at the controller, based on configurations. To view the KPIs, navigate to **Diagnostics** > **CGF** > **Transactions**.

The below table lists the key performance indicators for CGF transaction statistics based on the request and response messages that the CDR transfers.

NOTE For information on configuring CGF Service, refer to the *Administrator Guide for SmartZone* (PDF) or the *SmartZone Online Help*, which is accessible from the controller's web interface.

Figure 8: CGF transactions



MVNO Account	Control Plane	CGF Service	CGF IP	CDRs Transfer	CDRs as Duplicat	CDRs to Release	CDRs to Cancel	DRT Req Sent	DRT Req Rcvd	Created On	Last Modified On
Super	setup-1-C	ruckus_cgf	10.1.13.48	0/0	0/0	0/0	0/0	0	0/0	2017/01/24 13:25:18	2017/03/24 18:35:26

1 total records « 1 »

Table 11: KPIs for CGF Transaction

KPI	Description
MVNO Account	Indicates the mobile virtual network operator account.
Control Plane	Indicates the control plane name.
CGF Service	Indicates the CGF service name.
CGF IP	Indicates the CGF server IP.
CDRs Transfer	Indicates the number of CDRs transferred to the CGF server (successful / failed).
CDRs as Duplicate	Indicates the number of CDRs sent as possible duplicate (successful / failed).
CDRs to Release	Indicates the number of CDRs that the controller wants the CGF server to release (successful / failed).
CDRs to Cancel	Indicates the number of CDRs that the controller wants the CGF server to cancel (successful / failed).
DRT Req Rcvd	Indicates the number of data record transfer responses received (successful / failed).

KPI	Description
DRT Req Sent	Indicates the number of data record transfer requests sent.
Created On	Indicates the date and time the service was created.
Last Modified On	Indicates the date and time the service was last modified.

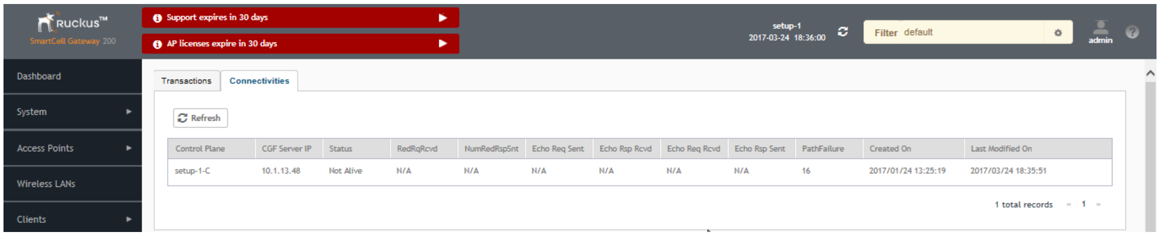
CGF Connectivities

CGF Connectivities is related to management messages. It checks the connectivity of the node and sends the echo and node alive requests. To view the KPIs, navigate to **Diagnostics** > **CGF** > **Connectivities**.

The below table lists the key performance indicators related to the connectivity between the controller and CGF for management messages.

NOTE For information on configuring CGF Connectivities, refer to the *Administrator Guide for SmartZone* (PDF) or the *SmartZone Online Help*, which is accessible from the controller's web interface.

Figure 9: CGF connectivity



Control Plane	CGF Server IP	Status	RedRqRcvd	NumRedRspSnt	Echo Req Sent	Echo Rsp Rcvd	Echo Req Rcvd	Echo Rsp Sent	PathFailure	Created On	Last Modified On
setup-1-C	10.1.13.48	Not Alive	N/A	N/A	N/A	N/A	N/A	N/A	16	2017/01/24 13:25:19	2017/03/24 18:35:51

1 total records « 1 »

Table 12: KPIs for CGF connectivity

KPI	Description
Control Plane	Indicates the control plane name.
CGF Server IP	Indicates the CGF server IP.
Status	Indicates the status, for example: alive or not alive.
RedRqRcvd	Indicates the number of redirection requests received by the controller from CGF.
NumRedRspSnt	Indicates the number of redirection responses sent by the controller to CGF.

KPI	Description
Echo Req Sent	Indicates the number of echo requests initiated by the controller towards CGF.
Echo Rsp Rcvd	Indicates the number of echo responses received by the controller from CGF.
Echo Req Rcvd	Indicates the number of echo requests initiated by CGF towards the controller.
Echo Rsp Sent	Indicates the number of echo responses received by CGF from the controller.
Path Failure	Indicates the number of times the CGF server was unreachable.
Created On	Indicates the date and time the service was created.
Last Modified On	Indicates the date and time the service was last modified.

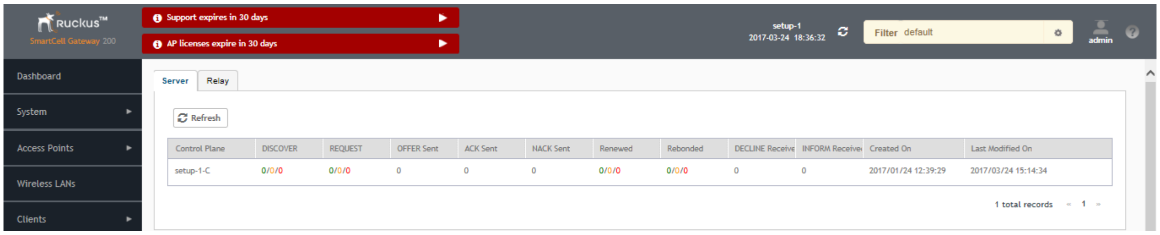
DHCP Server

The controller comes with a built-in DHCP server, which can be enabled for assigning IP addresses to devices that are connected to it. The controller’s DHCP server will only assign addresses to devices that are on its own subnet and are a part of the same VLAN (if VLANs are assigned). To view the KPIs, navigate to **Diagnostics** > **DHCP** > **Server**.

The below table lists the key performance indicators related to the Dynamic Host Configuration Protocol (DHCP) server functions.

NOTE For information on configuring DHCP Service, refer to the *Administrator Guide for SmartZone* (PDF) or the *SmartZone Online Help*, which is accessible from the controller''s web interface.

Figure 10: DHCP server



Control Plane	DISCOVER	REQUEST	OFFER Sent	ACK Sent	NACK Sent	Renewed	Rebonded	DECLINE Receive	INFORM Receive	Created On	Last Modified On
setup-1-C	0/0/0	0/0/0	0	0	0	0/0/0	0/0/0	0	0	2017/01/24 12:39:29	2017/03/24 15:14:34

1 total records « 1 »

Table 13: KPIs for DHCP server

KPI	Description
Control Plane	Indicates the control plane name.
DISCOVER	Indicates the number of DHCP discover messages processed by the DHCP server.
REQUEST	Indicates the number of DHCP request messages sent by the DHCP server.
OFFER Sent	Indicates the number of DHCP offer messages processed by the DHCP server. This excludes duplicate messages.
ACK Sent	Indicates the number of DHCP acknowledgment messages sent by the DHCP server.
NACK Sent	Indicates the number of DHCP not acknowledged (NACK) messages sent by the DHCP server.
Renewed	Indicates the number of DHCP request messages for renewing the lease period handled.
Rebonded	Indicates the number of DHCP request messages for rebonding.
DECLINE Received	Indicates the number of DHCP decline messages received.
INFORM Received	Indicates the number of DHCP inform messages received.
Created On	Indicates the date and time the service was created.
Last Modified On	Indicates the date and time the service was last modified.

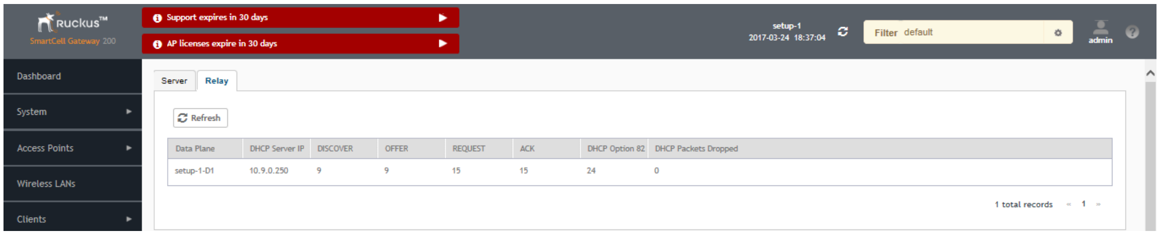
DHCP Relay

DHCP relay is when the DHCP server acts as relay at the controller. To view the KPIs, navigate to **Diagnostics** > **DHCP** > **Relay**.

The below table lists the key performance indicators related to the DHCP relay.

NOTE For information on configuring DHCP Service, refer to the *Administrator Guide for SmartZone* (PDF) or the *SmartZone Online Help*, which is accessible from the controller web interface.

Figure 11: DHCP relay



Support expires in 30 days

AP licenses expire in 30 days

Data Plane	DHCP Server IP	DISCOVER	OFFER	REQUEST	ACK	DHCP Option 82	DHCP Packets Dropped
setup-1-D1	10.9.0.250	9	9	15	15	24	0

Table 14: KPIs for DHCP relay

KPI	Description
Data Plane	Indicates the data plane name.
DHCP Server IP	Indicates the IP address of the DHCP server.
DISCOVER	Indicates the number of DHCP discover messages forwarded to the DHCP server.
OFFER	Indicates the number of DHCP offer messages received from the DHCP server.
REQUEST	Indicates the number of DHCP request messages forwarded to the DHCP server.
ACK	Indicates the number of DHCP acknowledgment messages received from the DHCP server.
DHCP Opt82	Indicates the number of DHCP reply messages received, which include Option 82 in the header. (replies include offer and acknowledgment messages.)
DHCP Packets Dropped	Indicates the number of DHCP packets that are dropped.

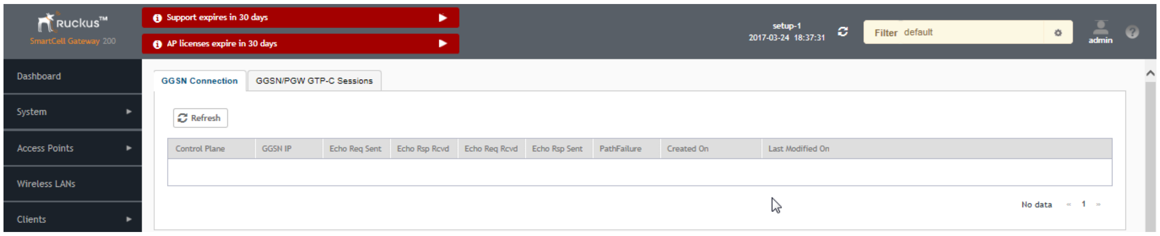
GGSN Connections

The controller has 3GPP defined Tunnel Terminating Gateway (TTG) functionality, which enables it to act as a gateway between the UE (southbound) and the telecom core (northbound). This is to tunnel the traffic between the UE (User Equipment such as mobile phone) and the controller's gateway, which terminates the tunnel and transfers the data over to the GGSN (Gateway GPRS Serving Node).

To view the KPIs, navigate to **Diagnostics** > **GGSN** > **GGSN Connection**. The following table lists the key performance indicators for path management message statistics of GGSN connections.

NOTE For information on configuring GGSN Service, refer to the *Administrator Guide for SmartZone* (PDF) or the *SmartZone Online Help*, which is accessible from the controller's web interface.

Figure 12: GGSN connections



Support expires in 30 days

AP licenses expire in 30 days

Control Plane	GGSN IP	Echo Req Sent	Echo Rsp Rcvd	Echo Req Rcvd	Echo Rsp Sent	PathFailure	Created On	Last Modified On

Table 15: KPIs for GGSN connections

KPI	Description
Control Plane	Indicates the name of the control plane.
GGSN IP	Indicates the IP address of the GGSN node.
Echo Req Sent	Indicates the number of echo requests initiated by the controller towards GGSN.
Echo Rsp Rcvd	Indicates the number of echo responses received by the controller from GGSN.
Echo Req Rcvd	Indicates the number of echo requests initiated by GGSN towards the controller.
Echo Rsp Sent	Indicates the number of echo responses received by GGSN from the controller.
Path Failure	Indicates the number of times GGSN was unreachable.

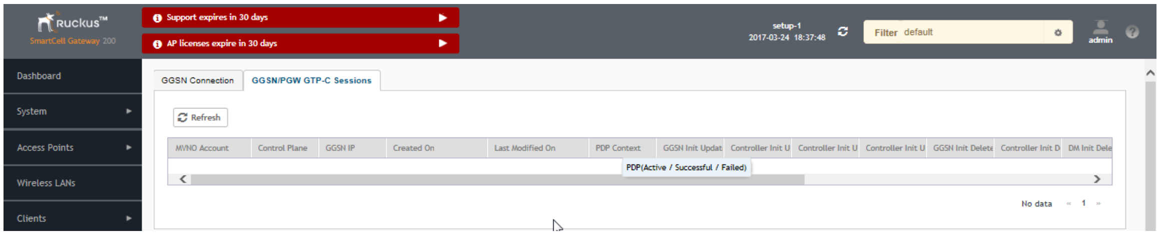
KPI	Description
Created On	Indicates the date and time the service was created.
Last Modified On	Indicates the date and time the service was last modified.

GGSN/PGW GTP-C Sessions

To view the KPIs, navigate to **Diagnostics** > **GGSN** > **GGSN/PGW GTP-C Sessions**. The following table lists the key performance indicators for tunnel management messages of GGSN/PGW GTP-C sessions.

NOTE For information on configuring GGSN Service, refer to the *Administrator Guide for SmartZone* (PDF) or the *SmartZone Online Help*, which is accessible from the controller's web interface.

Figure 13: GGSN/PGW GTP-C session



Support expires in 30 days

AP licenses expire in 30 days

setup-1
2017-03-24 18:37:48

Filter default

MVNO Account	Control Plane	GGSN IP	Created On	Last Modified On	PDP Context	GGSN Init Updat	Controller Init U	Controller Init U	Controller Init U	GGSN Init Delete	Controller Init D	DM Init Dele

PDP(Active / Successful / Failed)

No data

Table 16: KPIs for GGSN/PGW GTP-C connection

KPI	Description
MVNO Account	Indicates the mobile virtual network operator account.
Control Plane	Indicates the control plane name.
GGSN IP	Indicates the IP address of the GGSN node.
Created On	Indicates the date and time the service was created.
Last Modified On	Indicates the date and time of last modification.
PDP Context	Indicates the Policy Decision Point (PDP) which can either be active, successful or failed.
GGSN Init Update	Indicates the PDP update received (successful / failed).

KPI	Description
Controller Init Update (Roaming)	Indicates the PDP update initiated (successful / failed).
Controller Init Update (CoA from AAA)	Indicates the number of controller initiated update - CoA from AAA (successful / failed).
Controller Init Update (Events from HLR)	Indicates the number of controller initiated update - Event from HLR (successful / failed).
GGSN Init Delete	Indicates the number of successful GGSN initiated delete session (successful / failed).
Controller Init Delete (Error)	Indicates the number of controller initiated delete due to critical error (successful / failed).
DM Init Delete	Indicates the number of the controller initiated delete due to Dynamic Multipoint (DM) from AAA (successful / failed).
Controller Init Delete (Event from HLR)	Indicates the number of controller initiated delete due to event from HLR (successful / failed).
Controller Init Delete (Timeout)	Indicates the number of controller initiated delete due to timeout at the controller (successful / failed).
AP Init Delete	Indicates the number of AP initiated delete due to timeout at Access Point (AP) (successful / failed).
DP Init Delete	Indicates the number of data plane initiated delete due to timeout at Data Plane (DP) (successful / failed).
Client Init Delete	Indicates the number of client initiated delete (successful / failed).
Admin Init Delete	Indicates the number of admin initiated delete (successful / failed).

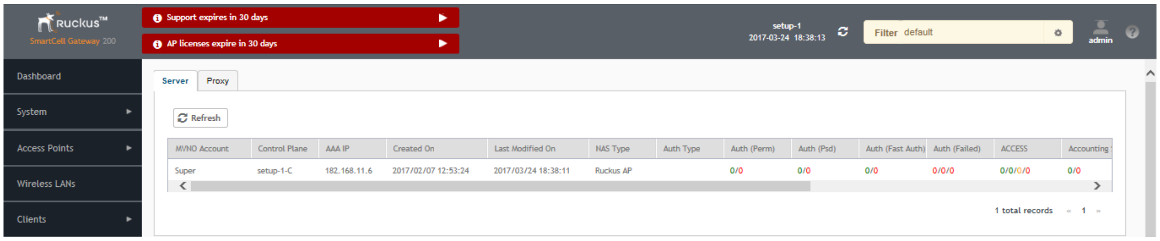
RADIUS Server

A RADIUS service defines the external RADIUS server configuration. RADIUS services authenticates profiles to specify external RADIUS services used based on the realm value.

To view the KPIs, navigate to **Diagnostics** > **RADIUS** > **Server**. The following table lists the key performance indicators for the statistics related to the RADIUS server.

NOTE For information on configuring RADIUS Service, refer to the *Administrator Guide for SmartZone* (PDF) or the *SmartZone Online Help*, which is accessible from the controller's web interface.

Figure 14: RADIUS server



MVNO Account	Control Plane	AAA IP	Created On	Last Modified On	NAS Type	Auth Type	Auth (Perm)	Auth (Psd)	Auth (Fast Auth)	Auth (Failed)	ACCESS	Accounting
Super	setup-1-C	182.168.11.6	2017/02/07 12:53:24	2017/03/24 18:38:11	Ruckus AP		0/0	0/0	0/0	0/0/0	0/0/0/0	0/0

Table 17: KPIs for RADIUS server

KPI	Description
MVNO Account	Indicates the mobile virtual network operator account.
Control Plane	Indicates the control plane name.
AAA IP	Indicates the IP address of the AAA server.
Created on	Indicates the date and time the entry was created.
Modified On	Indicates the date and time the entry was last modified.
NAS Type	Indicates the NAS type.
Auth Type	Indicates the authentication type.
Auth (Perm)	Indicates the number of authentications done using Permanent ID (successful / failed).
Auth (Psd)	Indicates the number of authentications done using Pseudonym ID (successful / failed).
Auth (Fast Auth)	Indicates the number of authentications done using fast re-auth ID (successful / failed).
Auth (Failed)	Indicates the number of authentication requests for (unknown pseudonym ID / unknown fast re-auth ID) the number of incomplete authentications processed.
ACCESS	Indicates the number of RADIUS access from NAS (requests received / accepts sent / challenge sent / rejects sent).

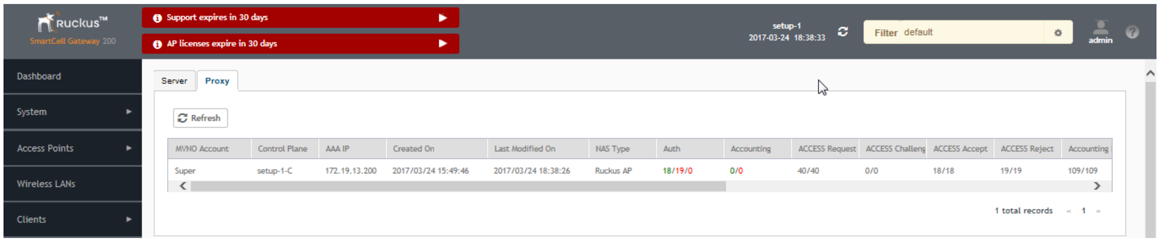
KPI	Description
Accounting Session	Indicates the number of accounting sessions established (successful / failed).
Accounting Request	Indicates the number of AP accounting sessions established (successful / failed).
AP Accounting	Indicates the number of AP accounting sessions established (successful / failed).
AP Accounting Request/Response	Indicates the number of AP accounting (request / response).
AP Accounting ON Request	Indicates the number of AP accounting ON (request / response).
AP Accounting OFF Request	Indicates the number of AP accounting OFF (request / response).

RADIUS Proxy

To view the KPIs, navigate to **Diagnostics** > **RADIUS** > **Proxy**. The below lists the key performance indicators related to the RADIUS proxy..

NOTE For information on configuring RADIUS Proxy, refer to the *Administrator Guide for SmartZone* (PDF) or the *SmartZone Online Help*, which is accessible from the controller's web interface.

Figure 15: RADIUS proxy



MVNO Account	Control Plane	AAA IP	Created On	Last Modified On	NAS Type	Auth	Accounting	ACCESS Request	ACCESS Challeng	ACCESS Accept	ACCESS Reject	Accounting
Super	setup-1-C	172.19.13.200	2017/03/24 15:49:46	2017/03/24 18:38:26	Ruckus AP	18/19/0	0/0	40/40	0/0	18/18	19/19	109/109

1 total records « 1 »

Table 18: KPIs for RADIUS proxy

KPI	Description
MVNO Account	Indicates the mobile virtual network operator account.
Control Plane	Indicates the control plane name.
AAA IP	Indicates the IP address of the AAA server.

KPI	Description
Created On	Indicates the date and time the entry was created.
Last Modified On	Indicates the date and time the entry was last modified.
NAS Type	Indicates the NAS type.
Auth	Indicates the number of authentications (successful / failed / incomplete).
Accounting	Indicates the number of accounting sessions established (successful / failed).
ACCESS Request	Indicates the number of RADIUS access requests received from NAS or the number of RADIUS access requests sent to AAA server.
ACCESS Challenge	Indicates the number of RADIUS access challenges received from AAA server or the number of RADIUS access challenge sent to NAS.
ACCESS Accept	Indicates the number of RADIUS access accepts received from AAA server or the number of RADIUS access accepts sent to NAS.
ACCESS Reject	Indicates the number of RADIUS access rejects received from AAA server or the number of RADIUS access rejects sent to the NAS.
Account Request	Indicates the number of RADIUS accounting requests received from NAS or the number of RADIUS accounting requests sent to AAA server.
Accounting Response	Indicates the number of RADIUS accounting responses received from AAA server or the number of RADIUS accounting responses sent to NAS.
CoA (AAA)	Indicates the number of RADIUS CoA requests received from AAA server or the number of RADIUS CoA responses sent to AAA server (successful) or the number of RADIUS CoA responses sent to AAA server (failed).

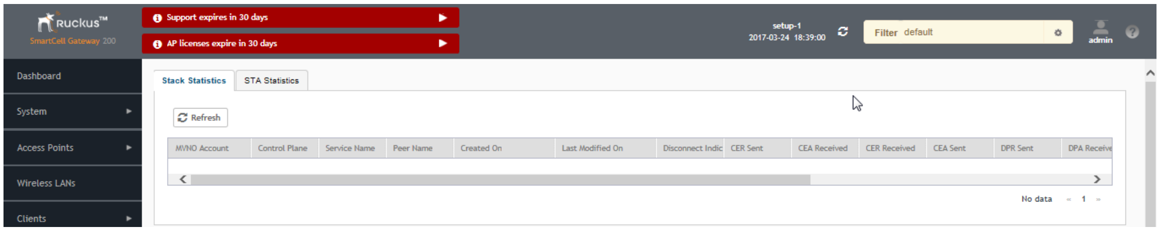
KPI	Description
DM (AAA)	Indicates the number of RADIUS DM requests received from AAA server or the number of RADIUS DM responses sent to AAA server (successful) or the number of RADIUS DM responses sent to AAA server (failed).
DM (NAS)	Indicates the number of RADIUS DM requests sent to NAS or the number of RADIUS DM responses received from NAS (successful) or the number of RADIUS DM responses received from NAS (failed).
AP Accounting	Indicates the number of AP accounting sessions established (successful / failed).
AP Accounting Request/Response	Indicates the number of AP accounting (request / response).
Dropped Requests	Indicates the actual number of dropped requests when the total number of requests received from NAS is greater than MOR value against each RADIUS service / server.
CoA (NAS)	Indicates the number of CoA requests proxied to NAS (3rd party AP).
CoA Autz Only	Indicates the number of RADIUS authorize only requests.

Diameter Stack Statistics

To view the KPIs, navigate to **Diagnostics** > **Diameter** > **Stack Statistics**. The below table lists the key performance indicators related to the Diameter Stack Statistics.

NOTE For information on configuring Diameter Services refers to the *Administrator Guide for SmartZone* (PDF) or the *SmartZone Online Help*, which is accessible from the controller's web interface.

Figure 16: Diameter stack statistics



Support expires in 30 days

AP licenses expire in 30 days

setup-1
2017-03-24 18:39:00

Filter default

MVNO Account	Control Plane	Service Name	Peer Name	Created On	Last Modified On	Disconnect Indic	CER Sent	CEA Received	CER Received	CEA Sent	DPR Sent	DPA Receive

No data « 1 »

Table 19: KPIs for Diameter stack statistics

KPI	Description
MVNO Account	MVNO account created with management privileges
Control Plane	Name of the control plane
Service Name	Diameter service name
Peer Name	Diameter peer name, to which the connection is established
Created On	Date of record creation
Last Modified On	Date when the record was last modified
Disconnect Indication	Number of disconnection indications
CER Sent	Number of Capacity Exchange Request (CERs) sent by the stack to the remote diameter peer
CEA Received	Number of Capability-Exchange-Answer (CEA) responses received by the stack from the remote diameter peer
CER Received	Number of CERs received by the stack from the remote diameter peer
CEA Sent	Number of CEA responses sent by the stack to the remote diameter peer
DPR Sent	Number of Disconnect Peer Request (DPR) sent by the stack to the remote diameter peer
DPA Received	Number of Disconnect Peer Answer (DPA) received by the stack from the remote diameter peer
DPR Received	Number of disconnect peer requests received by the stack from the remote diameter peer
DPA Sent	Number of disconnect peer answers sent by the stack to the remote diameter peer
DWR Sent	Number of Device WatchDog Request (DWR) sent by the stack to the remote diameter peer
DWA Received	Number of Device WatchDog Answer (DWA) received by the stack from the remote diameter peer
DWR Received	Number of device watchdog requests received by the stack from the remote diameter peer

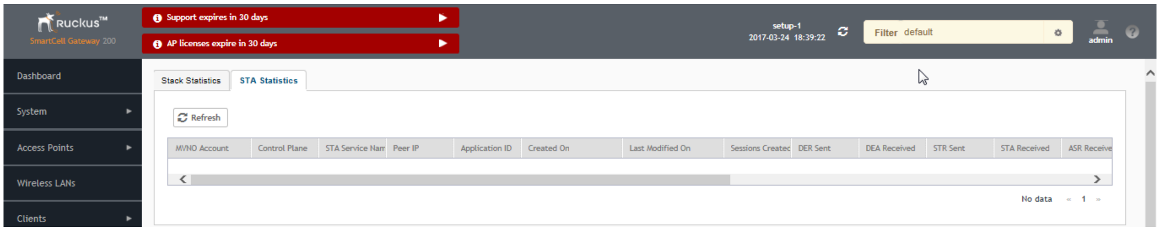
KPI	Description
DWA Sent	Number of device watchdog answers) sent by the stack to the remote diameter peer

Diameter STA Statistics

To view the KPIs, navigate to **Diagnostics** > **Diameter** > **STA Statistics**. The below table lists the key performance indicators related to the Diameter STa Statistics.

NOTE For information on configuring Diameter Services refers to the *Administrator Guide for SmartZone* (PDF) or the *SmartZone Online Help*, which is accessible from the controller's web interface.

Figure 17: Diameter STA statistics



Support expires in 30 days

AP licenses expire in 30 days

setup-1
2017-03-24 18:39:22

Filter default

MVNO Account	Control Plane	STA Service Nam	Peer IP	Application ID	Created On	Last Modified On	Sessions Createc	DER Sent	DEA Received	STR Sent	STA Received	ASR Receive

No data « 1 »

Table 20: KPIs for Diameter STa statistics

KPI	Description
MVNO Account	MVNO account created with management privileges
Control Plane	Name of the control plane
STA Service Name	Diameter service name
Peer IP	Diameter IP address, to which the connection is established.
Application ID	Application identifier of the STa interface
Created On	Date of record creation
Last Modified On	Date when the record was last modified
Session Created	Number of sessions created
DER Sent	Number of Diameter EAP Request (DER) sent from the controller to 3GPP AAA Radius server
DEA Received	Number of Diameter EAP Answer (DEA) received from the 3GPP AAA Radius server

KPI	Description
STR Sent	Number of Session Termination Request (STR) sent from the controller to 3GPP AAA Radius server
STA Received	Number of Session Termination Answer (STA) received from the 3GPP AAA Radius server
ASR Received	Number of Abort Session Request (ASR) with session termination indication received from the 3GPP AAA Radius server
ASA Sent	Number of Abort Session Answer (ASA) sent with result code (success or failure)
RAR Received	Number of Re-Auth Request (RAR) with session update indication received from the 3GPP AAA Radius server
RAA Sent	Number of Re-Auth Answer (RAA) sent.
AAR Sent	Number of AA-Request (AAR) sent from the controller to the 3GPP AAA Radius server
AAA Received	Number of AAA received from 3GPP AAA Radius server
DER ReAuth Sent	Number of Diameter EAP Request (DER) re-authorization sent from the controller to the 3GPP AAA Radius server
DEA ReAuth Received	Number of Diameter EAP Answer (DEA) re-authorization received from 3GPP AAA Radius server
Tx Timeout	Number of Tx timeouts
Msgs Dropped	Number of messages from 3GPP AAA that were dropped or had a decode failure

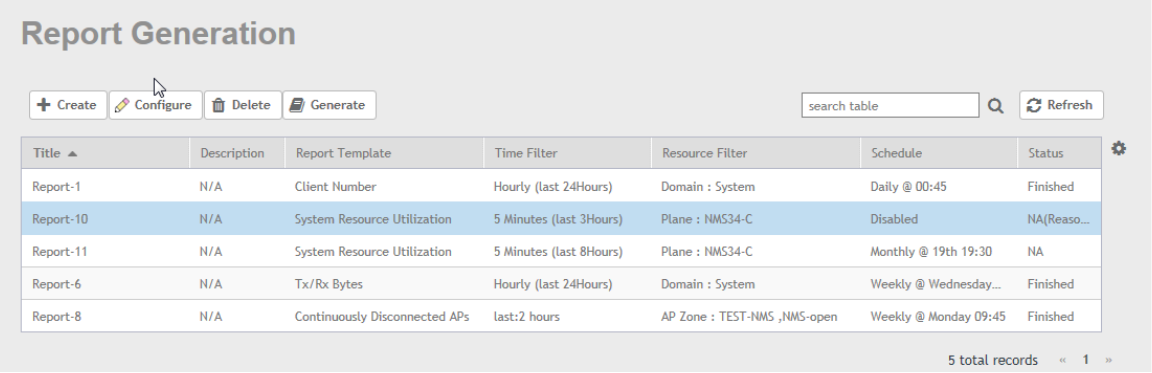
Reports

2

Report Generation

Report Generation list the reports that have been created and saved Figure 18: Report Generation on page 37. To view the list of saved reports navigate to **Report** > **Report Generation**. Click a report name to view the details or to modify the report settings.

Figure 18: Report Generation



Title ▲	Description	Report Template	Time Filter	Resource Filter	Schedule	Status
Report-1	N/A	Client Number	Hourly (last 24Hours)	Domain : System	Daily @ 00:45	Finished
Report-10	N/A	System Resource Utilization	5 Minutes (last 3Hours)	Plane : NMS34-C	Disabled	NA(Reaso...
Report-11	N/A	System Resource Utilization	5 Minutes (last 8Hours)	Plane : NMS34-C	Monthly @ 19th 19:30	NA
Report-6	N/A	Tx/Rx Bytes	Hourly (last 24Hours)	Domain : System	Weekly @ Wednesday...	Finished
Report-8	N/A	Continuously Disconnected APs	last:2 hours	AP Zone : TEST-NMS ,NMS-open	Weekly @ Monday 09:45	Finished

5 total records « 1 »

All the controller's reports can be displayed in different time intervals (15 minutes, hourly, daily, or monthly) for the specified time filter (in hours) and exported in comma-separated value (CSV) format and portable document format (PDF).

NOTE For information on creating reports, refer to the *Administrator Guide for SmartZone* (PDF) or the *SmartZone Online Help*, which is accessible from the controller's web interface.

The following is the list of reports that can be generated:

- Client Number Report on page 37
- Continuously Disconnected APs Report on page 38
- System Resource Utilization Report on page 38
- Tx/Rx Bytes Report on page 38

Client Number Report

Generate the client number report to view the minimum and maximum number of clients connected to SCG for a given period of time. You can generate this report based on a specific management domain, AP zone, AP, SSID, or radio type.

Continuously Disconnected APs Report

The continuously disconnected APs report lists access points that were disconnected within a specified time period (hours). You can generate this report based on a specific management domain or AP zone.

System Resource Utilization Report

Generate the system resource utilization report to view the system's CPU and memory usage. You can generate this report based on a single plane or multiple planes.

Tx/Rx Bytes Report

Generate the Tx/Rx Bytes report to view the number of bytes that have been sent and received through SCG. You can generate this report based on a specific management domain, AP zone, AP, SSID, or radio type.

Viewing Rogue Access Points

Rogue (or unauthorized) APs pose problems for a wireless network in terms of airtime contention, as well as security.

Usually, a rogue AP appears in the following way: an employee obtains another manufacturer's AP and connects it to the LAN, to gain wireless access to other LAN resources. This would potentially allow even more unauthorized users to access your corporate LAN - posing a security risk. Rogue APs also interfere with nearby Ruckus Wireless APs, thus degrading overall wireless network coverage and performance.

The controller's rogue AP detection options include identifying the presence of a rogue AP, categorizing it as either a known neighbor AP or as a malicious rogue.

If you enabled rogue AP detection when you configured the common AP settings (see Configuring APs), click **Report** > **Rogue Access Points**. The Rogue Access Points page displays all rogue APs that the controller has detected on the network, including the following information:

- **Rogue MAC**: MAC address of the rogue AP.
- **Type**: Rogue, a normal rogue AP, not yet categorized as malicious or non-malicious.
- **Channel**: Radio channel used by the rogue AP.
- **Radio**: WLAN standards with which the rogue AP complies.
- **SSID**: WLAN name that the rogue AP is broadcasting.
- **Detecting AP Name**: Name of the AP.
- **Zone**: Zone to which the AP belongs.
- **RSSI**: Radio signal strength.
- **Encryption**: Indicates whether the wireless signal is encrypted or not.
- **Last Detected**: Date and time when the rogue AP was last detected by the controller.

Marking Rogue Access Points

You can mark a Rogue (or unauthorized) AP as known.

To mark a Rogue AP as known:

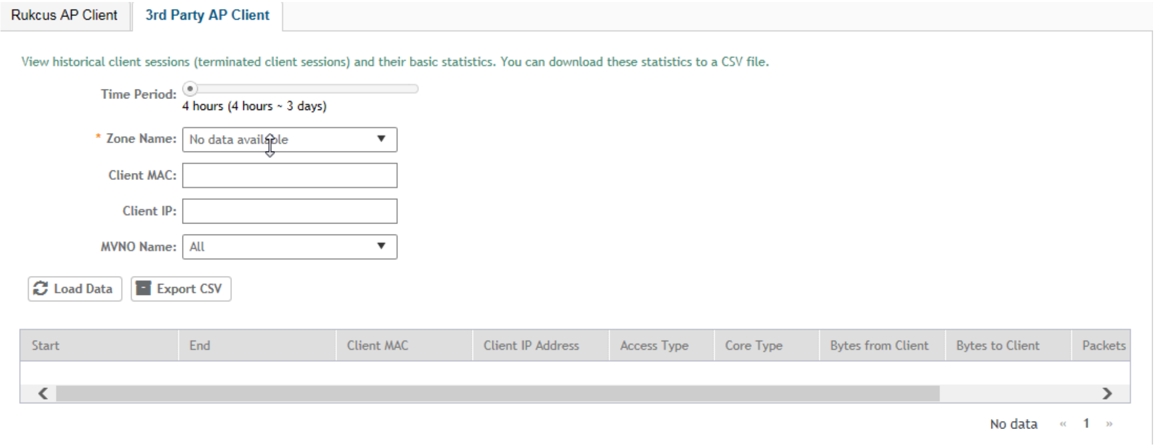
1. From the left pane, click **Report** and **Rogue Access Points**. The Rogue Access Points page appears.
2. Select the Rogue AP from the list and click **Mark as Known**. The classification **Type** of the Rogue AP changes to **Known**. You can also select the Rogue AP from the list and click **Unmark**, to change the classification.

Historical Client Statistics

Historical client report is based on the UE session statistics. This report is displayed under **Report** > **Historical Client Stats**. See Figure 19: Historical client statistics on page 39.

Table 21: Historical data attributes on page 40 contains the report for UE sessions. This is a cumulative value per session and one entry is created per session. Data is reported every 60 seconds and is not bin data. The user interface displays the table and its corresponding graph chart. The two representations are synchronized and controlled by the search criteria. For performance reasons, the controller may pre-calculate the total counters per DP or per GGSN IP for each bin.

Figure 19: Historical client statistics



View historical client sessions (terminated client sessions) and their basic statistics. You can download these statistics to a CSV file.

Time Period: 4 hours (4 hours ~ 3 days)

* Zone Name: No data available

Client MAC:

Client IP:

MVNO Name: All

Start	End	Client MAC	Client IP Address	Access Type	Core Type	Bytes from Client	Bytes to Client	Packets

No data « 1 »

Table 21: Historical data attributes

Attribute	Type	Description
Start	Long	Indicates the session creation time.
End	Long	Indicates the session end time.
Client MAC	String	Indicates the Mac address of the client.
Client IP Address	String	Indicates the IP address of the client.
Access Type	String	Indicates the AP that serves this client.
Core Type	String	Indicates the core network tunnel type.
Bytes from Client	Long	Indicates the number of bytes received from the client.
Bytes to Client	Long	Indicates the number of bytes sent to the client.
Packets from Client	Long	Indicates the number of packets received from the client.
Packets to Client	Long	Indicates the number of packets sent to the client.

Ruckus AP Tunnel Stats

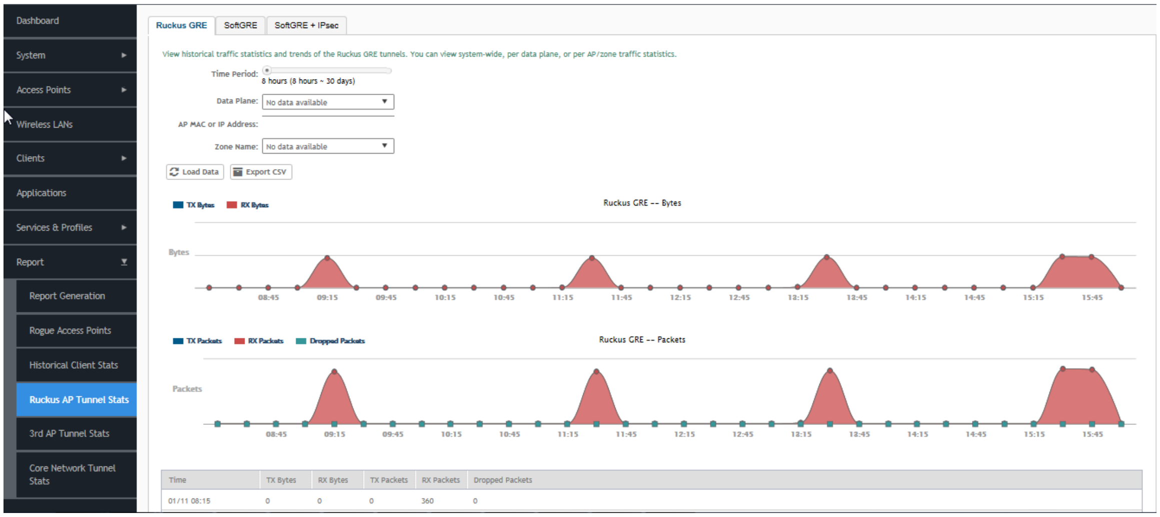
Ruckus AP Tunnel statistics or report is displayed under **Report** > **Ruckus AP Tunnel Stats**.

Ruckus AP Tunnel GRE Report

Table 22: Ruckus GRE report attributes on page 41 Table 22: Ruckus GRE report attributes on page 41 contains the report based on the statistics for access Ruckus GRE. Each entry contains the 15 minutes cumulative data.

The controller's web interface (**Report** > **Ruckus AP Tunnel Stats** > **Ruckus GRE**) displays the table and its corresponding graph chart as seen in Figure 20: Ruckus GRE report on page 41. The two representations are synchronized and controlled by the search criteria. For performance reasons, the controller may pre-calculate the total counters per DP or per AP for each bin.

Figure 20: Ruckus GRE report



View historical traffic statistics and trends of the Ruckus GRE tunnels. You can view system-wide, per data plane, or per AP/zone traffic statistics.

Time Period: 8 hours (8 hours ~ 30 days)

Data Plane: No data available

AP MAC or IP Address:

Zone Name: No data available

Time	TX Bytes	RX Bytes	TX Packets	RX Packets	Dropped Packets
01/11 08:15	0	0	0	360	0

Table 22: Ruckus GRE report attributes

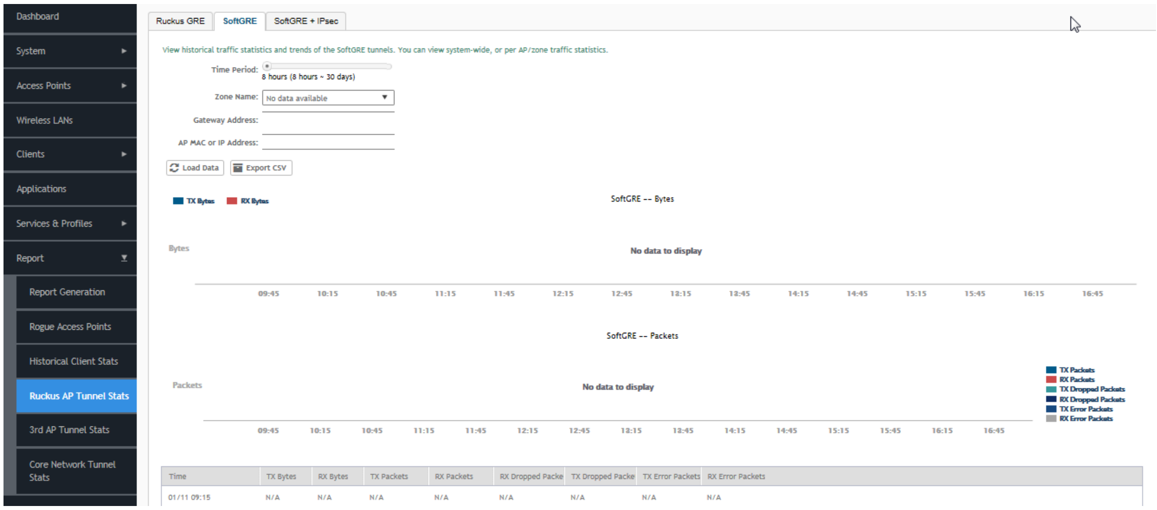
Attribute	Type	Description
Time	Long	Bin ID, which is stamped at a 15 minute interval. For example, 10:00, 10:15.
TXBytes	Long	Indicates the number of bytes sent.
RXBytes	Long	Indicates the number of bytes received.
TXPkts	Long	Indicates the number of packets sent.
RXPkts	Long	Indicates the number of packets received.
Dropped Packets	Long	Indicates the number of packets dropped.

Ruckus AP Tunnel SoftGRE Report

Table 23: Ruckus AP Tunnel SoftGRE Report Attributes on page 42 contains the report based on the statistics for access point Soft GRE. Each entry contains the 15 minutes cumulative data.

The controller's web interface (**Report** > **Ruckus AP Tunnel Stats** > **SoftGRE**) displays the table and its corresponding graph chart as seen in Figure 21: Ruckus AP Tunnel SoftGRE Report on page 42. The two representations are synchronized and controlled by the search criteria. For performance reasons, the controller may pre-calculate the total counters per DP or per AP for each bin.

Figure 21: Ruckus AP Tunnel SoftGRE Report



View historical traffic statistics and trends of the SoftGRE tunnels. You can view system-wide, or per AP/zone traffic statistics.

Time Period: 8 hours (8 hours ~ 30 days)

Zone Name: No data available

Gateway Address:

AP MAC or IP Address:

Time	TX Bytes	RX Bytes	TX Packets	RX Packets	RX Dropped Packe	TX Dropped Packe	TX Error Packets	RX Error Packets
01/11 09:15	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A

Table 23: Ruckus AP Tunnel SoftGRE Report Attributes

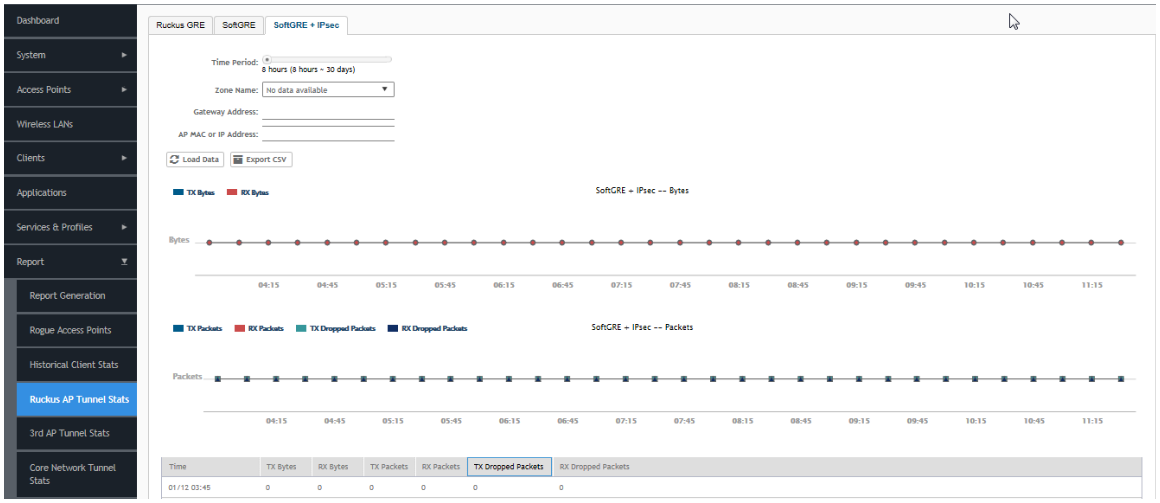
Attribute	Type	Description
Time	Long	Bin ID, which is stamped at a 15 minute interval. For example, 10:00, 10:15.
TXBytes	Long	Indicates the number of bytes sent.
RXBytes	Long	Indicates the number of bytes received.
TXPkts	Long	Indicates the number of packets sent.
RXPkts	Long	Indicates the number of packets received.
RX Dropped Packets	Long	Indicates the number of packets dropped.
TX Dropped Packets	Long	Indicates the number of packets dropped.
TX Error Packets	Long	Indicates the number of packets with a header error.
RX Error Packets	Long	Indicates the number of packets with a header error.

Ruckus AP Tunnel SoftGRE + IPsec Report

Table 24: Ruckus AP Tunnel SoftGRE + IPSec Report Attributes on page 43 contains the report based on the statistics for access point IPsec. Each entry contains the 15 minutes cumulative data.

The controller's web interface (**Report** > **Report AP Tunnel Stats** > **SoftGRE + IPsec**) displays the table and its corresponding graph chart as seen in Figure 22: Ruckus AP Tunnel SoftGRE + IPsec Report on page 43. The two representations are synchronized and controlled by the search criteria. For performance reasons, the controller may pre-calculate the total counters per DP or per AP for each bin.

Figure 22: Ruckus AP Tunnel SoftGRE + IPsec Report



Time Period: 8 hours (8 hours ~ 30 days)
Zone Name: No data available
Gateway Address:
AP MAC or IP Address:

Time	TX Bytes	RX Bytes	TX Packets	RX Packets	TX Dropped Packets	RX Dropped Packets
01/12 03:45	0	0	0	0	0	0

Table 24: Ruckus AP Tunnel SoftGRE + IPSec Report Attributes

Attribute	Type	Description
Time	Long	Bin ID, which is stamped at a 15 minute interval. For example, 10:00, 10:15.
TXBytes	Long	Indicates the number of bytes sent.
RXBytes	Long	Indicates the number of bytes received.
TXPkts	Long	Indicates the number of packets sent.
RXPkts	Long	Indicates the number of packets received.
TX Dropped Packets	Long	Indicates the number of packets dropped.
RX Dropped Packets	Long	Indicates the number of packets dropped.

3rd Party AP Stats

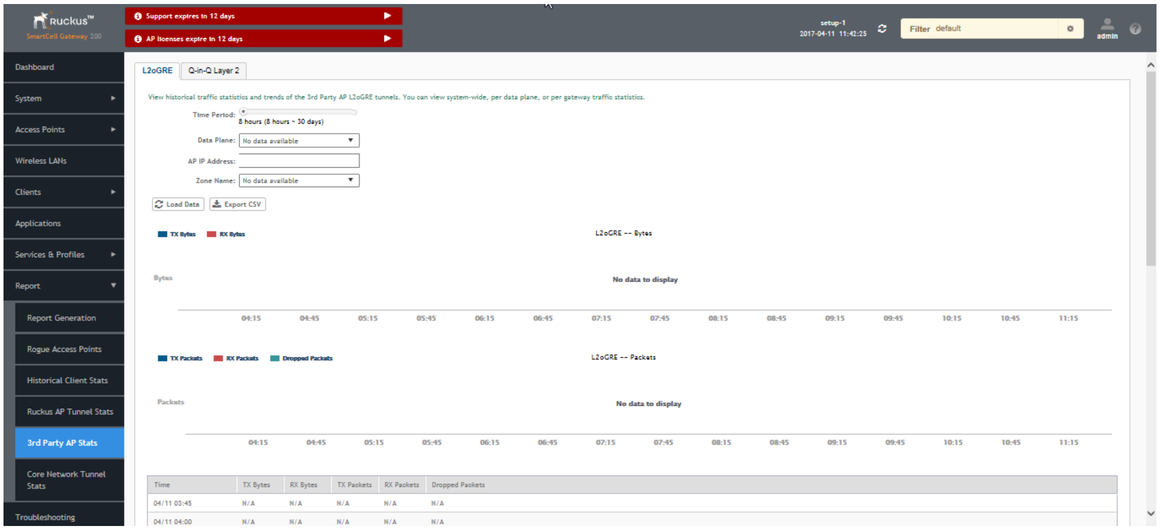
3rd Party AP statistics or report is displayed under **Report** > **3rd Party AP Stats**.

3rd Party AP L2oGRE Report

Table 25: 3rd Party AP L2oGRE Report Attributes on page 44 contains the report based on the statistics for access side tunnels. Each entry contains the 15 minutes cumulative data.

The controller's web interface (**Report** > **3rd Party AP Stats** > **L2oGRE**) displays the table and its corresponding graph chart as seen in Figure 23: 3rd Party AP L2oGRE Report on page 44. The two representations are synchronized and controlled by the search criteria. For performance reasons, the controller may pre-calculate the total counters per DP or per AP for each bin.

Figure 23: 3rd Party AP L2oGRE Report



View historical traffic statistics and trends of the 3rd Party AP L2oGRE tunnels. You can view system-wide, per data plane, or per gateway traffic statistics.

Time Period: 8 hours (8 hours ~ 30 days)

Data Plane: No data available

AP IP Address:

Zone Name: No data available

Time	TX Bytes	RX Bytes	TX Packets	RX Packets	Dropped Packets
04/11 03:45	N/A	N/A	N/A	N/A	N/A
04/11 04:00	N/A	N/A	N/A	N/A	N/A

Table 25: 3rd Party AP L2oGRE Report Attributes

Attribute	Type	Description
Time	Long	Bin ID, which is stamped at a 15 minute interval. For example, 10:00, 10:15.
TXBytes	Long	Indicates the number of bytes sent.
RXBytes	Long	Indicates the number of bytes received.
TXPkts	Long	Indicates the number of packets sent.

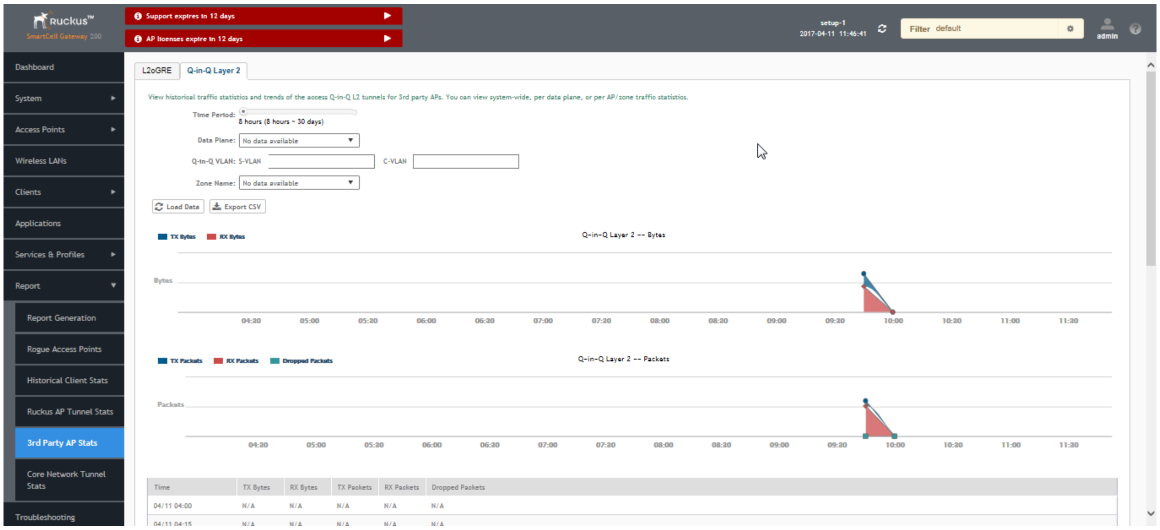
Attribute	Type	Description
RXPkts	Long	Indicates the number of packets received.
Dropped Packets	Long	Indicates the number of packets dropped.

3rd Party AP Q-in-Q Layer2 Report

Table 26: 3rd Party AP Q-in-Q Layer2 Report Attributes on page 45 contains the report based on the statistics for access side tunnels Q-in-Q. Each entry contains the 15 minutes cumulative data.

The controller's web interface (**Report** > **3rd Party AP Stats** > **Q-in-Q Layer 2**) displays the table and its corresponding graph chart as seen in the following image. The two representations are synchronized and controlled by the search criteria. For performance reasons, the controller may pre-calculate the total counters per DP or per Q-in-Q tag pair for each bin.

Figure 24: 3rd Party AP Q-in-Q Layer2 Report



Support expires in 12 days

AP licenses expire in 12 days

View historical traffic statistics and trends of the access Q-in-Q L2 tunnels for 3rd party APs. You can view system-wide, per data plane, or per AP/zone traffic statistics.

Time Period: 8 hours (8 hours ~ 30 days)

Data Plane: No data available

Q-in-Q VLAN: S-VLAN

C-VLAN

Zone Name: No data available

Time	TX Bytes	RX Bytes	TX Packets	RX Packets	Dropped Packets
04/11 04:00	N/A	N/A	N/A	N/A	N/A
04/11 04:15	N/A	N/A	N/A	N/A	N/A

Table 26: 3rd Party AP Q-in-Q Layer2 Report Attributes

Attribute	Type	Description
Time	Long	Bin ID, which is stamped at a 15 minute interval. For example, 10:00, 10:15.
TXBytes	Long	Indicates the number of bytes sent.
RXBytes	Long	Indicates the number of bytes received.
TXPkts	Long	Indicates the number of packets sent.

Attribute	Type	Description
RXPkts	Long	Indicates the number of packets received.
Dropped Packets	Long	Indicates the number of packets dropped.

Core Network Tunnel Stats

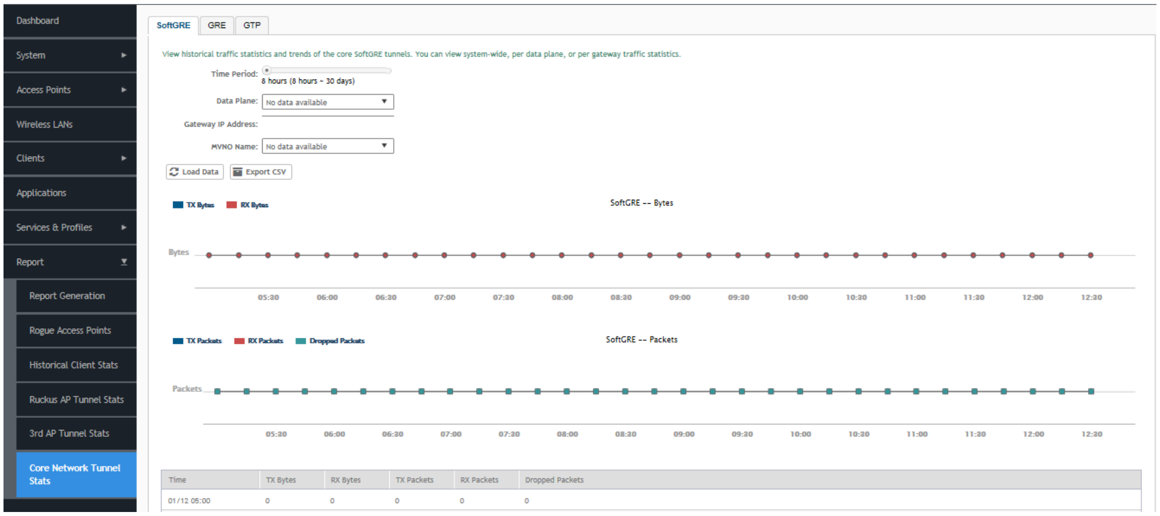
Core Network Tunnel statistics or report is displayed under **Report** > **Core Network Tunnel Stats**.

Core Network Tunnel SoftGRE Report

Table 27: Core Network Tunnel SoftGRE Report Attributes on page 47 contains the report based on the statistics for core side gateway. Each entry contains the 15 minutes cumulative data.

The user interface (**Report** > **Core Network Tunnel Statistics** > **SoftGRE**) displays the table and its corresponding graph chart as seen in Figure 25: Core Network Tunnel SoftGRE Report on page 46. The two representations are synchronized and controlled by the search criteria. For performance reasons, the controller may pre-calculate the total counters per DP or per Gateway IP for each bin.

Figure 25: Core Network Tunnel SoftGRE Report



View historical traffic statistics and trends of the core SoftGRE tunnels. You can view system-wide, per data plane, or per gateway traffic statistics.

Time Period: 8 hours (8 hours ~ 30 days)

Data Plane: No data available

Gateway IP Address:

MVNO Name: No data available

Time	TX Bytes	RX Bytes	TX Packets	RX Packets	Dropped Packets
01/12 05:00	0	0	0	0	0

Table 27: Core Network Tunnel SoftGRE Report Attributes

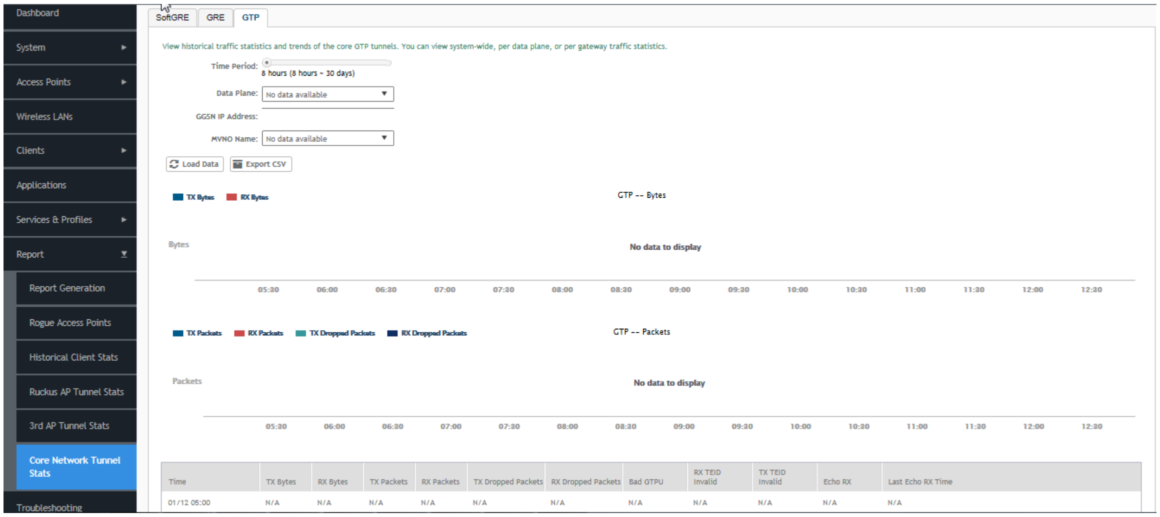
Attribute	Type	Description
Time	Long	Bin ID, which is stamped at a 15 minute interval. For example, 10:00, 10:15.
TXBytes	Long	Indicates the number of bytes sent.
RXBytes	Long	Indicates the number of bytes received.
TXPkts	Long	Indicates the number of packets sent.
RXPkts	Long	Indicates the number of packets received.
Dropped Packets	Long	Indicates the number of packets dropped.

Core Network Tunnel GTP Report

Table 28: Core Network Tunnel GTP Report Attribute on page 48 contains the statistics for core side gateway of GGSN GTP-U. Each record contains the accumulated data for a 15 minute period. The table entry contains TX/RX statistics from all packets received from a GGSN in the last 15 minutes. The attribute, MVNO-ID is provided by the SCG-CBlade.

The user interface (**Report** > **Core Network Tunnel Stats** > **GTP**) displays the table and its corresponding graph chart as seen in Figure 26: Core Network Tunnel GTP Report on page 48. The two representations are synchronized and controlled by the search criteria. For performance reasons, the controller may pre-calculate the total counters per DP or per GGSN IP for each bin.

Figure 26: Core Network Tunnel GTP Report



View historical traffic statistics and trends of the core GTP tunnels. You can view system-wide, per data plane, or per gateway traffic statistics.

Time Period: 8 hours (8 hours ~ 30 days)

Data Plane: No data available

GGSN IP Address:

MVNO Name: No data available

Time	TX Bytes	RX Bytes	TX Packets	RX Packets	TX Dropped Packets	RX Dropped Packets	Bad GTPU	RX TEID Invalid	TX TEID Invalid	Echo RX	Last Echo RX Time
01/12 05:00	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A

Table 28: Core Network Tunnel GTP Report Attribute

Attribute	Type	Description
Time	Long	Bin ID, which is stamped at a 15 minute interval. For example, 10:00, 10:15.
TXBytes	Long	Indicates the number of bytes sent.
RXBytes	Long	Indicates the number of bytes received.
TXPkts	Long	Indicates the number of packets sent.
RXPkts	Long	Indicates the number of packets received.
TX Dropped Packets	Long	Indicates the number of packets dropped that are to be sent to GGSN.
RX Dropped Packets	Long	Indicates the number of packets dropped by GGSN.
Bad GTPU	Long	Number of packets received from GGSN with bad GTP header.
RXTeidInvalid	Long	Number of packets received from GGSN with bad TEID.
TXteidInvalid	Long	Number of packets for GGSN with bad/unknown TEID.
EchoRX	Long	Number of GTPU echo request received from GGSN.

Attribute	Type	Description
LastEchoRxTime	Long	Timestamp of the last GTPU echo request/reply received from GGSN.

Index

Ruckus®

Simply Better Wireless.

350 West Java Drive, Sunnyvale, CA

www.ruckuswireless.com