



Technical Guide

User Bandwidth Throttling

Released: January 2018

Doc Rev No: R1

Copyright Notification

Edgecore Networks Corporation

© Copyright 2019 Edgecore Networks Corporation.

The information contained herein is subject to change without notice. This document is for informational purposes only and does not set forth any warranty, expressed or implied, concerning any equipment, equipment feature, or service offered by Edgecore Networks Corporation. Edgecore Networks Corporation shall not be liable for technical or editorial errors or omissions contained herein.

Table of Contents

1	Introduction	2
2	Configurations	3
1.1	User Flow	3
1.2	WLAN Controller Configuration.....	3
3	Testing Results.....	6
4	Logs and Reports for Guest and Social Users	7
5	Remarks	7

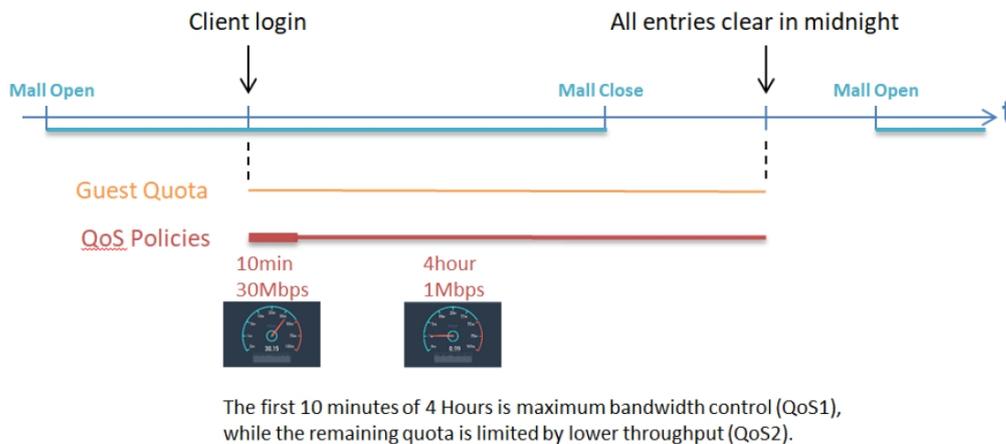
1 Introduction

The article is aimed at explaining the practical setup flow of “User Bandwidth Throttling”, which is a new feature available in version 3.43 for all EWS series. The newly added feature allows network administrators to enforce double QoS policies on users, providing greater flexibility in traffic control especially for guest users. For all authentication options, especially Guest Authentication and Social Media Login for now, time-based bandwidth throttling feature as a part of the policy profile is the win-win solution for providing free Wi-Fi service in public areas.

This technical guide should help network administrators to easily setup and configure bandwidth limitation for all users in the network. We will be using Guest Authentication in this document as an example to illustrate this new feature.

2 Configurations

1.1 User Flow



- Clients can access the login page after connecting to the SSID
- Clients can access the Internet after submitting their email and answers to a questionnaire (if configured) asking for information such as name, phone and postal code. They can enjoy the Internet service for 4 hours, and for the first 10 minutes, their maximum bandwidth is governed by QoS profile 1 (30 Mbps), while for the remainder of the time, it is governed by QoS profile 2 (1 Mbps).
- The Guest account will be automatically cleared at midnight.

1.2 WLAN Controller Configuration

- Go to **System>WAN** to enable “Bandwidth Limitation”

WAN Traffic Settings

Bandwidth Limitation	<input checked="" type="checkbox"/> Enable Bandwidth Limitation on WAN
Max Uplink Bandwidth	<input type="text" value="2000000"/> Kbps
Max Downlink Bandwidth	<input type="text" value="2000000"/> Kbps

- Go to **Users>Policies>Policies** to select a desired policy profile and do the necessary configurations for the QoS Profile

Select Policy Policy 1

Policy Configuration

Policy Name: Policy 1
 Firewall Profile: Firewall 1
 Privilege Profile: Privilege 1
 QoS Profile: QoS 1 Enable Bandwidth Throttling in 5 min(s) and change the profile to QoS 2
 Specific Route Profile: Specific Route 1
 Prefer DHCP Pool: None

QoS Configuration

QoS Profile Name: QoS 1

Traffic Class: IPv4 IPv6

Bandwidth Control: Enable Disable

Group Total Downlink: 0 Mbps

Group Total Uplink: 0 Mbps

Individual Maximum Downlink: 0 Mbps

Individual Maximum Uplink: 0 Mbps

Individual Request Downlink: 0 Mbps

Individual Request Uplink: 0 Mbps

*(Unlimit: 0, Range: 1-999)

QoS Profile Name: QoS 2

Traffic Class: IPv4 IPv6

Bandwidth Control: Enable Disable

Group Total Downlink: 90 Mbps

Group Total Uplink: 90 Mbps

Individual Maximum Downlink: 20 Mbps

Individual Maximum Uplink: 20 Mbps

Individual Request Downlink: 5 Mbps

Individual Request Uplink: 5 Mbps

*(Unlimit: 0, Range: 1-999)

A new field in “User Policy Configuration”

- QoS Profile: Administrators are able to enable/disable the bandwidth throttling feature by checking/unchecking the checkbox. If enabled, the user applied with this policy will use QoS 1 for the first 5 minutes, and be limited by QoS 2 since the 5th minute until session is expired. If the guest user logs in following email verification, the bandwidth limitation will be refreshed in the moment of the email verification.
 - This feature is also applicable when using Local, On-demand, RADIUS database and other external authentication databases supported by the EWS.
- c. Go to **Users > Groups > Configuration** to apply the configured policy to the corresponding Group (Using Policy 1 for this example)

Group Configuration

Select Group:

Group Name:

Remark:

Number of devices which are allowed to login:
(0 to 9999 devices, 0: Unlimited)
 For On-Demand accounts, number of devices is configured individually per different billing plans. The number is for the following types: LOCAL, POP3, RADIUS, LDAP, and NT Domain.

Allow to logout other devices when exceeding the maximum amount of devices: Enabled Disabled
For On -Demand accounts, allowing to logout others devices is always enabled. This setting id for the following types: LOCAL, POP3, RADIUS, LADP, and NT Domain.

Zone Permission Configuration & Policy Assignment

Enabled	Zone Name	Time Span 1	Time Span 2	Time Span 3
		<input type="text" value="Schedule 1"/>	<input type="text" value="Schedule 1"/>	<input type="text" value="Schedule 1"/>
<input checked="" type="checkbox"/>	Service Zone : Default	<input type="text" value="Policy 1"/>	<input type="text" value="Policy 1"/>	<input type="text" value="Policy 1"/>
<input checked="" type="checkbox"/>	Service Zone : SZ1	<input type="text" value="Policy 1"/>	<input type="text" value="Policy 1"/>	<input type="text" value="Policy 1"/>
<input checked="" type="checkbox"/>	Service Zone : SZ2	<input type="text" value="Policy 1"/>	<input type="text" value="Policy 1"/>	<input type="text" value="Policy 1"/>
<input checked="" type="checkbox"/>	Service Zone : SZ3	<input type="text" value="Policy 1"/>	<input type="text" value="Policy 1"/>	<input type="text" value="Policy 1"/>
<input checked="" type="checkbox"/>	Service Zone : SZ4	<input type="text" value="Policy 1"/>	<input type="text" value="Policy 1"/>	<input type="text" value="Policy 1"/>
<input checked="" type="checkbox"/>	Service Zone : SZ5	<input type="text" value="Policy 1"/>	<input type="text" value="Policy 1"/>	<input type="text" value="Policy 1"/>
<input checked="" type="checkbox"/>	Service Zone : SZ6	<input type="text" value="Policy 1"/>	<input type="text" value="Policy 1"/>	<input type="text" value="Policy 1"/>
<input checked="" type="checkbox"/>	Service Zone : SZ7	<input type="text" value="Policy 1"/>	<input type="text" value="Policy 1"/>	<input type="text" value="Policy 1"/>
<input checked="" type="checkbox"/>	Service Zone : SZ8	<input type="text" value="Policy 1"/>	<input type="text" value="Policy 1"/>	<input type="text" value="Policy 1"/>

- d. Go to *Users > Internal Authentication > Guest* to do the necessary configuration. In this page, chose the configured Group that uses policy 1 so that users login through this database will be applied with the configured QoS profile.

Guest Authentication

Group:

Guest Information:

Guest Questionnaire:

Guest Access Time: Unlimited 1 Day Access Multi-Day Access

Quota: day(s)

Email Verification: Disable Enable

Email Activation Time: hour(s) minute(s)
SMTP server is ready

Sender Name: *(name@domain)

Activation Email Subject:

Activation Email Content:

Activation Link:

E-mail Denial List: Disable Enable

Note that if enabled "Email verification" it is necessary to configure the SMTP server. To

configure SMTP Server simply click on the Assign SMTP Server button to do the necessary configuration

- e. Go to *System > Service Zones* and the desired zone to enable Guest for the authentication option.

Authentication Options	Auth. Option	Auth. Database	Postfix	Default	Enabled
	Server 1	LOCAL	local	<input checked="" type="radio"/>	<input checked="" type="checkbox"/>
	Server 2	RADIUS	radius	<input type="radio"/>	<input checked="" type="checkbox"/>
	Server 3	NTDOMAIN	ntdomain	<input type="radio"/>	<input checked="" type="checkbox"/>
	Server 4	LDAP	ldap	<input type="radio"/>	<input checked="" type="checkbox"/>
	Server 5	POP3	pop3	<input type="radio"/>	<input checked="" type="checkbox"/>
	On-Demand	ONDEMAND	ondemand	<input type="radio"/>	<input checked="" type="checkbox"/>
	SIP	SIP	N/A	<input type="radio"/>	<input type="checkbox"/>
	Guest	FREE	N/A	<input type="radio"/>	<input checked="" type="checkbox"/>
	Social Media Login	SOCIAL	N/A	<input type="radio"/>	<input type="checkbox"/>
	One Time Password	OTP	N/A	<input type="radio"/>	<input type="checkbox"/>

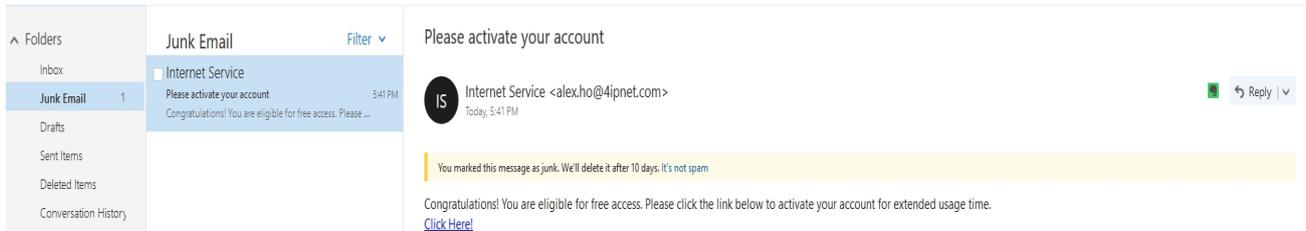
3 Testing Results

- a. Client device associates to SSID and get the following login page

The screenshot shows a web-based login interface. At the top, there is a decorative header with wavy lines in shades of blue, purple, and red. Below this, the page is divided into two main sections. The first section is titled 'LOGIN' and contains two input fields: 'Username' and 'Password'. A red 'Login' button is positioned to the right of the password field. The second section is titled 'FREE LOGIN' and contains an 'Email' input field. Below the email field, there is a text prompt: 'Enter your Email account to login for free.' and a red 'Login' button.

- b. Fill in a valid email for the system to send Email verification. Go to the mailbox to open the verification Email and click on the hyperlink to be granted Internet access. Check the Spam folder if the verification Email is not found in the Inbox.

Note that before Email verification, the user will only have limited internet access depending on the activation time settings in Guest configuration page.



- c. Once verified, the user will be have full bandwidth for the first 5 minutes (QoS 1). Starting from the 5th minutes, the user will only have a maximum bandwidth of 20 Mbps (QoS 2).

4 Logs and Reports for Guest and Social Users

There are related Logs and Reports for checking authenticated user status and information for troubleshooting or other marketing purposes.

Online Users List: Like in previous versions, it shows current logged in user information

User Event: Like in previous versions, it shows all event of every client during the login process and adds the new event when bandwidth throttling is enabled. Besides, Max Download/Max Upload fields will show the bandwidth limitation.

Type	Date	Name	IP	MAC	Event	Max Download	Max Upload
FREE	2018-01-22 16:56:32 +0800	alexho@4ipnet.com	172.21.0.11	D4:A3:3D:AE:ED:7B	Login	Unlimited	Unlimited
FREE	2018-01-22 17:02:08 +0800	alexho@4ipnet.com	172.21.0.11	D4:A3:3D:AE:ED:7B	Email-Verified		
FREE	2018-01-22 17:07:09 +0800	alexho@4ipnet.com	172.21.0.11	D4:A3:3D:AE:ED:7B	Bandwidth_Throttling	20mbit	20mbit
FREE	2018-01-22 17:10:10 +0800	alexho@4ipnet.com	172.21.0.11	D4:A3:3D:AE:ED:7B	Logout		

System Log: Like in previous versions.

5 Remarks

Please contact Technical Support Team for additional inquiries.