





QUICK START GUIDE

QoE Appliance

Release 4.20



Reservation of Rights

Cambium reserves the right to make changes to any products described herein to improve reliability, function, or design, and reserves the right to revise this document and to make changes from time to time in content hereof with no obligation to notify any person of revisions or changes. Cambium recommends reviewing the Cambium Networks website for the latest changes and updates to products. Cambium does not assume any liability arising out of the application or use of any product, software, or circuit described herein; neither does it convey license under its patent rights or the rights of others. It is possible that this publication may contain references to, or information about Cambium products (machines and programs), programming, or services that are not announced in your country. Such references or information must not be construed to mean that Cambium intends to announce such Cambium products, programming, or services in your country.

Copyrights

This document, Cambium products, and 3rd Party software products described in this document may include or describe copyrighted Cambium and other 3rd Party supplied computer programs stored in semiconductor memories or other media. Laws in the United States and other countries preserve for Cambium, its licensors, and other 3rd Party supplied software certain exclusive rights for copyrighted material, including the exclusive right to copy, reproduce in any form, distribute and make derivative works of the copyrighted material. Accordingly, any copyrighted material of Cambium, its licensors, or the 3rd Party software supplied material contained in the Cambium products described in this document may not be copied, reproduced, reverse engineered, distributed, merged or modified in any manner without the express written permission of Cambium. Furthermore, the purchase of Cambium products shall not be deemed to grant either directly or by implication, estoppel, or otherwise, any license under the copyrights, patents or patent applications of Cambium or other 3rd Party supplied software, except for the normal non-exclusive, royalty free license to use that arises by operation of law in the sale of a product.

Restrictions

Software and documentation are copyrighted materials. Making unauthorized copies is prohibited by law. No part of the software or documentation may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, without prior written permission of Cambium.

License Agreements

The software described in this document is the property of Cambium and its licensors. It is furnished by express license agreement only and may be used only in accordance with the terms of such an agreement.

High Risk Materials

Cambium and its supplier(s) specifically disclaim any express or implied warranty of fitness for any highrisk activities or uses of its products including, but not limited to, the operation of nuclear facilities, aircraft navigation or aircraft communication systems, air traffic control, life support, or weapons systems ("High Risk Use").

This product is not restricted in the EU. Any High Risk is unauthorized, is made at your own risk and you shall be responsible for any and all losses, damage or claims arising out of any High-Risk Use.

© 2024 Cambium Networks Limited. All rights reserved

Contents

Contents	
Chapter 1: About This Guide	5
Chapter 2: Product Description	
Chapter 3: Hardware Configuration	7
Chapter 4: Network Deployment	
External bypass device	
Defining a bypass link	
Chapter 5: Accessing User Interface (UI)	
Chapter 6: Configuring QoE	
Configuring management interface	
Management interface firewall	
Setting time zone	14
Setting TCP acceleration	
Wire configuration	
Chapter 7: QoE Functionalities	
Basic concepts for QoE configuration	
Profiles	
Subscriber flow policies	
Shaping per subscriber	20
Burst options	
Shaping per flow	
Blocking incoming traffic	
Subscriber rate policies	
Automatic Congestion Management (ACM)	25
Rules	
APIs	
RADIUS API	
REST API	

Subscriber identification	
Subscriber flows decision tree	
Subscriber rate decision tree	
Checking the policy and subscribers	
Policy examples	
Chapter 8: Connecting to the QoE License Server	
Chapter 9: Traffic and Latencies	
Average Internet Latency per Service	
Chapter 10: Analytics	
Chapter 11: Denial of Service (DoS)	41
Chapter 12: Updating the Software	
Glossary	
Cambium Networks	

Chapter 1: About This Guide

This Quick Start Guide assists operators in acquiring a high-level understanding of the following QoE platform:

- <u>Hardware</u>
- Installation method
- Initial login procedures
- Configuration.

Chapter 2: Product Description

The QoE product provides a centralized traffic management solution that allows the Wireless Internet Service Provider (WISP) operator to manage network traffic. The following operations can be configured by QoE:

- Application-level shaping: to limit the rate of certain applications.
- Subscriber rate limiting: to limit the subscriber rate.
- TCP optimization: to optimize TCP flows by working as TCP a proxy that manages the TCP sessions by:
 - Acknowledging TCP packets on behalf of the receiver
 - Retransmitting TCP segments on behalf of the sender
 - Controlling the TCP flow to increase or decrease the session rate based on the session health.
- Denial of Service (DoS) attack detection: QoE can be configured to detect DoS and generate a report for the potential attacks. It does not act on the attack. It does not mitigate and block the attack.
- Application Insight: QoE provides an insight into the traffic consumed by applications.

The Advantech FWA-1112VC hardware, when running on QoE, can manage and accelerate traffic up to 1 Gbps.

Chapter 3: Hardware Configuration

This chapter describes the hardware configuration of the QoE appliance.



Figure 1: QoE hardware -Front view





The default QoE appliance configuration of the system are explained in Table 1.

Table	1: QoE	appliance	configuration	n.
TUDIC	1. 0.0 L	appnance	configuratio	ł

Port number	Description			
0	Management port: 192.168.0.121/24, gateway: 192.168.0.1, no VLAN.			
3	Port en0o4 is not configured and should not be used.			
1 and 2,	The remaining port pairs are bridged to form a wire, as follows:			
4 and 5	 Ports (en0o2 and en0o3) for Wire 1 which is GigE (1 G) 			
	• Ports (en0o5 and en0o6) from Wire 2, which is SFP+ (10 G)			

The default QoE configuration is explained in Table 2.

Table 2: QoE configuration

Port number	Description
1	Port (en0o2): AP interface of Wire 1. APs are connected to this port.

Port number	Description
2	Port (en0o3): Internet interface of Wire 1. The Internet interface is connected to this port.
4	Port (en0o5): AP interface of Wire 2. APs shall be connected to this port.
5	Port (en0o6): Internet interface of Wire 2. The Internet interface shall be connected to this port.



Attention

Ensure that the APs and the Internet links are connected to the correct port. This is very important for proper TCP acceleration operation. If they are swapped, the TCP optimizer shows a warning message and impacts the optimization performance.

Chapter 4: Network Deployment

The QoE functionality is required to view the subscribers' individual IP addresses (to limit each subscriber's maximum rate). It is important to deploy the QoE platform in a network where there is no NAT between the QoE and the subscribers.



Figure 3: Network deployment

It is recommended that a bypass path is established between the neighboring nodes of the QoE (Access and Internet Gateways in the diagram above). If there is a failure in the active link or the QoE, the traffic is automatically steered through the bypass path. Such bypass link can be set up at layer-2 (Example: Mikrotik's *active-backup* link bonding or an active-backup LACP setup) or layer-3 (Example: OSPF or BGP dynamic routing).



Note

Since the links are established directly between the two neighboring nodes, transparently with the QoE in the middle, the link monitoring mechanism should not be electrical (Example: MII), but based on messages (Example: ARP or fast LACP).

External bypass device

A bypass device is connected to the external links and the QoE. The device triggers an internal bypass if it detects the QoE is down (monitoring takes place through a USB connection between the QoE server and the Niagara). A bypass device is enabled by selecting Normal in **Configuration > Interfaces > Bypass**. It is also possible to force the bypass from the QoE with the option Forced Bypass in the same screen.

Figure 4 shows the bypass device connection that is connected to the external links and the QoE.



Figure 4: External bypass device

Note



Only Niagara devices are supported in this release.

Defining a bypass link

A bypass link can be set up at layer-2 (for example, Mikrotik's active-backup link bonding, or an activebackup LACP setup) or layer-3 (for example, OSPF or BGP dynamic routing). Since the links are established directly between the two neighboring nodes, transparently with the QoE in the middle, the link monitoring mechanism should not be electrical (for example, MII), but based on messages (for example, ARP or fast LACP).



Figure 5 shows how to define a bypass link.

Figure 5: Defining a bypass link

Chapter 5: Accessing User Interface (UI)

The QoE has a web-based UI used to perform the common management tasks. Web browsers such as

Chrome, Firefox, Safari, and Microsoft Edge are supported. Click the Help icon (¹) on the top-right of the UI to access the corresponding contextual help page.



The MS Explorer browser is not supported.

To access the management UI, navigate to <u>https://192.168.0.121</u> and type the below username and password.

• Username: admin

Note

• Password: cambium

The home page has a lateral menu, a dashboard, and a small summary of system information.

The dashboard displays all the icons in **Green**. The network interfaces icon will not be in green until all the configured wires are connected (if there are interfaces that are not used in any of the configured wires, it remains in orange) and the icon traffic will not be in green until traffic flows through the QoE. In some icons, clicking on them navigates to a window with more information about the QoE status.

If Cambium Networks logo is not displayed at the top-left corner of the UI, then refer to **QoE Appliance Installation Guide** and execute the **Step 5** of *Automatic setup* procedure.

An overview of the user interface is given in Figure 6.

			👱 cambiur	nsupport@bqn50 🗸	
DASHBOARD				(?) C	
System Name	bqn50	CPU NORMAI	Disk NORMAI	Network Interfaces	
BQN Release Hardware ID	R4.14.2 0x546586E5				
Serial Number System Time	GRCFCP2 2023-07-03 12:15:44 -0700	NORMAL	NORMAL	NORMAL	
License Limit License Expiration	3000 2023-11-14T23:02:24-0700		License NORMAL	Billing System Sync NORMAL	
		_		_	
Downlink		Uplink			
2.301 Gbps	227.059 Кррз	261.958	/lbps 16	56.406 Кррз	
Shaping Percentage	3.9 %	Shaping Percentage		1.4 %	
Rate-limit Percentage	100.0 %	Rate-limit Percentag	Rate-limit Percentage 96.4 %		
Access Latency	7.5 ms	Internet Latency		13.9 ms	
				_	
98%		5,368	5,368 1		
TCP Optimized		Subscribers		Flows	
	DASHBOARD System Name BQN Release Hardware ID Start Time Serial Number System Time License Limit License Expiration Downlink 2.301 Gbps Shaping Percentage Rate-limit Percentage Access Latency TCP Optimized	DASHBOARD System Name bqn50 BQN Release R4.14.2 Hardware ID 0x546586E5 Start Time 2023-06-12 15:09:42-0700 Serial Number GRCFCP2 System Time 2023-07-03 12:15:44-0700 License Limit 3000 License Expiration 2023-11-14T23:02:24-0700 Downlink 2.3001 Gbps 227.059 Kpps Shaping Percentage 3.9 % Rate-limit Percentage 100.0 % Access Latency 7.5 ms	DASHBOARD System Name bqn50 BQN Release R4.14.2 Hardware ID 00x54658655 Start Time 2023-07-12 15:09:42-0700 Serial Number GRCFCP2 System Time 2023-07-03 12:15:44-0700 License Limit 3000 License Expiration 2023-11.14T23:02:24-0700 Downlink 2.3001 Gbps 2.27.059 Kpps Shaping Percentage 3.9 % Rate-limit Percentage 3.9 % Rate-limit Percentage 100.0 % Access Latency 7.5 ms Difference Construction 2023-11.14T23-02:24-0700 Shaping Percentage 100.0 % Shaping Percentage 100.0 % Shaping Percentage 5.9 % Babala Percentage 100.0 % Shaping Percentage	▲ Carbon ▲ Carbon	

Figure 6: User interface

Chapter 6: Configuring QoE

This chapter describes the configuration of the QoE appliance. It includes the following topics:

- <u>Configuring management interface</u>
- Setting timezone
- Setting TCP acceleration
- Wire configuration

Configuring management interface

To change the settings of the management interface, perform the following procedure:

1. Navigate to Configuration > Interfaces > Management.

IP settings include the IP address and mask, the default gateway, and the VLAN identifier (if any).

\bigcirc	Note				
ŕ'n					
\cup	Confi	gure management ne	etwork	(interface to en0o1 .	
Cambium Ne	etworks™ uant Technology				💄 admin@cnInsight 🗸
Dashboard	A	-			
Status	+	MANAGEMENT INTERFACE SETTINGS Press Apply Configuration button at the end of the page	e to set the new con	figuration values.	C
1. Statistics	+	Network Interface		Static IP address and mask	
Configuration		Management network Interface.		Management network static IP address and mask.	
Interfaces		Interface en0o1	~	IP address 10.120.212.250 / 24	
Management		VLAN		Default gateway	
Management Firev	vall	Management network Interface VLAN ID.		Optional. Default gateway and static IP address must be in the same subnet.	
Data Wires		VLAN ID None	~	IP address 10.120.212.254	
Profiles	+			DNS server	
Subscriber Flows				Optional. If DNS server and static IP address are not in the same subnet, default gateway is	
Subscriber Rates				mandatory.	
Radius				IP address 10.120.12.169	
REST API					
DoS					Apply Configuration
TCPO Settings					

Figure 7: Configuring management interface

2. Configure an optional DNS server IP address.



Administration

Note

Do not change the network interface used for management, unless indicated by the Cambium Networks support personnel.

3. After completing the new settings, click **Apply Configuration** to apply the changes.

Connecting back to the node requires access from the new subnet and logging back into the UI.

Management interface firewall

To set up the management interface firewall, which applies only to the management interface (not to the interfaces configured in wires), perform the following steps:

1. Navigate to **Configuration > Interfaces > Management Firewall**.

Cambium Netwo	orks™ chnology	👤 adr	nin@cnInsight 🗸
Dashboard		A	
	_	MANAGEMENT INTERFACE FIREWALL	0 C :
Status	+		
1. Statistics	+	No firewall rules configured: all IP addresses allowed.	
Configuration	-		_
Interfaces	-		
Management			
Management Firewall			
Data Wires			
Bypass			
Profiles	+		
Subscriber Flows			
Subscriber Rates			
RADIUS			
REST API			
DoS			
TCPO Settings			
cnMaestro Settings			
🔌 Administration	+	*	

The IP address ranges allowed to access the management interface is displayed. By default, no IP address ranges are configured, and all are allowed.

2. To add an allowed IP address range, click ⁱ icon and Add IP Address Range....

When one IP address range is allowed, the firewall is enabled and all IP addresses not covered by the configured IP address ranges are blocked.



Note

It is important to include an IP address range that includes the IP address from which the user is accessing the UI and the subnet of the management IP address.

Setting time zone

To change local date and time, click **Apply Date** and **Apply Zone**. Enter initials of the country of interest (for example, ES for Spain) in **System Date & Time** window through the list of time zones. By default, the system is set to **Central Standard Time Zone (Chicago, IL, USA)**.

To change the system time zone, perform the following steps:

1. Navigate to Administration > System Date > Set Date & Time from the home page.

The **System Date & Time** page appears, as shown below:

Cambium Netwo	orks ^{tor}	🛓 admin@onl	nsight 🗸
Dashboard			
		SYSTEM DATE & TIME	c
Status	+		
1. Statistics	+	Current Date: 2022-01-16 21:59	
Configuration	+	Year 2022 û Month 01 û Day 16 û Hour 21 û Min 59 û ApplyDate	
Administration	-		
Backup	+	Time Zone: US America/Lincago • Approvidence	
System Date	-		_
NTP Servers			
Set Date & Time			
Diagnostic			
License			
Software			
Users			
Reboot			
Shutdown			
1 About			

- 2. Set the date and time and, click **Apply Date**.
- 3. Select the time zone from the drop-down and click Apply Zone.

Setting TCP acceleration

By default, TCP Optimization is enabled for all TCP flows. Some TCP flows can be excluded from TCP optimization by turning off the **TCP Optimization** option in the appropriate subscriber flow policy.

To change the TCP Optimization setting, perform the following steps:

1. Navigate to **Configuration > Subscriber Flows** from the home page.

The Subscriber Flows Configuration page appears as shown below:

	Cambium Network	KS [™] alogy					💄 admin@cnInsight 🗸
55	Dashboard		SUBSCRIBER FLOWS CONFIGURATION				0 C ;
0	Status	+					
ıl.	Statistics	+	RULES TREE-VIEW RULES TABLE-VIEW POLICIES				
۵	Configuration	-	INTERNET	ACCESS	THROUGHPUT	DPI	POLICY RULE ACTIONS
	Interfaces	+					
	Profiles	+	voip				flow-no-rate-limit
	Subscriber Flows		0	0	0	0	2 🖍 🔳
	Subscriber Rates		root				
	Radius		~	subs-no-tcpo	0	0	flow-no-tcpo
	REST API				0	0	
	DoS		any-other		above-5Ghpr	video-streaming	flow-RMhns
	TCPO Settings						
	cnMaestro Settings			any-other		U	
٩	Administration	+		-0-<	any-other	_	flow-default
0	About				0	0	

2. Click the appropriate flow policy (for example, flow-default).

The EDIT SUBSCRIBER FLOW POLICY page appears, as shown below:

EDIT SUBSCRIBER FLOW POLICY			
Name flow-8Mbps			
Block: disabled			
TCP Optimization: enabled			
TCP Advanced Parameters	~		
Downlink shaping per Subscriber: enabled		Uplink shaping per Subscriber: enabled	•
Max rate per Subscriber	8.000 Mbps 🗘 ⊠	Max Rate per Subscriber	4.000 Mbps 🗘 🚳
Burst Options	•	Burst Options	۷
Downlink shaping per Flow: disabled		Uplink shaping per Flow: disabled	
Drop Incoming Connections	•		
Skip subscriber rate limitation: disabled			
			Apply Cancel

- 3. Enable or disable TCP Optimization.
- 4. Click **Apply** to save the configuration.

Wire configuration

A wire is a network interface pair processing subscriber traffic.

To configure wires, perform the follwing steps:

1. Navigate to **Configuration > Interfaces > Data Wires**.

The Wires Configuration page appears as shown below:

Cambium Net	tworks [™] Int Technology							👱 admi	n@cnInsight 🗸
Dashboard	A								
Status	+	WIRES CONFIGURATION Press Apply Configuration button at t	he end of the page to set the ne	w configuration valu	ies.				0 C :
d. Statistics	+	ACCESS INTERFACE	UP	LINK	INTERNET INTERFACE	UP	LINK	ACTIONS	
Configuration		en0o2	\checkmark	~	en0o3	~	~	≣ ∉	
Interfaces	-	en0o6	~	×	en0o5	~	×	∎ ≓	
Management									
Management Firewa	311								
Data Wires									
Profiles	+								
Subscriber Flows									
Subscriber Rates	_								
Radius									
REST API									
DoS	_								
TCPO Settings	_								
cnMaestro Settings									
Administration	+								
~	-								

Wires are directional, with the first network interface connected to the access towards the subscribers and the second interface on the Internet side.



Warning

If any mistake happens while connecting the ports, then click 😅 icon to swap.

2. To add a wire, click [‡] icon and select **Add Wire...**.

A form allows selecting the access and Internet interfaces (the form lists the available interfaces).

3. To remove a wire, click delete icon.

Note



Do not delete the wires unless indicated by the Cambium Networks support personnel, as misconfiguration may lead to service loss.

4. Click Apply Configuration to apply the changes.

Chapter 7: QoE Functionalities

QoE supports the following functionalities on the traffic processed:

- TCP Optimization (TCPO)
- Limit application speeds on a per-application basis (shaping)
- Limit the maximum total speed of a subscriber (rate plan management)
- DoS attacks detection
- Usage monitoring per subscriber and per application

Basic concepts for QoE configuration

All IP data packets that flows through QoE belong to a subscriber and a flow. The QoE acts on traffic grouped per subscriber and per flow.

- A subscriber refers to an IPv4 address on the access side, or any IPv6 address from the same or 64 subnet on the access side. Refer to Subscriber Identification section for more details.
- A flow is a TCP connection, a UDP flow, or a flow with another protocol (for example, ICMP ping). A subscriber can have many flows at the same time.

To decide the corresponding functionality to the flows or subscribers, QoE uses the following three concepts:

- **Policies** define the actions to perform on the traffic, along with action parameters (for example, a speed limit).
- **Profiles** classify the traffic according to certain criteria (for example, an access profile identifies all the traffic from subscribers whose IP address is within the set of IP address ranges in that access profile).
- **Rules** relate to policies and profiles (for example, a rule may specify that some specific access profiles are limited by a rate policy. That is, subscribers whose IP addresses are in same subnet which contain a specific rate limit).

Profiles

Profiles classify the traffic and help to determine the rules and policies that are applied to the each subscriber and flow. There are different profile types, according to the properties being used for classification. To configure the profile, navigate to **Configuration > Profiles** from the home page.

The current version supports the following profile types:

- Interface Profile identifies the flows or subscribers whose first data packet comes in through a network interface within the list of network interfaces specified by the interface profile.
- VLAN Profile identifies the flows or subscribers whose first data packet uses a VLAN tag within the set of VLAN tags (or the absence of any tag) specified by the VLAN profile.

- **Policy-Rate Profile** is used to select the Flow Policies based on the Rate Policy of the subscriber. It is a list of Subscriber Rate Policy names, or patterns with wildcards. These profiles match the name of the subscriber rate policy assigned to the subscriber session.
- Internet Profile identifies the flows coming from or going to an IP address on the Internet side, contained in the set of IP address ranges specified by the Internet profile. Optionally, Internet side ports can also be specified (for example, port 80).
- Access Profile identifies the flows or subscribers coming from or going to an IP address on the access side, contained in the list of IP address ranges specified by the access profile. Optionally, access side ports can also be specified.
- **Time Time-based profile** activates the rule during a period of time. A time profile is a list of time ranges, and it is true if any of the ranges is true. The ranges within the same profile cannot overlap. A range can apply to all days of the week or just to a period of days.
- **Throughput Profile** identifies all the flows, which are created when the total downlink traffic going through the QoE is above the threshold specified by the throughput profile.
- DPI (Deep Packet Inspection) Profile identifies the flows that use an HTTP/HTTPS/QUIC. This domain is included in the list of HTTP/HTTPS/QUIC domains specified by the DPI profile. There are a set of pre-defined DPI signatures, which include the domains for popular applications (like the most important video streaming apps or the most common software updates).

Subscriber flow policies

When a new flow is created, a subscriber flow policy is assigned to it, which specifies how to treat all the flows within that subscriber, which share that same policy. The following are the actions that can be defined in a subscriber flow policy:

- **TCP Optimization**: It improves TCP traffic performance. It specifies whether to apply optimization to TCP traffic. It is recommended to set I to ON (the default value).
- Shaping per subscriber: It limits the speed to a given value. It is possible to limit the downlink and/or uplink direction. The limit applies to all flows matching the policy belonging to the same subscriber. For example, if a limit of 6 Mbps is specified for video streaming, and the subscriber has three video streaming flows from different servers, the three flows will share the 6 Mbps limit (getting around 2 Mbps for each subscriber). It is possible to define bursts that allow flows to exceed temporally the limit.
- Shaping per flow: It limits the speed of one flow to a given value. It is possible to limit in the downlink and/or uplink direction. The limit applies to any flow matching the policy. For example, if video streaming flows are assigned to a per flow 2 Mbps limit, a video flow cannot exceed those 2 Mbps. Shaping per flow can be combined with shaping per subscriber. For example, if there is a per subscriber 6 Mbps limit, and a 2 Mbps per flow, a subscriber with four flows has them limited to the 6 Mbps maximum (around 1.5 Mbps for each subscriber). Per flow shaping has no burst option. Because per-flow shaping is not applied per subscriber, it can be used even when there is a NAT between the QoE and the end subscribers.
- **Block**: It blocks all flows falling in the blocking policy, in both the directions, and does not allow to proceed. It should be used with care, to avoid affecting traffic different to the one intended.

• Skip subscriber rate limitation: The traffic from flows getting this policy does not affected by the rate limitation specified in the rate policy for this subscriber. They only gets the rate limitation specified by this flow policy (if any).

To configure the policies, navigate to **Configuration > Subscriber Flows**, and select the **POLICIES** tab.

Cambium Net	works [™] nt Technology					💄 admin@cnInsight 🗸
Dashboard						
Status	+	SUBSCRIBER FLOWS CONFIGU	IRATION			0 C :
d. Statistics	+	RULES TREE-VIEW RULES TABLE-VIE	W POLICIES			
Configuration	-	NAME	OPTIMIZATION	SHAPING-DOWN	SHAPING-UP	ACTIONS
Interfaces	+	flow-8Mbps	yes	8.000	4.000	/ 1
Profiles	+	flow-default	yes	no	no	11
Subscriber Flows	_	flow-no-rate-limit	ves	ne	ne	1 8
Radius			Prov			
REST API		flow-no-tcpo	no	no	no	/ •
DoS		flow-policy-example	yes	10.000	8.000	/ 1
TCPO Settings						
cnMaestro Settings						
Administration	+					
About						

Figure 8: Subscriber flow policies

Shaping per subscriber

Figure 9 defines a downlink speed limit of 10 Mbps, an uplink limit of 8 Mbps and bursts of 3 seconds of double the normal speed.

lock: disabled									
TCP Optimization: enabled					Compression: disabled				
TCP Advanced Parameters				*					
Downlink shaping per Subscri	ber: enable	d			Uplink shaping per Subscribe	r: enabled			
Max rate per Subscriber	10.	000 Mb	ps	≎ 🛛	Max Rate per Subscriber	8.0	000 Mb	ps	¢ 6
Burst Options				^	Burst Options				-
Burst Rate	20.000) Mbps	\$	⊠	Burst Rate	16.000	Mbps	\$	×
Burst Duration	3	seconds	\$	×	Burst Duration	3	seconds	٥	×
Burst Threshold	10.000	Mbps	¢	×	Burst Threshold	8.000	Mbps	\$	×
Burst Threshold Window	300	seconds	~ ~	≤	Burst Threshold Window	300	seconds	\$	×
	abled				Uplink shaping per Flow: disab	led			
ownlink shaping per Flow: dis									

Figure 9: Shaping per subscriber

Burst options

Bursts are configured under **Advanced** parameters of the appropriate direction (for example downlink shaping). Figure 10 displays the burst threshold, shaping rate and burst rate.

Burst policy is defined by four parameters:

- **Burst Rate**: Maximum rate during the burst, typically bigger than the normal shaping max rate (Example: allow a burst of 20 Mbps for flows normally limited to 10 Mbps).
- Burst Duration: Duration of the burst, for how long the burst rate can be sustained.
- Burst Threshold: An average speed that, if exceeded, prevents a new burst from happening. It is the way to control when a new burst can be granted. For example, for a 10 Mbps limit with 20 Mbps bursts, a 5 Mbps burst threshold will require the subscriber flows to drop the speed to half its normal limit before allowing a new burst.
- **Burst Threshold Window**: The period in seconds used to compute the average speed that is checked versus the threshold. The longer the window, the bigger the weight of past subscriber activity on the decision of grating a new burst.





Shaping per flow

It is possible to add a shaping per subscriber. Per flow and per subscriber shaping limits act at the same time. Per flow shaping limits the speed of individual flows and subscriber shaping limits the combined flow speed per subscriber.

Figure 11 is a policy with a limit per flow of 4 Mbps in either direction.

EDIT SUBSCRIBER FLOW POLICY Press Apply button at the end of the page to set the new configuration	i values.				
Name flow-4Mbps-per-flow					
Block: disabled					
TCP Optimization: enabled		Compression: disabled			
TCP Advanced Parameters	*				
Downlink shaping per Subscriber: disabled		Uplink shaping per Subscriber: disabled			
Downlink shaping per Flow: enabled		Uplink shaping per Flow: enabled			
Max Rate per Flow 4.000 Mbps		Max Rate per Flow 4.000	Mbps	\$	⊠
Drop Incoming Connections	*				
Skip subscriber rate limitation: disabled					
			App	ly	Cancel

Figure 11: Shaping per flow

Blocking incoming traffic

It is possible to block incoming traffic, initiated from the Internet (TCP connections, UDP flows or other IP traffic like ICMP pings). To perform this, there are **Drop Incoming Connections** section as part of a Subscriber Flow policy. Figure 12 displays the blocking incoming traffic options.

Blocking incoming Traffic	>		
It is possible to block incoming traff flows or other IP traffic like ICMP pi section as part of a Subscriber Flow EDIT SUBSCRIBER FLOW POLICY Press Apply button at the end of the page to set the new configurat	fic, initia ngs). To w policy. tion values.	ited from the Internet (TCP connections, UI do so, there are <i>Drop Incoming Connection</i>	DP Is
Name flow-default			
Block: disabled			
TCP Optimization: enabled		Compression: enabled	
TCP Advanced Parameters	*		
Downlink shaping per Subscriber: disabled		Uplink shaping per Subscriber: disabled	
Downlink shaping per Flow: disabled		Uplink shaping per Flow: disabled	
Drop Incoming Connections	^		
TCP Connections	\checkmark		
UDP Connections	\checkmark		
Other IP Connections	V		
Skip subscriber rate limitation: disabled			
		Apply	Cancel

Figure 12: Blocking incoming traffic

Subscriber rate policies

Subscriber rate policies are applied per subscriber. The following are the possible actions:

- Maximum downlink speed: The maximum speed in the downlink direction for all traffic going towards the subscriber's IP address.
- Maximum uplink speed: The maximum speed in the uplink direction for all traffic coming from the subscriber's IP address.
- Under Advanced Parameters, you can find the same burst options as for Subscriber Flow Policies.
- There is an Automatic Congestion Management (ACM) option, that detects congestion and select a rate limit automatically (off by default).

To configure policies, perform the following steps:

1. Navigate to **Configuration > Subscriber Rates** from the home page.

The Subscriber Rate Configuration page appears as shown below:

Camb	bium Networks [™] ated with bequant Technology		💄 adr	min@cnInsight 🗸
Dashboard		SUBSCRIBER RATE CONFIGURATION		0 C :
 Status 	+	RULES TREE-VIEW RULES TABLE-VIEW POLICIES		
II. Statistics	+			
Configuratio	n –	ACCESS POLICY	RULE	ACTIONS
Interfaces	+	subs-100Mbps rate-100M	bps	
Profiles	+	00	4	
Subscriber	Flows			
Subscribe	r Rates	subs-10Mbps rate-10M	ops	
Radius		0 0	5	
REST API		root		
DoS		subs-50Mbps rate-50M	ops	
TCP0 Setti	ngs		6	
cnMaestro	Settings			
🔌 Administrati	ion +	any-other rate-defa	ult	
About		00	7	/ 🖬

2. Select the **POLICIES** tab.

SUBSCRIBER RATE CONFI	GURATION				0 0
RULES TREE-VIEW RULES TAB	LE-VIEW POLICIES				
NAME	RATE-LIMIT-DOWN	RATE-LIMIT-UP	SOURCE	AUTO-CONG	ACTIONS
10down_Sup	10.000	5.000	static	no	/ 1
rate-100Mbps	100.000	100.000	static	no	/ 1
rate-10Mbps	10.000	8.000	static	no	∕ ≣
rate-50Mbps	50.000	50.000	static	no	∕ ≣
rate-default	no	no	static	no	∕ ≣

3. Click **Edit** icon to configure the policies.

ame rate-50Mbps				
lock: disabled				
Maximum subscriber downlink spe	ed: enabled	-	Maximum subscriber uplink speed	I: enabled
Rate	50.000	Abps 🗘 🛚	Rate	50.000 Mbps 🗘
Automatic Congestion Management	t		Advanced Parameters	
Advanced Parameters		^	Burst Rate	100.000 Mbps 🗘 🖣
Burst Rate	100.000 Mb	ps 🗘 🖾	Burst Duration	5 seconds 🗘
Burst Duration	5 secon	ds 🗘 🖾	Burst Threshold	50.000 Mbps 🗘 🍕
Burst Threshold	50.000 Mb	ps 🗘 💌	Burst Threshold Window	300 seconds 🗘 🕻
Burst Threshold Window	300 secon	ds 🗘 💌		

Refer to <u>Subscriber Identification</u> section to know how all the traffic from the same subscriber are identified.



Note

Policy changes takes minimum one minute to make the changes for the existing subscriber sessions.

Automatic Congestion Management (ACM)

When the subscriber rate limits are unknown, then the QoE can automatically detects them using machine learning. So the QoE becomes the bandwidth management element, and the network can be benefited from QoE reduced latencies. The ACM also detects the congestions below the subscriber rate limit when rate limits are known.

To enable the ACM from QoE configured Rate Policies, enable the **Automatic Congestion Management** of a Subscriber Rate Policy (typically the rate-default one). Figure 13 shows enabling ACM from QoE configured Rate Policies tab.

EDIT SUBSCRIBER RATE POLICY Press Apply button at the end of the page to set the new	configuration values.		
Name rate-default			
BIOCK: UISADIEU		Automatic Congestion Management enabled	
Maximum subscriber downlink speed: disabled		Maximum subscriber uplink speed: disabled	
		Apply	Cancel

Figure 13: Enabling ACM from QoE configured Rate Policies tab

To enable this feature in Dynamic Rate Policies from RADIUS, navigate to **Configuration > External Subscriber Data > RADIUS** and enable **Automatic Congestion Management**. Figure 14 shows enabling ACM from RADIUS tab.

RADIUS CONFIGURATIO	N g (%) value will be applied 3 seconds	after it is changed.	(?) C :
RADIUS service: enabled	-	•	
AVP Selection	•	Rate-Limit Scaling (%)	100 🗘 🖾
		Automatic Congestion Management: enabled	
Clients Table			
ADDRESS	DESCRIPTION	SECRET	ACTIONS
192.168.88.12		mysecrel	/ 1

Figure 14: Enabling ACM from RADIUS tab

Rules

Rules specify which policies are assigned to each subscriber and flow, as a function of how they match the profiles in the rule.

There are independent sets of rules for each policy type: subscriber flow rules select the appropriate subscriber flow policy for each flow, subscriber rate rules select the appropriate subscriber rate policy for each subscriber.

A rule can use one profile of each type (or use the **any** option, if the profile type is indifferent), and it defines only one policy to apply.

Every set of rules may have many rules, but only the one with the best match will be selected for each flow or subscriber. To evaluate the rules in a way that maximizes performance, profiles are checked in order. This pre-defined order determines which rule is finally selected. A tree-view of the rules helps in identifying which rule is selected in each case. See the *Decision Tree* sections for more information on the trees and the profile evaluation order.

Manually configured rule priorities are not used because of the performance penalties they entail and the burden on the operator to keep priorities consistent.

To configure subscriber flow rules, perform the following steps:

1. Navigate to **Configuration > Subscriber Flows** from the home page.

The Subscriber Flows Configuration page appears as shown below:



2. Select RULES TREE-VIEW or RULES TABLE_VIEW tab.

To configure the subscriber rate rules, navigate to Configuration > Subscriber Rates.



APIs

The QoE has two APIs to select subscriber rate policies, instead of using the QoE local rules, that act as a default. There are two APIs:

- RADIUS API
- REST API

RADIUS API

When QoE receives a RADIUS accounting indicating that a subscriber with an IP address has a rate policy, that policy is selected independently according to the configured rules. Rules apply only for subscribers without radius information.



Figure 15: Radius API

The QoE receives RADIUS *accounting*, configuring the RADIUS source (for example, a PPPoE server or a RADIUS server) to send accounting information to the QoE management IP address.

In the QoE UI, navigate to **Configuration** > **Radius** and set RADIUS as **ON**. On the top-right corner click and select **Add Client...** from the upper-right menu to configure the IP address of the radius accounting source and the secret used.

\bigcirc	Note
\Box	More than one source can be configured.

RADIUS CONFIGU	RATION imit Scaling (%) value will be applied 3 se	econds after it is changed.	(?) C
ADIUS service: enabled		•	
AVP Selection		✓ Rate-Limit Scaling (%)	100 💠 🛛
Clients Table			
Clients Table	DESCRIPTION	SECRET	ACTIONS
Clients Table ADDRESS 10.10.10.3	DESCRIPTION	SECRET radiussecret	ACTIONS
Clients Table ADDRESS 10.10.10.3	DESCRIPTION	SECRET radiussecret	ACTIONS

Figure 16: The RADIUS Configuration page

The supported **Radius** field specifies the rate policy that is Mikrotik Address List. The address list name must match the name given to the Subscriber Rate policy in the QoE.

REST API

A REST API allows QoE to be integrated into an external system (for example, a billing system) to receive instructions of which rate policy applies to the corresponding subscriber. The REST API is based on

HTTPS GET/POST /PUT/DELETE methods with JSON objects for exchanging information.

The REST API can be used to map policies configured in QoE to subscriber IP addresses. It also supports defining dynamic policies, that takes precedence over any local policy. To configure the REST API, navigate to **Configuration > REST API** in the UI.

\bigcirc	

Note

Add at least one user/password to authenticate rest requests and set the toggle ON. Optionally, the user can define the IP addresses from which the request will be allowed.

ST API CONFIGURATION			
est API service enabled		•	
ort: 3443			
llowed REST API Client IP Add	resses	REST API Users	
ADDRESS	ACTIONS	USER	PASSWORD
1.1.1.1	Î	apiadmin	admin
1.1.1.2	ĩ	restapi-1	password1
0.10.10.5	ii.	restapi-2	password2

Figure 17: REST API tab

For more information on the QoE REST API definition, refer to QoE Appliance REST API Guide.

Subscriber identification

For QoE, traffic belongs to the same subscriber if it shares the same IP address on the access side (in IPv4), or if it is from the same /64 subnet on the access side (in IPv6).

If there is a NAT between the QoE server and real subscribers and subscribers whose IP address is translated to the same IP address does not considered as the same subscriber.

A new subscriber is identified when the first packet from an IP address is received. Hereby the subscriber rate rules are evaluated to choose the policies to be applied.

Subscriber flows decision tree

The evaluation of subscriber flow rules are, when a new traffic flow is created (for example, a TCP connection), the profiles in the subscriber flow rule set are checked to determine if the flow matches any of them, and to establish the flow policy to apply.

To view the subscriber flows decision tree, navigate to **Configuration** > **Subscriber Flows** > **Rules Tree View**.

For efficiency, profiles are evaluated in this pre-defined order:

- 1. Interface
- 2. VLAN
- 3. Policy Rate

- 4. Internet
- 5. Access
- 6. Throughput
- 7. DPI

The profile evaluation order defines a decision tree, whose nodes are the different profiles and with policies as leaves. The tree determines the final rule to be selected, because a rule can be excluded if it belongs to a branch that the decision tree does not follow. It may be the case that a flow matches more than one rule. In that case, the rule matching the Interface profile has a priority over the rule matching the VLAN profile, and so on in the previously specified order.

If two rules have a match with the same type of profile, then the more restrictive profile have the priority. For an example, a flow from a subscriber with IP address 192.168.0.1 matches a rule with an access profile with the 192.168.0.0/24 range and match another rule with an access profile with the 192.168.0.0/16 range, the one with the more restrictive range, is selected.

To facilitate the understanding of this order, the UI includes a graphic representation of the decision tree, where the top-most matching path leads to the selected policy (except when there is more than one match at the same profile level when the most restrictive wins). It is accessible in **Configuration** > **Subscriber Flows** > **Rules** and click the **Rules Tree-View** tab.



Figure 18: Subscriber flows decision tree

If there are common elements in two profiles of the same type and therefore a rule conflict, the decision tree flags it so the rules can be reviewed by the operator and the conflict corrected.

Subscriber rate decision tree

The evaluation of the subscriber rate rules happen if a new subscriber is detected. The profiles are checked to determine which ones are matched by the subscriber and to select the subscriber rate policy to apply. For efficiency, the profiles are evaluated in the following pre-determined order:

- 1. Interface
- 2. VLAN
- 3. Access

In subscriber rate rules, Internet profiles and DPI profiles cannot be used, because such profiles make no sense in policies that apply to all traffic of the same subscriber, regardless of the application.

The decision tree is like the one for subscriber flow rules. From the dashboard page, navigate to **Configuration > Subscriber Rate** and select **RULES TREE-VIEW** tab.

Ű	Cambium Networl	ks^m ology		👤 admin@cninsight 🗸
	Dashboard			
			SUBSCRIBER RATE CONFIGURATION	() C :
0	Status	+		
11.	Statistics	+	RULES TREE-VIEW POLICIES	
\$	Configuration	-	ACCESS	POLICY RULE ACTIONS
	Interfaces	+		
	Profiles	+	Client-10.10.1.1	15D_5Up
	Subscriber Flows		0	
	Subscriber Rates			
	Subscriber Monitoring		root Client-10.10.2.0	100Mbps-Rate-Limit
	Radius		o — — — — — — — — — — — — — — — — — — —	
	REST API			
	DoS		any-other	rate-default
	TCPO Settings		0	12 / 1
٩	Administration	+		
0	About			

Figure 19: Subscriber rate decision tree

Checking the policy and subscribers

This section explains how to check the policy of a subscriber and a subscriber for a policy. From the UI, you can check the policies applied to a subscriber in **Status** > **Subscribers**, based on the IP address. It provides useful information such as:

- Applied subscriber rate policy (Policy rate).
- Applied subscriber monitor policy (*Policy monitor*).
- Last measurement of downlink retransmissions in TCP traffic (*Latest downlink TCP RTX rate*) and its average value (*Average downlink TCP RTX rate*).
- Last measurement in milliseconds of the minimum access RTT (*Latest RTT-min*) and historical minimum (*Absolute RTT-min*).

Cambium Netwo	orks ^{te}						💄 admin@QoE 🗸
Dashboard							
• Status	-	ACTIVE SUBSCRIBERS STATUS					0 0
System	+	Total Active subscribers 32					
Interfaces	+	I≣ 10000	 All policies 		✓	80::/48	
Flows	+						
RADIUS/REST	+	Show 50 🗸 entries				Searc	h:
Subscribers		ADDR 🔶	FL-ACTIVE \$	FL-POLICY \$	BYTES-UPLINK \$	BYTES-DOWNUNK \$	LIFETIME \$
Policies		10.10.2.129 📈	66	41276	2794103715	156012081765	35:16:48
1. Statistics	+	10.10.2.116 ~	68	40890	2775138115	154826178390	35:17:15
Configuration	+	10.10.2.126 📈	74	40815	2773566385	154688315071	35:16:51
Administration	+	10.10.2.128 📈	68	40836	2766392665	154341477403	35:16:49
About		10.10.2.120 📈	69	40657	2760360741	153940036398	35:17:13
		10.10.2.122 📈	72	40541	2756257014	153681975201	35:16:55
		10.10.2.118 📈	68	40438	2755988793	153651047144	35:17:07
		10.10.2.125 ~	61	40589	2751260512	153491333755	35:16:52
		10.10.2.111 📈	59	40186	2739516555	152735726423	35:17:16
		10.10.2.104 📈	66	40194	2731798545	152357901935	35:17:03
		10.10.2.121 📈	63	40161	2728103656	152098920530	35:16:56
		10.10.2.130 📈	64	40035	2718670325	151493063904	35:16:47
		10.10.2.110 📈	63	39829	2710581849	151075430979	35:16:57
		10.10.2.103 📈	62	39811	2705953663	150923166452	35:17:04

Figure 20: Subscriber status

For a given a policy, to view the number of subscriber IP addresses are under each policy, navigate to **Status** > **Policies**.

Cambium Network	KS[™] ≫ogy						💄 admin@QoE 🗸
Dashboard							
• Status	-	ACTIVE SUBSCRIBERS IN POLICIE	S				0 C
System	++++++	Flow Policies					Saarch
Flows	+	NAME	▲ FLOWS \$	DOWNLINK-RCV 🖨	DOWNLINK-SND \$	UPLINK-RCV \$	UPLINK-SND \$
RADIUS/REST	+	flow-8Mbps	0	0	0	0	0
Subscribers	_	flow-default	1	0	0	11,090,335	11,090,335
Policies	-	flow-no-rate-limit	0	0	0	0	0
1. Statistics	+	flow-no-tcpo	1,917	4,562,905,049,441	4,562,905,049,441	82,176,628,786	82,176,628,786
Configuration	+	flow-policy-example	0	0	0	0	0
Administration	+	Showing 1 to 5 of 5 entries					Previous 1 Next
About		Rate Policies Show 50 v entries					Search
		NAME	SUBSCRIBERS 🛊	DOWNLINK-RCV \$	DOWNLINK-SND \$	UPLINK-RCV \$	UPLINK-SND \$
		10down_Sup	0	0	0	0	0
		rate-100Mbps	0	0	0	0	0
		rate-10Mbps	0	0	0	0	0
		rate-50Mbps	0	0	0	0	0
		rate-default	33	4,562,905,049,441	4,562,905,049,441	82,187,719,121	82,187,719,121
		Showing 1 to 5 of 5 entries					Previous 1 Next

Click policy name to list the subscribers using that policy (more volume consumption is listed).

Cambium Networ	ks™ ology				💄 admin@cnInsight ∨				
Dashboard									
Status	-	FLOWS IN FLOW POLICY: flow-default							
System	+	Subscribers shown: 1000							
Interfaces	+								
Flows	+								
Radius/REST	+	SUBSCRIBER	FL-ACTIVE	BYTES-UPLINK	BYTES-DOWNLINK				
Subscribers		192.168.1.110	1	145	0				
Policies		192.168.1.102	1	145	0				
Statistics	+	169.254.1.1	1	1434603	0				
	192.168.1.108	1	145	0					
Configuration	+								
Administration	+				Return				
About									
	Cambium Networ Dashboard Status System Interfaces Flows Radius/REST Subscribers Policies Statistics Configuration Administration About	Cambium Networks" Dashboard Status - System + System + Rows + Rodus/REST + Subscribers Folicies + Statistics + Configuration + Administration + About	Cambian Networks Dashboard Status - System + Interfaces + Hows + Radua/REST + Subscribers 192.168.1.100 Statistics + Configuration + Administration + About -	Combine Networks Dashboard Status - System + Interfaces + Rows + Rodus/REST + Statistics + Statistics + Statistics + Statistics + Administration + About -	Construction Set is beguint to water Dabboard FLOWS IN FLOW POLICY: flow-default System + System + Rows + Rows + Rodus/REST + Subscribers 1 Subscribers 1				

Policy examples

The following are the common examples of policies:

- Limiting the speed of some applications
- Exclude traffic from TCP optimization
- Implementing subscriber rate plans
- Services not limited by the subscriber rate

Limiting the speed of some applications

The goal is to reduce the network peak throughput to mitigate the congestion at rush hour. To that end, a DPI profile is defined (video in the example) to identify the applications to limit (streaming in this example). This example makes use of *video-streaming* pre-defined signatures. To include them, in **Add DPI profile**, select **Add Predefined Signatures** and choose the **Video-streaming** pre-defined signature.

Also, a throughput profile is created with the traffic load from which to start limiting (**above-5 Gbps** in this example). Then, a subscriber flow policy (*flow-8 Mbps* in the example) is created with a downlink limit (*Downlink shaping*) set at 8 Mbps. Finally, the DPI profile, the throughput profile, and the subscriber flow policy are tied together in a subscriber flow rule.



Figure 21: Limiting the speed of some applications

Exclude traffic from TCP optimization

QoE does not optimize certain traffic. To that end, an access profile is defined (*subs-no-tcpo* in the example), with the subscriber IP addresses to exclude. Next, a subscriber flow policy is defined with an optimization set to off (*flow-no-tcpo* in the example) and, then the access profile and the subscriber flow policy are combined in a subscriber flow rule.

EDIT SUBSCRIBER FLOW POLICY				
Name flow-8Mbps				
Block: disabled				
TCP Optimization: enabled				
TCP Advanced Parameters	*			
Downlink shaping per Subscriber: enabled		Uplink shaping per Subscriber: enabled		-
Max rate per Subscriber	8.000 Mbps 🗘 🐼	Max Rate per Subscriber	4.000 Mbps	≎ ⊠
Burst Options	*	Burst Options		*
Downlink shaping per Flow: disabled		Uplink shaping per Flow: disabled		
Drop Incoming Connections	*			
Skip subscriber rate limitation: disabled				
			Appl	(Cancel





Figure 23: Subscriber flows configuration

Implementing subscriber rate plans

The objective is to apply the speed limits in each subscriber's data plan.

The QoE applies these limits better than a conventional shaping element, because for TCP traffic (the most common), it does not need to discard packets. Furthermore, it uses independent queues per flow and that makes application latencies independent of each other, which improves the experience of interactive applications. Figure 24 shows the queue structure, with a queue per flow and policy control at flow and subscriber levels.



Figure 24: Implementing subscriber rate plans

Subscribers of each data plan must be identifiable by some of the profiles currently supported by the QoE, for example by VLAN or by IP address ranges. In the following example, three subscriber rate policies are defined, corresponding to three rate plans (rate-100 Mbps, rate-10 Mbps, and rate-50 Mbps in the example), and they are linked to their corresponding access profiles with three rules. Each of the access profiles consists of a list of IP address ranges belonging to each rate plan.



Figure 25: Subscriber rate configuration

Services not limited by the subscriber rate

To preserve the QoE of some services by granting throughput to them even the subscriber rate plan is being fully used, VoIP as an example. An Internet profile (*voip*) and a flow policy (with **Skip subscriber rate limitation** turned **ON**) are defined, then the Internet profile and the policy are linked by a subscriber flow rule.



Figure 26: Services not limited by the subscriber rate

Chapter 8: Connecting to the QoE License Server

To enable the different functionalities in QoE, a license is acquired. The first step to acquire a license is, connect QoE to the cloud license server. The management port must have an access to the Internet until the license is acquired. The dashboard on the UI displays the status of the license server connection.



- If the color is not in **Green**, then the connection is not established, and QoE does not register with the license server to acquire the license.
- If there is a firewall, then open TCP port 13152 for the IP addresses **146.59.206.4** (primary) and **46.26.190.166** (backup). For steps to debug the license server connectivity issues, refer to *QoE Appliance User Interface Guide*.

Chapter 9: Traffic and Latencies

Traffic and Latencies displays the temporal evolution of total traffic throughput, adding both directions and all *wires*. To view the traffic and latencies, navigate to **Statistics** > **Throughput** > **Overview**.

Figure 27 shows the throughput over time graph.



Figure 27: Throughput over time graph

The evolution over time per network interface is available in Statistics > Throughput > Interfaces.

Figure 28 shows the network interface throughput over time graph.



Figure 28: Network interface throughput over time graph

It is possible to check the status of processed traffic according to each of the configured policies. For subscriber flows policies, it can be checked in **Statistics** > **Throughput** > **Subscriber Flows Policies** and similarly for **Subscriber Rate Policies** and **Subscriber Monitoring Policies**.

The chart in **Statistics** > **System** > **Latencies** displays the access RTT (RTT-Down) and Internet RTT (RTT-Up). Average minimum values are provided.

Figure 29 shows the latency over time graph.



Figure 29: Latency over time graph

To see the number of flows per policy and per protocol, navigate to **Statistics** > **Flow** > **Per Policy and Statistics** > **Flow** > **Per Protocol** respectively.

Average Internet Latency per Service

Table of average Internet latencies (RTT) is measured from QoE to the servers in each service. The **all-average** category shows the average for all services.

For every category, you can get the distribution of the latencies (percentage of RTT samples in each

latency bin) by clicking on the i icon. You can also view the the distribution changes over the time. To view the percentage of samples in each bin at different times click i icon. To see the latency per service, navigate to **Statistics > DPI Service Analysis > Latency per Service**. Figure 30 shows the Average Internet Latency per Service page.

AVERAGE INTER	NET LATENCY PER SERVICE	() C
📅 1 Day 🗸 🗸	1≡ 10 Cats. ✓	
Filters		*
Show 50 🗸 entries	5	Search:
SERVICE	INTERNET-LATENCY-MS	♦ DETAILS
SERVICE all-average	INTERNET-LATENCY-MS 0.707	t details
SERVICE all-average 10.0.0.0/8	INTERNET-LATENCY-MS 0.707 0.707	t Details

Figure 30: Average Internet Latency per Service page

Chapter 10: Analytics

QoE displays the current traffic composition per service. To view the current traffic composition, navigate to **Statistics > DPI Analysis > Total Volume per Service**.

Figure 31 shows the total volume per service chart.



Figure 31: Total Volume per Service chart

The hourly evolution can be obtained in Statistics > DPI Analysis > Hourly Volume per Service.



Figure 32 shows the hourly volume per service chart.

Figure 32: Hourly Volume per Service chart

When you navigate to **Statistics > Subscribers > Top by Time and Statistics > Subscribers > Top Total**, the subscriber IP addresses appears. With the biggest traffic consumption over time or the total in the given period, respectively.

Chapter 11: Denial of Service (DoS)

QoE detects DoS attacks. To perform this, configure the DoS thresholds. Navigate to **Configuration > DoS** from home page to configure the DoS thresholds:

- Downlink failed handshake rate SYNs per second without an answer in the direction towards the subscribers (initialized from the Internet). The default value is 0 SYN/sec (feature is disabled). A typical value is 50 failed handshakes per second.
- Uplink failed handshake rate SYNs per second without an answer initialized by a subscriber. The default value is 0 SYN/sec (feature is disabled). A typical value is 50 failed handshakes per second.
- **Minimum rate** Minimum speed rate that can be considered a volumetric attack. The exact value depends on the network speed, but the default value is 50 Mbps.
- Multiplier of subscriber rate policy— If the subscriber has a known rate policy, a threshold is defined as multiplier * downlink limit. A typical multiplier is 3. For an example, a subscriber with a 20 Mbps plan has a DoS threshold of 3 * 20 = 60 Mbps. Figure 33 shows the DoS settings.

Downlink Volume Attacks			
V DOS attacks, failed TCP handshake Downlink Rate and 5s have to be specified. A zero value (click the reset parameter will disable the corresponding functionality. Speed is above that limit times the multiplier. A zero value default icon) in both parameters will disable the functional default icon) in both parameters will disable the functional default icon) in both parameters will disable the functional default icon) in both parameters will disable the functional default icon) in both parameters will disable the functional default icon) in both parameters will disable the functional default icon) in both parameters will disable the functional default icon) in both parameters will disable the functional default icon) in both parameters will disable the functional default icon) in both parameters will disable the functional default icon) in both parameters will disable the disable the disable the disable the dicon default icon) in	criber rec rate limita e (click th ality.	eives stion, e res	; more , the et
undshake rate 0 SYN/sec 🗘 <table-cell> Minimum rate 0.00</table-cell>	Mbps	\$	×
Ishake rate 0 SYN/sec 🗘 🐼 Multiplier of subscriber rate policy 0.00	Times	\$	×
	Appl	ly Set	ttings
		Appl	Apply Set

Figure 33: DoS settings

The DoS events are shown in **Statistics** > **DoS Attacks**. In DoS Attacks Over Time, the DoS attack events are displayed by showing its type, its duration, and parameters such as the affected subscriber IP and the main IP contributing the attack.

Figure 34 shows the DoS attacks over time.



Figure 34: DoS attacks over time

In **Details of DoS Attacks** all DoS events are listed, with information about the time, event type, IP address affected, the direction of the attack (Ingress or Egress), and its duration. In **SYN Attacks** can be found attacks of SYN type, with the number of failed SYN and its rate per second. In **Volume Attacks**, there is a list of volumetric attacks with information on the traffic volume and its average rate.

Chapter 12: Updating the Software

To download and update the software, perform the following steps:

- 1. Visit https://support.cambiumnetworks.com/files/qoe_qoe/.
- 2. Download the **.bpkg** file to a local drive.
- 3. Access the UI from the management port using the configured management IP address.

The following are the default credentials:

- IP address: 192.168.0.121
- Username: admin
- Password: cambium
- 4. Navigate to Administration > Software.

Cambium Networks"								
Dashboard							_	
Statue		SOFTWARE STA	TUS				0 C :	
O otatus		_					_	
1. Statistics	+	NAME	VERSION	ACTIVE	BOOT	ACTIONS	_	
Configuration	+	bqnos	R3.0.7		\checkmark			
Administration		linux	R3.0.1-20210119		\checkmark			
Backup	+	bgnkernel	R3.0.5-4.12.14-155.g4755291-default		\checkmark			
System Date	+	kernel	R3.0.2-4.12.14-155.g4755291-default	\checkmark	\checkmark			
Diagnostic		gui	R3.0.1		\checkmark			
License	_	bqn	R4.0.21		\checkmark	÷		
Users		cmbm	R1.0.2		\checkmark	Cy.		
Reboot								
Shutdown							_	
About								

5. Click icon on the top-right, and click Install....

Cambium Network	works [™] It Technology					💄 admin@cnInsight 🗸
Dashboard		-				
Status	+	SOFTWARE STAT	TUS			Install
1. Statistics	+	NAME	VERSION	ACTIVE	воот	ACTIONS
Configuration	+	bqnos	R3.0.7		\checkmark	
		linux	R3.0.1-20210119		\checkmark	
Reelaw		bqnkernel	R3.0.5-4.12.14-155.g4755291-default	\checkmark	\checkmark	
System Date	+	kernel	R3.0.2-4.12.14-155.g4755291-default			
Diagnostic		gui	R3.0.1		\checkmark	
License	_	bqn	R4.0.21			G
Users		bqn	R4.0.22	✓	\checkmark	G
Reboot		cmbm	R1.0.2			÷
Shutdown		cmbm	R1.0.3			€j
About About				-	-	

6. Browse and select the appropriate **.bpkg** file.

((S ¹⁴ logy							🛓 bqnadm@cnQo
	Dashboard		-		C				
•	Status	+	SOF	Transferrir	ng software file				00
۵	Statistics	+	NAM				IVE	воот	ACTIONS
×	Configuration	+	bqno			CANCEL			
7	Administration	-	linux		R3.0.1-20210119	E	2		
	Backup	+	bqnker	mel	R3.0.3-4.12.14-155.g4755291-default	E	2		
	System Date	+	kernel		R3.0.2-4.12.14-155.g4755291-default	E	2		

7. After the software update is complete, the **Software Installed Successfully** message appears.

Cambium Networks					🛓 bqnadm@cnQoE 🗸	
Dashboard		-	(i)			
Status	+	SOF So	ware installed successfully			001
Statistics	+	NAM		Th	л воот	ACTIONS
Configuration	+	bqno		ок		
Administration	-	linux	R3.0.1-20210119	2		
		bqnkernel	R3.0.3-4.12.14-155.g4755291-default			

To activate the new software, reboot the system, or click ${}^{\checkmark}$ icon for the updated software.

Glossary

Term	Definition		
DoS	Denial of Service		
DPI	Deep Packet Inspection		
QoE	Quality of Experience		
ТСРО	TCP Optimization		
WISP	Wireless Internet Service Provider		

Cambium Networks

Cambium Networks delivers wireless communications that work for businesses, communities, and cities worldwide. Millions of our radios are deployed to connect people, places and things with a unified wireless fabric that spans multiple standards and frequencies of fixed wireless and Wi-Fi, all managed centrally via the cloud. Our multi-gigabit wireless fabric offers a compelling value proposition over traditional fiber and alternative wireless solutions. We work with our Cambium certified ConnectedPartners to deliver purpose-built networks for service provider, enterprise, industrial, and government connectivity solutions in urban, suburban, and rural environments, with wireless that just works.

User Guides	http://www.cambiumnetworks.com/guides		
Technical training	https://learning.cambiumnetworks.com/learn		
Support website (enquiries)	https://support.cambiumnetworks.com		
Main website	http://www.cambiumnetworks.com		
Sales enquiries	solutions@cambiumnetworks.com		
Warranty	https://www.cambiumnetworks.com/support/standard-warranty/		
Telephone number list	http://www.cambiumnetworks.com/contact-us/		
Address	Cambium Networks Limited, Unit B2, Linhay Business Park, Eastern Road, Ashburton, Devon, TQ13 7UP United Kingdom		

Cambium Networks and the stylized circular logo are trademarks of Cambium Networks, Ltd. All other trademarks are the property of their respective owners.

© Copyright 2024 Cambium Networks, Ltd. All rights reserved.