USER GUIDE

Ruckus SmartZone 300 Key Performance Indicator and Report Reference Guide, 5.1.2

Supporting SmartZone 5.1.2

Part Number: 800-72355-001 Rev A
Publication Date: August 2019

Copyright, Trademark and Proprietary Rights Information

© 2019 CommScope, Inc. All rights reserved.

No part of this content may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation, or adaptation) without written permission from CommScope, Inc. and/or its affiliates ("CommScope"). CommScope reserves the right to revise or change this content from time to time without obligation on the part of CommScope to provide notification of such revision or change.

Export Restrictions

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

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

Disclaimer

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

Limitation of Liability

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

Trademarks

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

Contents

Preface

Document Conventions

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

TABLE 1 Text Conventions

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

Notes, Cautions, and Warnings

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

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

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

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

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

Command Syntax Conventions

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

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

Document Feedback

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

You can email your comments to Ruckus at ruckus-docs@arris.com.

When contacting us, include the following information:

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

For example:

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

Ruckus Product Documentation Resources

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

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

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

Online Training Resources

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

Contacting Ruckus Customer Services and Support

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

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

What Support Do I Need?

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

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

Open a Case

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

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

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

Self-Service Resources

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

- Technical Documentation—https://support.ruckuswireless.com/documents

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

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

About This Guide

This *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 devices. Consequently, it assumes a basic working knowledge of local area networks, wireless networking, and wireless devices.

NOTE
This guide assumes that the SZ300 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 Support web site at https://support.ruckuswireless.com/contact-us.

What's New in This Document

TABLE 2 Summary of Enhancements in SmartZone Release 5.1.2

Feature	Description	Location
Auth/Accounting sessions	Auth/Accounting numbers reset if AAA session is reset	Refer to RADIUS Proxy on page 21 for more information.
Ruckus GRE + IPsec	Display of Ruckus GRE + IPsec report	Refer to Ruckus AP Tunnel GRE + IPSec Report on page 29 for more information.

Terminology

Table 3 lists the terms used in this guide.

TABLE 3 Terms used in this guide

Term	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

TABLE 3 Terms used in this guide (continued)

Term	Description
DEA	Diameter EAP Answer
DER	Diameter EAP Request
DHCP	Dynamic Host Configuration Protocol
DM	Dynamic Multipoint
DP	Data Plane
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
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
UE-IP	User Equipment - IP Address
UE-MAC	User Equipment - MAC Address
VLAN	Virtual LAN
WLAN	Wireless LAN

Key Performance Indicators

Overview

The 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 9 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 APs and applying a particular set of settings (including WLANs and their settings) to these groups of Ruckus APs. By default, an AP zone named **staging zone** exists. Any AP that registers with the controller 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 following 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

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 this 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 clients that belong to each AP zone.
AP IP Mode	Indicates the IP version.
Mesh	Indicates the mesh SSID.
Tunnel Type	Indicates the tunnel type used.
DP Zone Affinity Profile	Indicates the data plane zone affinity profile.
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 following 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

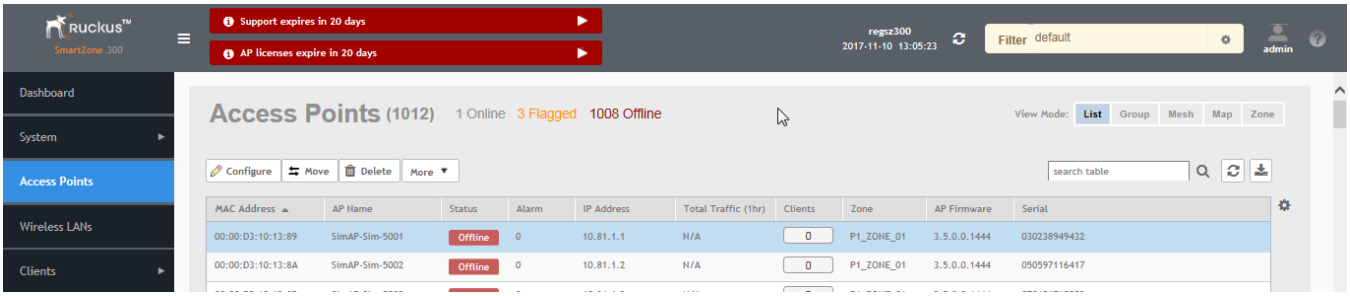


TABLE 5 KPIs for access points

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.
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 port.
AP Firmware	Indicates the firmware version installed on the access point.
Serial	Indicates the serial number.
Configuration Status	Indicates the status of the configuration settings.

TABLE 5 KPIs for access points (continued)

KPI	Description
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.
LBS Status	Indicates location-based service support.
Administrative State	Indicates the administration 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 configured management VLAN of the AP.
Packet Capture Status	Indicates AP packet capturing status.

KPI under the Clients Tab

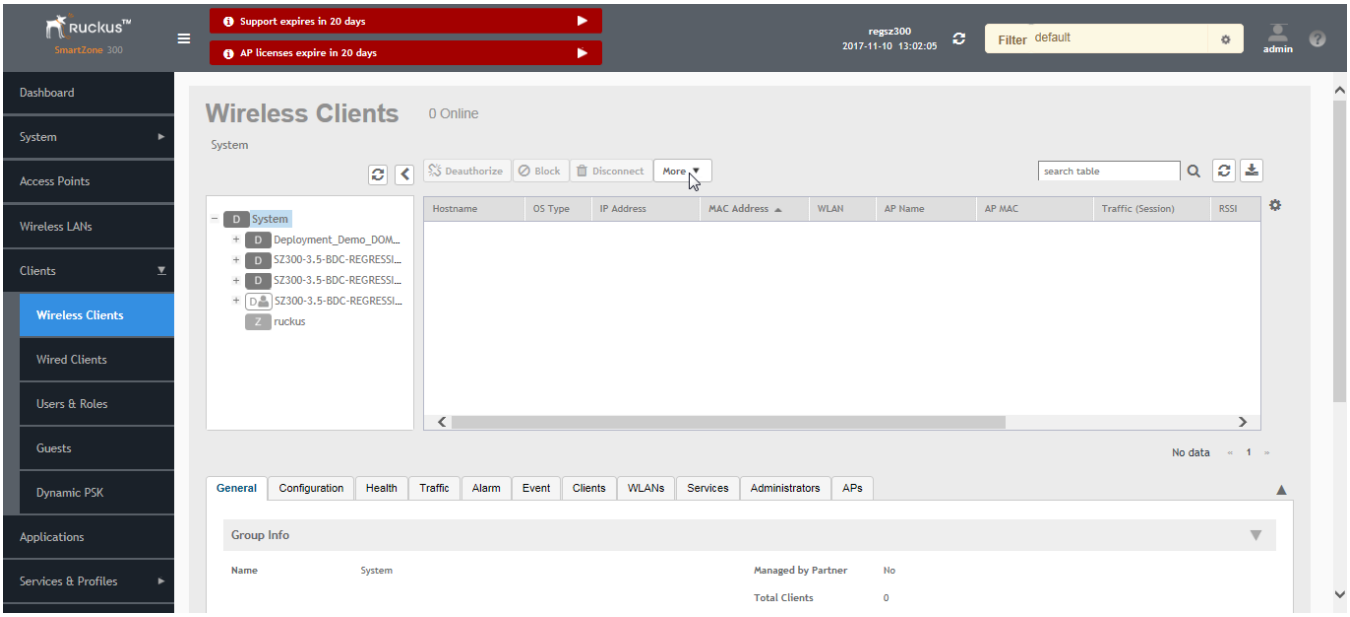
The following section describes the various key performance indicators that the controller provides in the **Clients** tab.

Wireless Clients KPI

To view the KPIs, navigate to **Clients** > **Wireless Clients**. See the following table 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



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 host name of the wireless client.
OS Type	Displays the operating system that the wireless client is using.
IP Address	Displays the IP address assigned to the wireless client.
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.
RSSI	Displays the Received Signal Strength Indicator (RSSI), which indicates how well a wireless client can recieve a signal from an AP. The RSSI value is shown in decibels (dBm) 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.

TABLE 6 KPIs for Wireless Clients (continued)

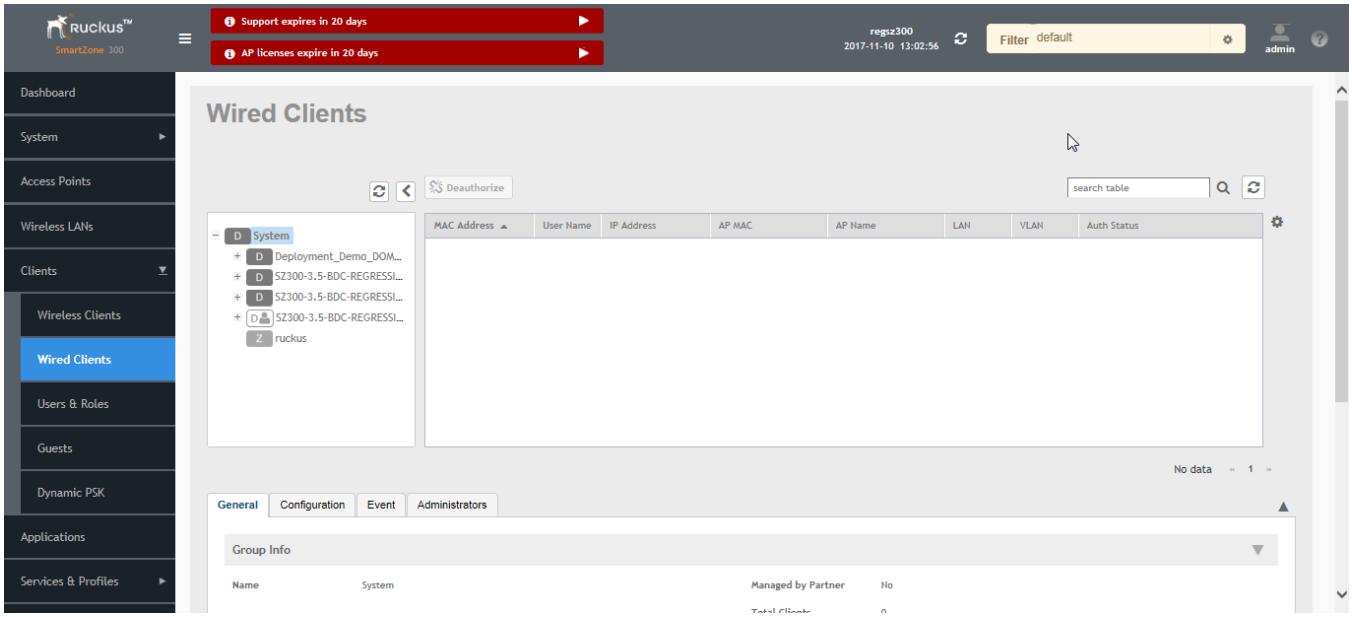
KPI	Description
Data Rate (down)	Displays the rate at which data is transmitted from the AP to the wireless client.
Auth Method	Displays the authentication method used by the AP to authenticate the wireless client.
Auth Status	Indicates whether the wireless client is authorized or unauthorized to access the WLAN service.
Encryption	Displays the encryption method used by the AP.
Control Plane	Displays the name of the 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 the following 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.

TABLE 7 KPIs for Wired Clients (continued)

KPI	Description
User Name	Displays the name of the user logged on to the wired client.
IP Address	Displays the IP address assigned to the wireless 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.
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**. The following table 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, 7 days and 30 days.
Memory status	CPU/memory/disk free usage/interface usage/ are available for 8 hours, 24 hours, 7 days 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.

TABLE 8 KPIs for the system (continued)

KPI	Description
	• 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

DHCP Relay (DP)

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

The following 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's web interface.

FIGURE 6 DHCP relay

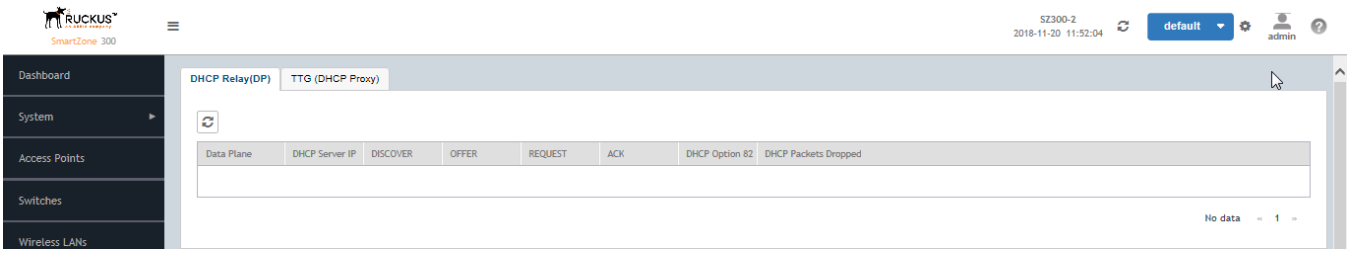


TABLE 9 KPIs for DHCP relay

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.

TTG (DHCP Proxy)

The controller has 3GPP-defined Tunnel Terminating Gateway (TTG) functionality. To view the KPIs, navigate to **Diagnostics** > **DHCP** > **TTG (DHCP Proxy)**.

The following table lists the key performance indicators related to the TTG (DHCP Proxy).

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 7 DHCP (DHCP Proxy)

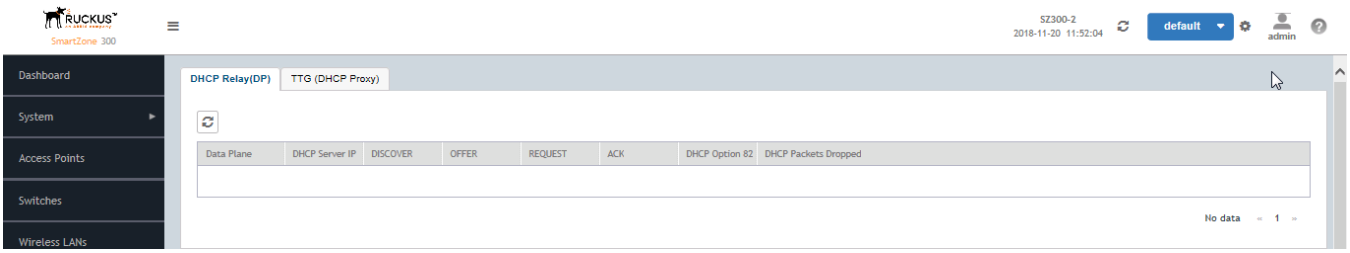


TABLE 10 KPIs for TTG (DHCP Proxy)

KPI	Description
Data Plane	Indicates the data plane name.
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.
NAK	Indicates the number of DHCP not acknowledged messages received from the DHCP server.
ACK	Indicates the number of DHCP acknowledgment messages received from the DHCP server.
DISCOVER	Indicates the number of DHCP discover messages forwarded to the DHCP server.
RELEASE	
DECLINE	Indicates the number of DHCP decline messages received.
DROP	Indicates the number of DHCP decline messages dropped.
INFORM	Indicates the number of DHCP inform messages received.
OTHERS	

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 8 RADIUS server

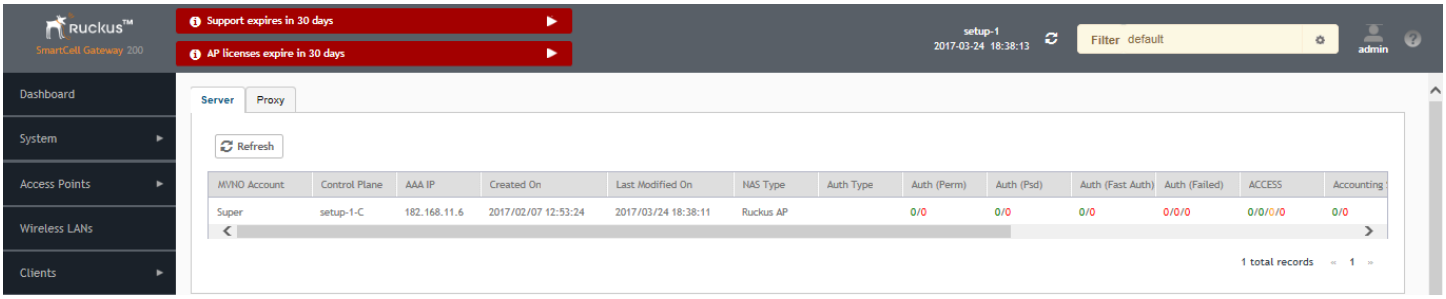


TABLE 11 KPIs for RADIUS server

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.
Last 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).
Accounting Session	Indicates the number of accounting sessions established (successful / failed).
Accounting Request	Indicates the number of RADIUS accounting requests received / number of RADIUS accounting accepts sent.
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 following table 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 9 RADIUS proxy

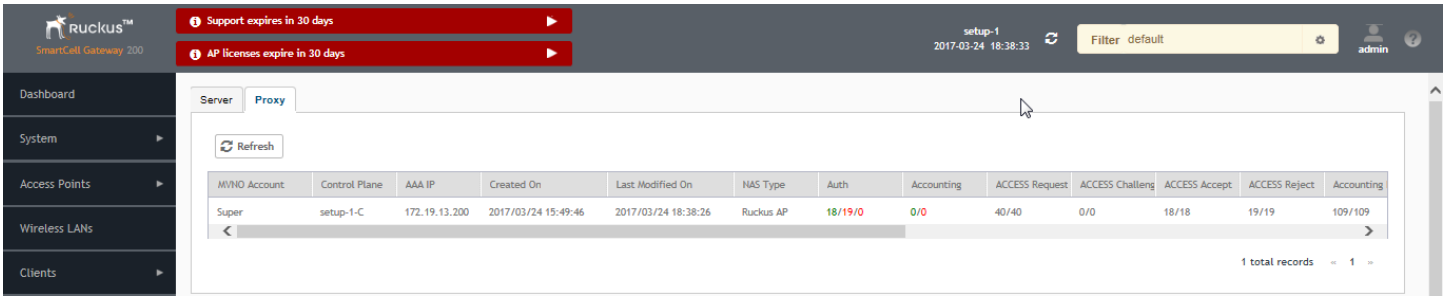


TABLE 12 KPIs for RADIUS proxy

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.
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). The numbers are reset if the auth AAA session is reset.
Accounting	Indicates the number of accounting sessions established (successful / failed). The numbers are reset if the acct AAA session is reset. AAA failovers are also counted.
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).
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).

TABLE 12 KPIs for RADIUS proxy (continued)

KPI	Description
CoA Autz Only	Indicates the number of RADIUS authorize only requests.

GGSN Connection

To view the KPIs, navigate to **Diagnostics** > **GGSN** > **GGSN Connection**. The following table lists the key performance indicators related to GGSN Connection.

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

FIGURE 10 GGSN Connection

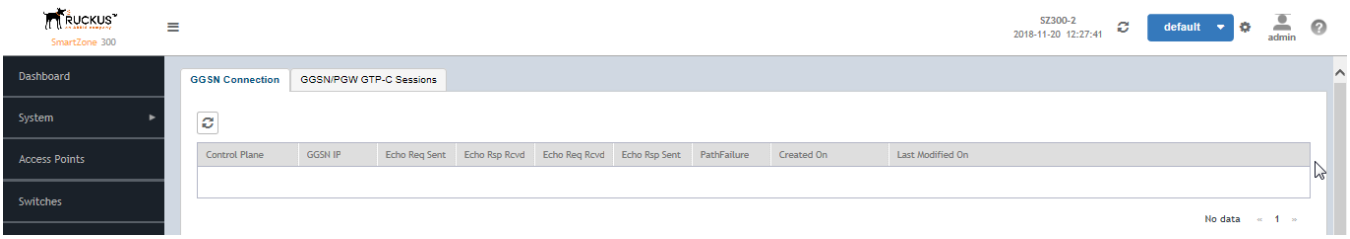


TABLE 13 KPIs for GGSN Connection

KPI	Description
Control Plane	Indicates the control plane name.
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.
PathFailure	Indicates the number of times GGSN 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.

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 11 GGSN/PGW GTP-C session

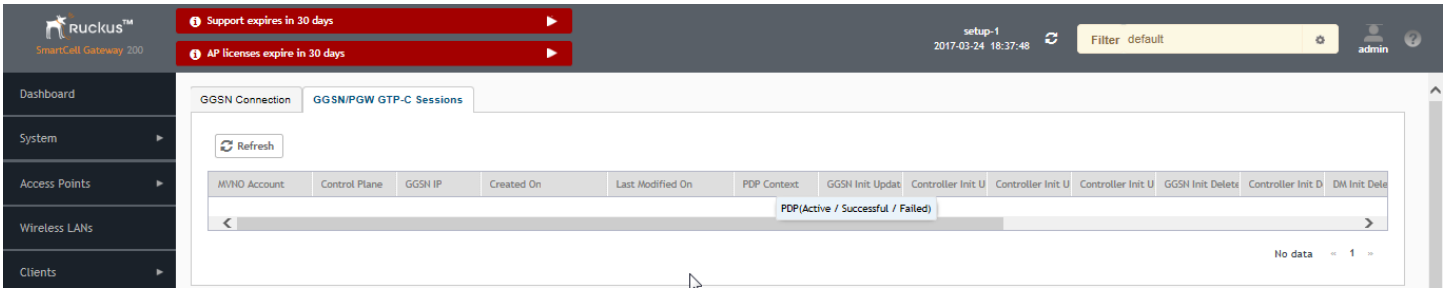


TABLE 14 KPIs for GGSN/PGW GTP-C connection

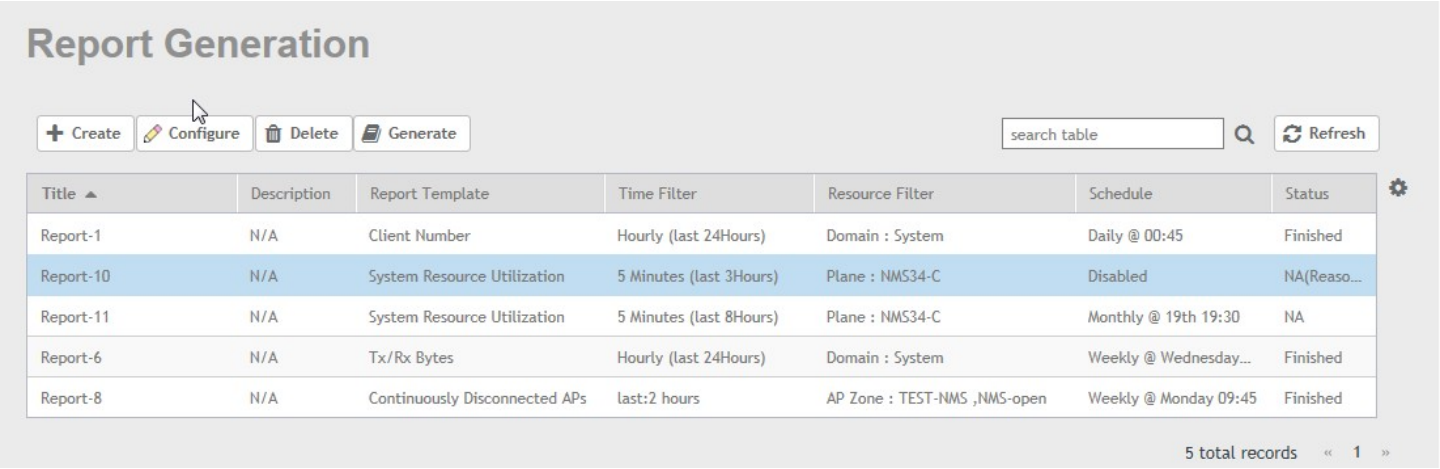
KPI	Description
MVNO Account	Indicates the mobile virtual network operator account.
Control Plane	Indicates the control plane name.
GGSN IP	Indicates the IP address of the GGSN node.
Created On	Indicates the date and time the service was created.
Last Modified On	Indicates the date and time the service was last modified.
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).
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).

Reports

Report Generation

Report Generation lists the reports that have been created and saved. 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 12 Report Generation



All the controller's reports can be displayed in different time intervals (hourly, daily, or monthly) for the specified time filter (in hours) and exported in 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 26
- Continuously Disconnected APs Report on page 26
- System Resource Utilization Report on page 26
- Tx/Rx Bytes Report on page 26
- Switch Traffic Statistics on page 26

Client Number Report

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

All bytes specific to user traffic are counted in this report. The count does not include the management frame.

Switch Traffic Statistics

Generates traffic statistics of switches, which includes the packets of InFrame, OutFrame, InMulticast, OutMulticast, InBroadcast, and OutBroadcast. The number of InError, CrcError and InDiscard are also included.

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 connect sit 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 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**.

The following table contains the report for UE session statistics. 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 13 Historical client statistics

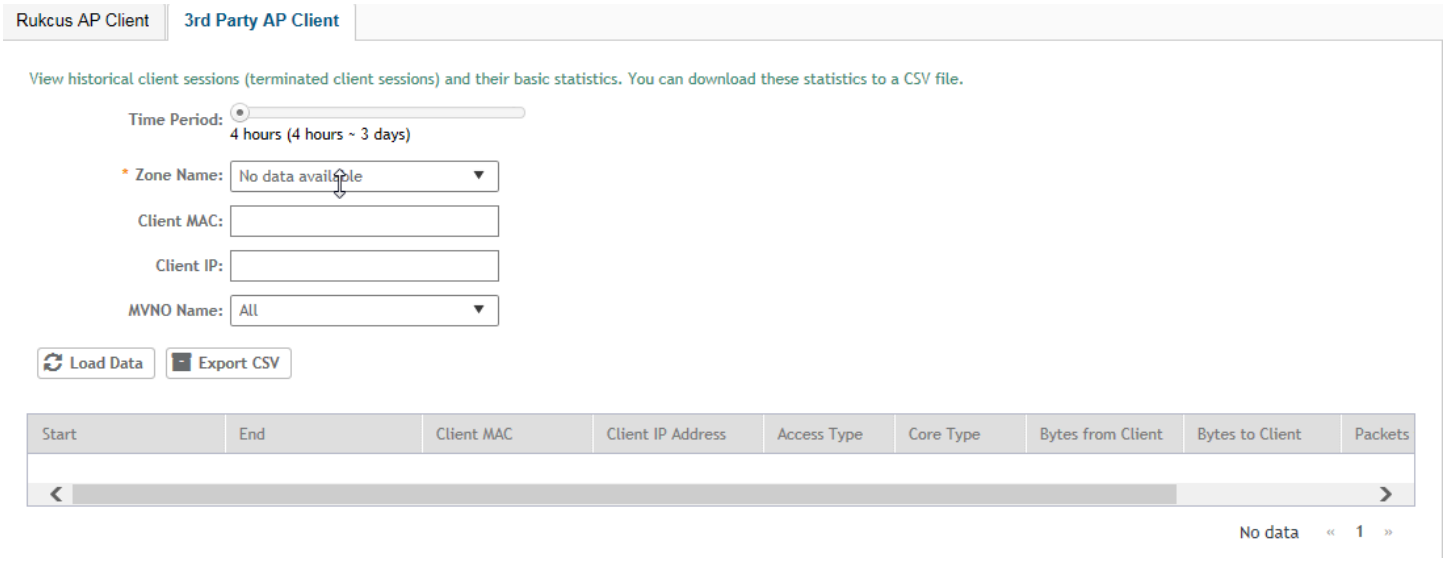


TABLE 15 Historical data attributes

Attribute	Type	Description
Start	Long	Indicates the session creation time.

TABLE 15 Historical data attributes (continued)

Attribute	Type	Description
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.

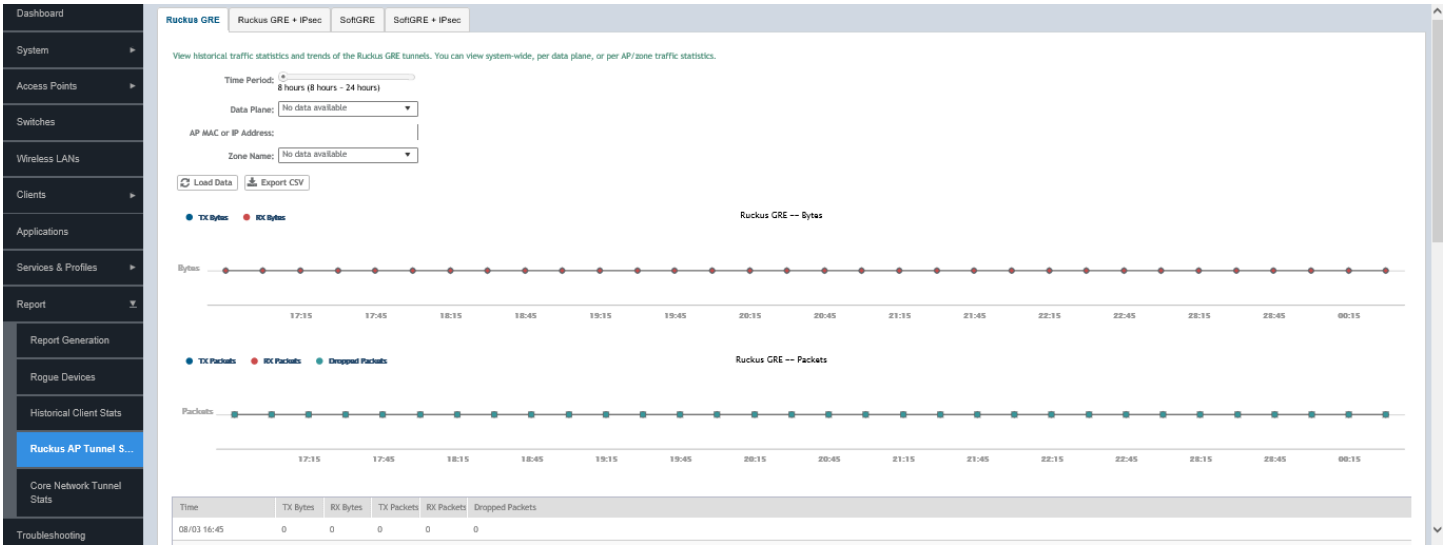
Ruckus AP Tunnel Stats

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

Ruckus AP Tunnel GRE Report

The controller's web interface (**Report** > **Ruckus AP Tunnel Stats** > **Ruckus GRE**) displays the table and its corresponding graph chart for a time period of 8 to 24 hours, as seen in the following figure. 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 14 Ruckus GRE report



The following table contains the report based on the statistics for access Ruckus GRE. Each entry contains the 15 minutes cumulative data.

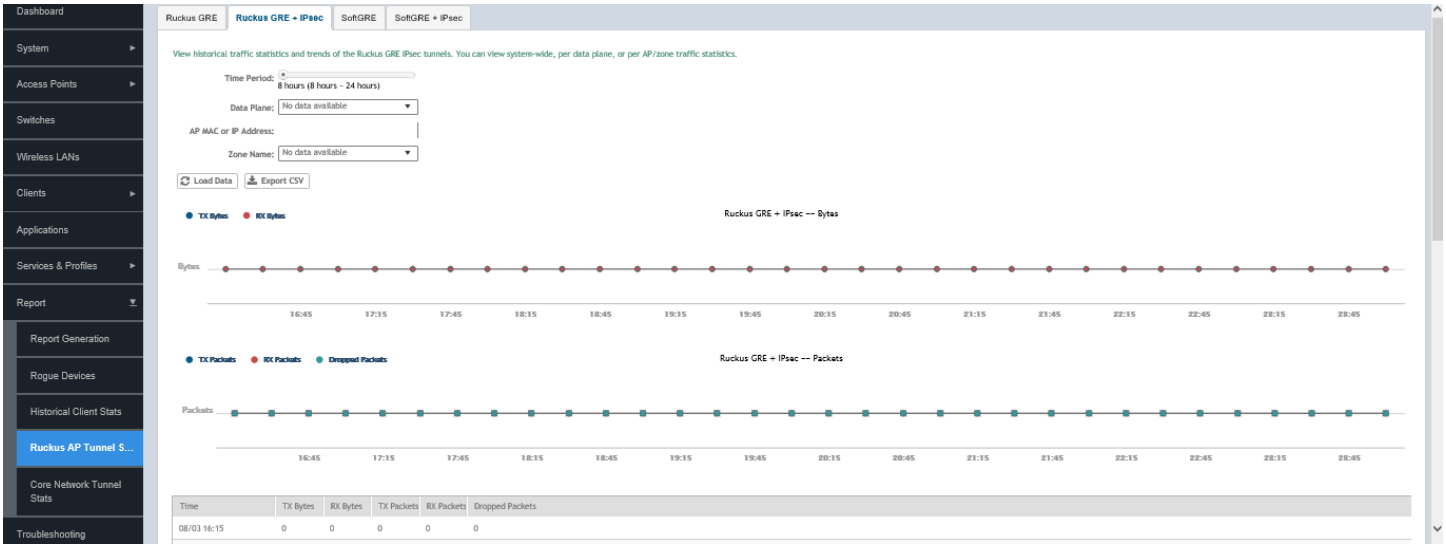
TABLE 16 Ruckus GRE report attributes

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 GRE + IPSec Report

The controller's web interface (**Report** > **Ruckus AP Tunnel Stats** > **Ruckus GRE + IPSec**) displays the table and its corresponding graph chart for a time period of 8 to 24 hours, as seen in the following figure. 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 15 Ruckus GRE + IPSec report



The following table contains the report based on the statistics for access Ruckus GRE +IPSec. Each entry contains the 15 minutes cumulative data.

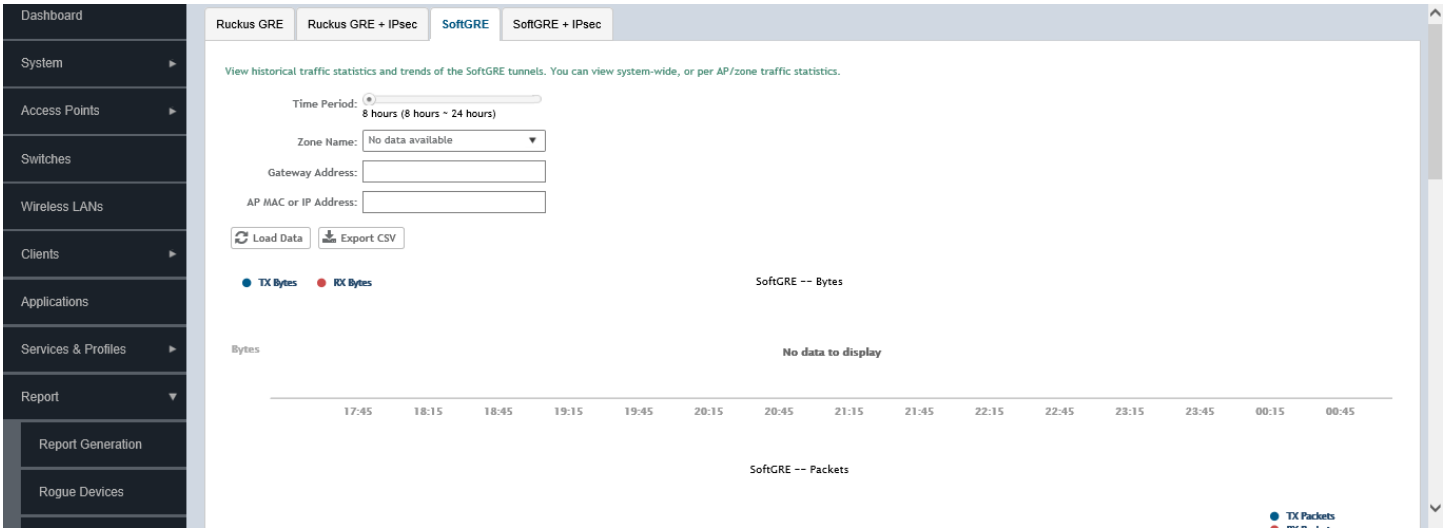
TABLE 17 Ruckus GRE + IPSec report attributes

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.
Dropped Packets	Long	Indicates the number of packets dropped.

Ruckus AP Tunnel SoftGRE Report

The controller's web interface (**Report** > **Ruckus AP Tunnel Stats** > **SoftGRE**) displays the table and its corresponding graph chart for a time period of 8 to 24 hours, as seen in the following figure. 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 16 Ruckus AP Tunnel SoftGRE Report



The following table contains the report based on the statistics for access point Soft GRE. Each entry contains the 15 minutes cumulative data.

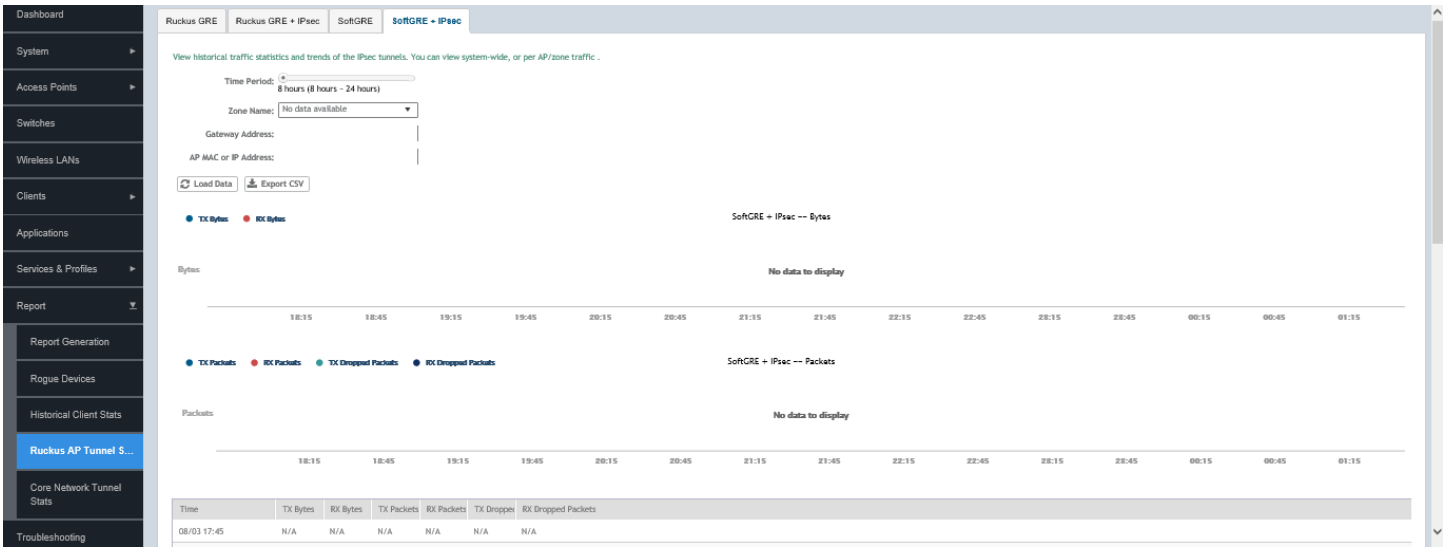
TABLE 18 Ruckus AP Tunnel SoftGRE Report Attributes

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

The controller's web interface (**Report** > **Report AP Tunnel Stats** > **SoftGRE + IPsec**) displays the table and its corresponding graph chart for a time period of 8 to 24 hours, as seen in the following figure. 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 17 Ruckus AP Tunnel SoftGRE + IPsec Report



The following table contains the report based on the statistics for access point IPsec. Each entry contains the 15 minutes cumulative data.

TABLE 19 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.

Core Network Tunnel Stats

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

Core Network Tunnel L2oGRE Report

The following table 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 Stats** > **L2oGRE**) displays the table and its corresponding graph chart as seen in the following figure. 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 18 Core Network Tunnel L2oGRE Report

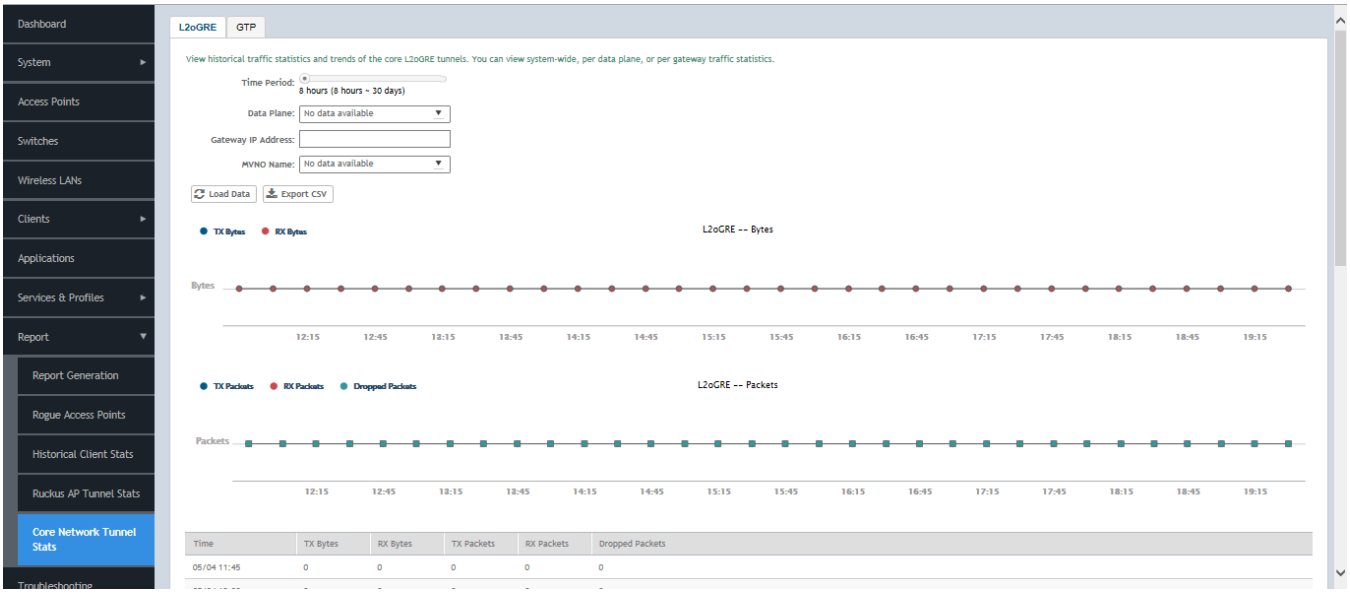


TABLE 20 Core Network Tunnel L2oGRE Report Attributes

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

© 2019 CommScope, Inc. All rights reserved.
Ruckus Wireless, Inc., a wholly owned subsidiary of CommScope, Inc.
350 West Java Dr., Sunnyvale, CA 94089 USA
www.ruckuswireless.com