

Grandstream Networks, Inc.

GWN700x Series

User Manual



WELCOME

GWN7001/7002/7003 are Multi-WAN Gigabit VPN routers with built-in firewalls that allow businesses to build comprehensive wired, wireless and VPN networks for one or many locations. They offer high-performance routing and switching power along with built-in VPN support for secure in-office and inter-office connectivity. To provide enterprise-grade security protection and ensure stable network operation, the GWN 7001/7002/7003 features a built-in firewall with advanced content security, filtering, threat detection, attack prevention and more. To maximize network reliability, they support traffic load balancing, failover (WAN backup) and bandwidth management capabilities. The GWN7001 includes 6 Gigabit Ethernet ports. The GWN7002/GWN7003 include 2 2.5 Gigabit SFP ports, 4/9 Gigabit Ethernet ports, and 2 PoE output ports that allow them to provide power to other endpoints. These routers can manage themselves and up to 150 Grandstream GWN Series Wi-Fi APs thanks to an embedded controller located in the products' web user interface. These routers can also be managed with GDMS Networking and GWN Manager, Grandstream's free cloud and on-premise network management tools. By providing high-performance routing, VPN support, powerful security protection and easy-to-use network management tools, the GWN Gigabit VPN routers are ideal for a wide variety of deployments including small-to- medium businesses, retail, education, hospitality, healthcare and more.

Changes or modifications to these products not expressly approved by Grandstream, or operation of these products in any way other than as detailed by this User Manual, could void your manufacturer warranty.

Please do not use a different power adapter with the GWN700X routers as it may cause damage to the products and void the manufacturer warranty.

PRODUCT OVERVIEW

Technical Specifications

	GWN7001	GWN7002	GWN7003		
СРИ	Dual ARM Cortex A53 1GHz				
Memory and NAT Sessions	256MB RAM, 256MB Flash, 30K NAT sessions	256MB RAM, 256MB Flash, 30K NAT sessions	512MB RAM, 256MB Flash, 60K NAT sessions		
Network Interfaces	6x Gigabit Ethernet ports * <i>All ports are WAN/LAN</i> configurable.	2x 2.5 Gigabit SFP ports and 4x Gigabit Ethernet ports * <i>All ports are WAN/LAN</i> <i>configurable</i>	2x 2.5 Gigabit SFP ports and 9 x Gigabit Ethernet ports * <i>All ports are WAN/LAN configurable</i>		
Number of VLANs Supported	Create up to 16 VLANs		Create up to 32 VLANs		
NAT Routing & IPSec VPN Performance	2.2Gbps				
IPsec VPN Throughput	530Mbps				
Auxiliary Ports	1x USB 2.0 port, 1 x Reset Pinhole				
Mounting	 Desktop Wall mounting 19" standard rack (only for GWN7003) 				
LEDs	8 x single-color LEDs for device	e tracking and status indication	13 x single-color LEDs for device tracking and status indication		

Connection Type	DHCP, Static IP, PPPoE, PPTP, L2TP					
Network Protocols	IPv4, IPv6, IEEE 802.1Q, IEEE 802.1p, IEEE 802.1x, IEEE 802.3, IEEE 802.3, IEEE 802.3u, IEEE802.3x, IEEE 802.3ab					
QoS	 VLAN, TOS Support multiple traffic classes, filter by port, IP address, DSCP, and policing App QoS VoIP Prioritizing 					
Firewall	DDNS, Port Forwarding, DMZ,	UPnP, Anti-DoS, traffic rules, NA	AT, ALG, TURN Service			
VPN	 SSL VPN Server / Client-to Site IPsec VPN Client-to-Site / Site-to-Site PPTP VPN Server / Client-to-Site L2TP Client-to-Site WireGuard IPSec Encryption: DES, 3DE, AES IPSec Authentication: MD5, SHA-1, SHA2-256 IPSec Key Exchange: Main/Aggressive Mode, Pres-shared Key, DH Groups 1/2/5/14 IPSec Protocols: ESP IPsec NAT Traversal SSL VPN Encryption: AES, DES SSL Authentication: MD5, SHA-1, SHA2-256, SHA2-384, SHA2-512 SSL VPN Certificate: RSA PPTP Encrpytion: MPPE 40-bit, 128-bit, IPSec PPTP/L2TP Authentication: MS-CHAPv1/2 					
Max Concurrent VPN Tunnels	Up to 50 Tunnels	Up to 50 Tunnels	Up to 100 Tunnels			
Network Management	GWN7001 embedded controller can manage itself and up to 100 GWN APs.	GWN7002 embedded controller can manage itself and up to 100 GWN APs.	GWN7003 embedded controller can manage itself and up to 150 GWN APs.			
	GWN.Cloud offers a free cloud	management platform for unlimit	ed GWN Routers and GWN APs			
PoE Input	N/A	Standard: IEEE 802.3af/at				
PoE Output	N/A	2 x PoE out ports Passive 48V or IEEE802.3af				
PoE Power Budget	N/A	24V DC 1A: 12.8W 24V DC 1.5A: 24.8W				
Power & Green Energy Efficieny	Universal power adaptor included Input: 100-240VAC 50-60Hz Output: 12V DC 1A (12W)	Universal power adaptor included Input: 100-240VAC 50-60Hz Output: 24V DC 1A (24W)				
Environmental	Operation: 0°Cto 40°C Storage: -30°C to 60°C Humidity: 10% to 90% Non-con	ndensing				
Physical	Unit Dimension: 210mm(L)x130mm(W)x35m m(H); Unit Weight: 453g Entire Package Dimension: 246mm(L)x235mm(W)x45m m(H); Entire Package Weight: 672g	Unit Dimension: 210mm(L)x130mm(W)x35m m(H); Unit Weight: 505g Entire Package Dimension: 246mm(L)x235mm(W)x54m m(H); Entire Package Weight: 730g	Unit Dimension: 260mm(L)x149mm(W)x35mm(H); Unit Weight: 1096g Entire Package Dimension: 297mm(L)x255.5mm(W)x54mm(H); Entire Package Weight: 1443g			

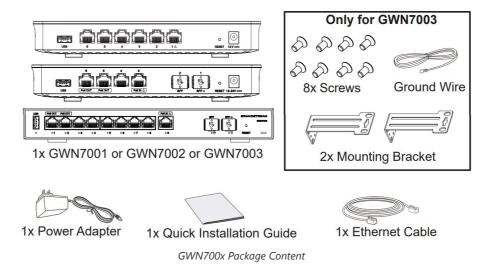
Package Content	GWN7001 router, universal power supply unit, network cable, quick installation guide	GWN7002 router, universal power supply unit, network cable, quick installation guide	GWN7003 router, universal power supply unit, network cable, quick installation guide, 8 x screws, 1 ground wire, 2 x mounting brackets.
Compliance	FCC, CE, RCM, UC, UKCA		

GWN700x Technical Specifications

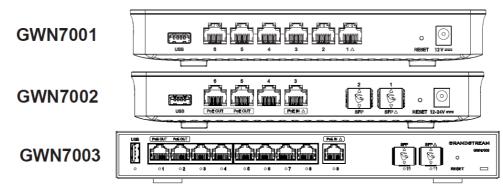
INSTALLATION

Before deploying and configuring the GWN700x router, the device needs to be properly powered up and connected to the network. This section describes detailed information on the installation, connection, and warranty policy of the GWN700x router.

Package Contents



GWN700x Ports



GWN700x ports

No.	Port	Description
1		 GWN7001: 6x Gigabit Ethernet ports GWN7002: 4x Gigabit Ethernet ports GWN7003: 9 x Gigabit Ethernet ports Note: All ports support WAN/LAN configurable. The Gigabit Ethernet ports include 2 x PoE OUT ports and 1 x PoE IN port (GWN7002/7003 only).
2	SFP \triangle	2x 2.5 Gigabit SFP ports (GWN7002/7003 only).

3		USB 2.0 port
4		 GWN7001: Power adapter connector (DC 12V, 1A) GWN7002: Power adapter connector (DC 24V, 1A) GWN7003: Power adapter connector (DC 24V, 1A)
5		Grounding terminal (GWN7003 only).
6	RESET	Factory Reset pinhole. Press for 5 seconds to reset factory default settings

GWN700x ports

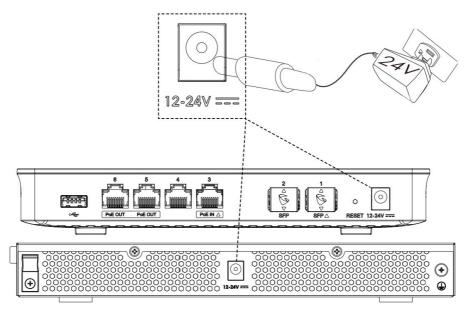
Note:

Ports with this symbol \bigtriangleup are configured to be used as a WAN port by default at the factory.

Powering and Connecting GWN700x

1. Power the GWN700x

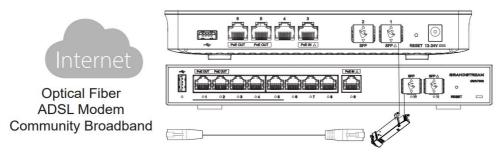
GWN7002/GWN7003 can be powered on using the right PSU (DC 24V, 1A) or PoE (IEEE 802.3af/at).



Powering the GWN700x routers

2. Connect to the Internet

Connect the LAN/WAN or SFP/WAN port to an optical fiber broadband modem, ADSL broadband modem, or community broadband interface.



Connect GWN700x to the Internet

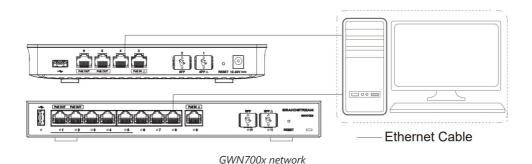
Note:

The \triangle sign indicates the default WAN ports:

- GWN7001: Ethernet port 1
- GWN7002: Ethernet port 3 and SFP 1
- GWN7003: Ethernet port 9 and SFP 11

3. Connect to GWN7002/7003 Network

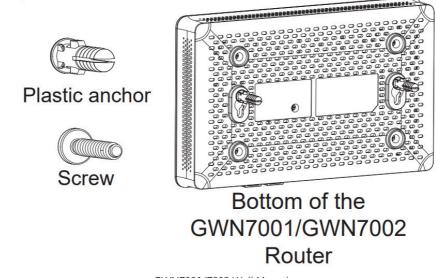
Connect your computer to one of the LAN ports.



GWN700x installation

• Mounting GWN7001/7002 to the Wall

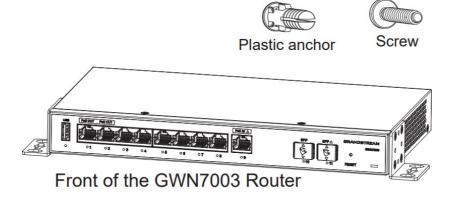
- 1. Using a drill, make two holes in the wall with 135.0mm spacing, 6.0mm diameter. Put a plastic anchor and screw (not provided) on each hole.
- 2. Mount the GWN7001/7002 router on the mounting screws.



GWN7001/7002 Wall Mounting

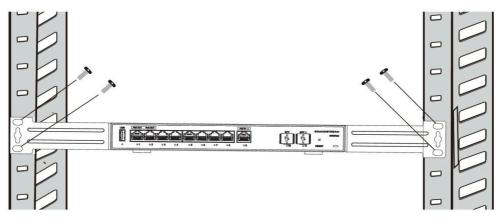
• Mounting GWN7003 to the Wall

- 1. Use the provided screws to fix the two L-shaped Mounting bracket (rotated 90°) on both sides of the GWN7003 router.
- 2. Stick the router port up and horizontally on the selected wall, mark the position of the screw hole on the L-shaped mounting brackets with a marker. Then, drill a hole at the marked position with an impact drill, and drill the plastic anchors (prepared by yourself) into the drilled hole in the wall.
- 3. Use a screwdriver to tighten the screws (prepared by yourself) that have passed through the L-shaped mounting brackets to ensure that the GWN7003 router is firmly installed on the wall.



GWN7003 Wall Mount

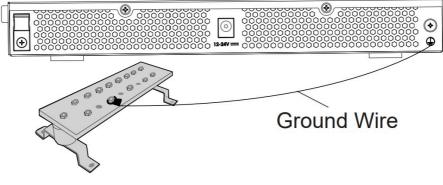
- Install on a 19" Standard Rack
- 1. Check the grounding and stability of the rack.
- 2. Install the two L-shaped rack-mounting in the accessories on both sides of the router, and fix them with the screws provided.
- 3. Place the router in a proper position in the rack and support it by the bracket.
- 4. Fix the L-shaped rack mounting to the guide grooves at both ends of the rack with screws(prepared by yourself) to ensure that the router is stably and horizontally installed on the rack.



19" standard rack installation

• Grounding GWN7003

- 1. Remove the ground screw from the back of the router, and connect one end of the ground cable to the wiring terminal of the router.
- 2. Put the ground screw back into the screw hole, and tighten it with a screwdriver.
- 3. Connect the other end of the ground cable to other device that has been grounded or directly to the terminal of the ground bar in the equipment room.



Grounding GWN7003

GWN7002/GWN7003's default password information is printed on the MAC tag at the bottom of the unit.

Safety Compliances

The GWN700x Router complies with FCC/CE and various safety standards. The GWN700x power adapter is compliant with the UL standard. Use the universal power adapter provided with the GWN700x package only. The manufacturer's warranty does not cover damages to the device caused by unsupported power adapters.

Warranty

If the GWN700x Router was purchased from a reseller, please contact the company where the device was purchased for a replacement, repair or refund. If the device was purchased directly from Grandstream, contact our Technical Support Team for an RMA (Return Materials Authorization) number before the product is returned. Grandstream reserves the right to remedy the warranty policy without prior notification.

GETTING STARTED

The GWN700x Multi-WAN Gigabit VPN Routers provide an intuitive web GUI configuration interface for easy management to give users access to all the configurations and options for the GWN700x's setup.

Use the WEB GUI

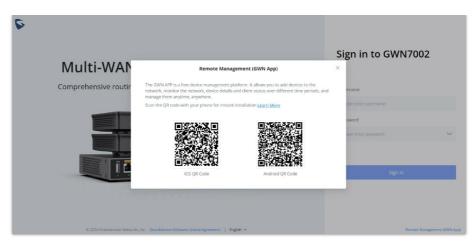
Access WEB GUI

The GWN700x embedded Web server responds to HTTPS GET/POST requests. Embedded HTML pages allow users to configure the device through a Web browser such as Microsoft IE, Mozilla Firefox, or Google Chrome.



GWN700x Web GUI Login Page

To download the App, click on Remote Management (GWN App).



Remote Management (GWN App)

To access the Web GUI:

- 1. Connect a computer to a LAN port of the GWN700x.
- 2. Ensure the device is properly powered up, and the Power and LAN port LEDs light up in green.
- 3. Open a Web browser on the computer and enter the web GUI URL in the following format: https://192.168.80.1 (Default IP address).
- 4. Enter the administrator's login and password to access the Web Configuration Menu. The default administrator's username is "admin" and the default password is printed on the MAC tag of the unit.

At first boot or after factory reset, users will be asked to change the default administrator and user passwords before accessing the GWN700x web interface. The password field is case-sensitive with a maximum length of 32 characters. Using strong passwords including letters, digits, and special characters are recommended for security purposes.

Once the user enters the password, this is the initial page that will be shown. This page contains general information and status about the router.

	Overview									
ort Info pitem Info	Network Connection WAN1(Port 3) ×			Network Traffic All W 78.13 Klass 70.21 Klass	Ni ports				Tetal († 5.5040) († 11.63	-
ienwork Settings v Ienes PN v outing v		1 22.17 forst \$ 17.04 forst		645 Steps 5469 Reps 5569 Reps 1360 Reps 1360 Reps 2144 Reps 7317 Reps Digs					-	
raffic Management 🗸	Access Devices >	Switches >	Cients) Alerts						
	0 Tecal	2 Tecal	1 Total	Details			Th.		Level Time	
nernal Access 🤍 rewalt 🗸 🗸 apove Portal 🗸	c Online Office 0 0	Online Office 0 2	2.45 55 65 Wred 0 0 0 1				No Alert			
	TH 12H 10 1W									
	Wired Client Speed		Total 1/01/03048 0/624/0348	> APP Traffic Statistics						
	240 kps				No.	Name	Total	Uplead	Downland	
	140 kps				• 1	AmazonAWS	1.14MB	↑ 722.06KB	438.7268	
	120 tes		1 mar		2	MTP	261.7KB	135.45KB	126.25KB	
	80 kps				• 3	DNS	125.15KB	† 54.87KB	♣ 70.28×8	
	40 ters 0 ters 10/24 12:00 10:24 14:00 10:24 16:00 10:24 16:00	n walnut halon holme works	- W71400 W71000 W71000 W71000		• 4	ICMP	2.63KB	1.31KB	4 1.3162	
	Tep Clients		Sort by download	> Top SSIDs					Sort by total	

WEB GUI Configuration

Search

To make it easier for the user to find a particular option quickly, the GWN700X web UI has a search feature which can be accessed by clicking on the magnifier icon on the top right corner of the screen and typing the option name.

		🗛 💽 admin 🗸
	Press enter to search VPN	
	The search results related to "VPN"	↑ OB ↓ OB >
	☑ VPN VPN > OpenVPN®	-
÷	VPN > OpenVPN® > OpenVPN® Clients VPN > OpenVPN® > OpenVPN® Servers	

Search

Setup Wizard and Feedback

Setup Wizard

If the user missed the Setup Wizard at the first boot of GWN700X. It's accessible all the time at the top of the page and it contains the necessary settings that the user must configure in 2 steps, first country and time zone, and Internet Settings.

	😋 Q 👤 admin ^
	🗛 Language >
	ပံ Reboot
	🖉 Setup Wizard
Network Traffic All WAN ports 🗸	🖑 User Guide
18.75 Kbps	🖆 Feedback
15.63 Kbps	🗋 Remote Management (GWN App)
12.5 Kbps	Logout
9.38 Kbps	• • • • • • • • • • • • • • • • • • • •

Setup Wizard

Click on \bigcirc button to go through the setup wizard.

	Setup Wizard country / Time Zone Settings Internet Setting	185
	Country / Region United States Time Zone (UTC+01:00) West Centr	al Africa v
< Exit	٥	
	2023 Grandstream Networks, Inc. Grandstream Software License	Agreement

Setup Wizard

If the user has a question or a suggestion to make the GWN700x product even better or has an issue, he can always send feedback, in case of a problem it's better as well to include Syslog as it may help solve the problem faster.

	😋 Q 🚺 admin ^
	🛆 Language >
	じ Reboot
	🧭 Setup Wizard
Network All WAN p	🔟 User Guide
35.16 Kbps	E Feedback
31.25 Kbps	
27.34 Kbps	🗋 Remote Management (GWN App)
23.44 Kbps	Logout
19.53 Kbps	
15.63 Kbps	
11.72 Kbps	•
7.81 Kbps	•
3.91 Kbps	
0 bps	

Feedback – part 1

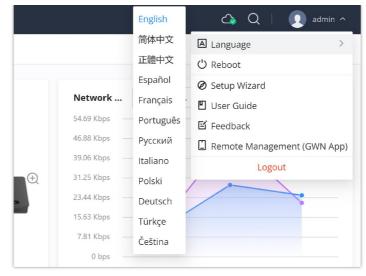
After that, click on the corresponding feedback type to get redirected to the help-desk.

	Feedback	×
?	I have an issue/bug to report and need a solution.	
\$	I need help on my configurations	
É	l have feedback	
	Others	

Feedback – part 2

Web UI Languages

To change the Web UI interface language, on the right corner of the page, click on the username and then click on Language then select the preferred language as shown below:



change language

OVERVIEW

Overview Page

Overview is the first page shown after successful login to the GWN700x's Web Interface. It provides an overall view of the GWN700x's information presented in a Dashboard style for easy monitoring. Please refer to the figure and table below:

verview									
Network Connection	ч 1 22.86 горт — ¥ 18.92 горт (WANT)	Q	Network Traffic All WAY 35.16 Rbps 17.25 Rbps 27.44 Rbps 19.50 Rbps 19.50 Rbps 19.72 Rbps 30.70 Rbps 30.70 Rbps 0 Rbps			2	Tetal	*661MB \$12.52MB	4
Access Devices >	Switches >	Clients	Alerts					Time	
Ordian Online Offline O O	2 Total Online Offline 0 2	1 Total 2.4G 5G 6G Wired 0 0 0 1	U.C.I.S			No Alert	Level	1.8510	
12H ID 1W		Total 1928.6KB 4631.31KB >	APP Traffic Statistics						
D bps				No.	Name	Total	Upload	Download	
10 bps		-		. 1	AmazonAWS	1.14MB	1732.06KB	↓ 438.72KB	
80 bps				2	NTP	261.7KB	135.45KB	↓ 126.25KB	
00 hps		1		3	DNS	125.15KB	\$ 54.87KB	↓ 70.28KB	

Overview Page

Network Connection	Displays the current state of the network connection for the selected WAN port and shows the current upload and download speed. Note: the user can select the WAN port from the drop-down list.
Network Traffic	Shows network traffic in real time. Note: the user can select the WAN port from the drop-down list or select All WAN ports.
Access Devices	shows the total number of Access Devices online and offline.
Switches	Displays the number of switches managed by the router, both the offline and online ones.
Clients	Shows the total number of clients connected either wirelessly (2.4G, 5G and 6G) and also wired connections.
Alerts	Shows Alerts General, Important or Emergency with details and time.
Clients Speed	Displays Clients speed based on time (1H, 12H, 1D or 1W)

APP Traffic Statistics	Displays traffic statistics based on apps usage (%).
Top Clients	Shows the Top Clients list, users may assort the list of clients by their upload or download. Users may click on to go to Clients page for more options.
Top SSIDs	Shows the Top SSIDs list, users may assort the list by number of clients connected to each SSID or data usage combining upload and download. Users may click on to go to SSID page for more options.
Top Access Devices	Shows the Top Access Devices list, assort the list by the number of clients connected to each access device or data usage combining upload and download. Click on the arrow to go to the access point page for basic and advanced configuration options.
	Overview page

Overview page

Port Info

Port Info page displays an overview of all ports status including the USB Port, Gigabits ports, and SFP ports, indicating the links up with green color and links down with grey color, furthermore the user can click on the port icon to get more info about the select link, refer to the figure below:

Navigate to Web UI \rightarrow Overview \rightarrow Port Info:

Port Info				
	2.5Gbps 1000Mbps	100Mbps/10Mbps	Link down Disabled	Connected to the Internet
WAN2 🗹				
Basic Info				
Port enable	d Enai	bled		
Status	Ena	bled		
MAC Addre	ss CO:7	4:AD:BF:AF:52		
Port Type	GE			
Speed/Dup	lex 100	0M Full Duplex		
Flow Contro	ol Status Auto	Negotiation		
Bridge Mod	e Disa	bled		
Network Tr	affic 🕇 F	kts / Bytes: 540926 / 516.7	3MB 🛛 🕹 Pkts / Bytes: 7064	42 / 900.56MB
Current Rai	te 🛉 6	8.71Kbps 🕹 8.21Mbps		
IPv4				
Connection	Type Obt	ain IP automatically (DHCP)		

Port Info

System Info

System Info page shows many info related to GWN700x router like device name, system version, MAC address, system up time, CPU and memory usage, temperature, etc.

The router's System Info can be accessed from the Web GUI \rightarrow Overview \rightarrow System Info Tab.

Temperature	83°C
Load Average	1min: 2.16 5min: 2.22 15min: 1.4
Memory Usage	71%
CPU Usage	Total: 25% CPU0: 28% CPU1: 229
System Time	2023-10-03 15:10
System Up Time	11min
Boot Version	0.0.0.5
Serial Number	2
Part Number	9
MAC Address	C0:74:AD:
System Version	1.0.4.6
Hardware Version	V1.3A
Device Name	GWN7002 🗹

NETWORK SETTINGS

In this section, the user can find general network settings of the router. These settings include WAN port configuration, general LAN ports configuration, in addition to IGMP protocol configuration, and hardware acceleration settings for the router.

Port Configuration

To access port configuration, please access the user interface of the GWN700X router and then navigate to **Network Settings** \rightarrow **Port Configuration**.

• Port Status

On the top, you can find the status of all the ports of the router.

- Violet color: port speed is 2.5Gbps (works only with SFP ports and 2.5Gbps SFP module).
- Green color: port speed is 1Gbps.
- Light green color: port speed is 100Mbps/10Mbps.
- Grey color: link down.
- White color: port disabled.
- Internet icon: port connected to the internet (for WAN ports).

Port Configuration	
	100Mbps/10Mbps Link down Disabled Connected to the Internet extour Petitik
	6 5 4 3 9 2 sep sep
USB	LAN LAN WAN LAN WAN

Port configuration – part 1

• Port Configuration

Port configuration page allows the user to configure the settings related to all the ports of the router; this includes the gigabit Ethernet ports as well as the SFP ports. The settings that can be edited include flow control, speed and duplex mode.

Port	Port Enable 🕕	Port Type	Name	Role	Speed/Duplex 🛈	Flow Control ①
Port 1		GE	÷-	LAN	Auto Negotiation ~	Auto Negotiation
Port 2		GE	2	LAN	Auto Negotiation \sim	Auto Negotiation
Port 3		GE		LAN	Auto Negotiation \sim	Auto Negotiation
Port 4		GE	-	LAN	Auto Negotiation $~~$	Auto Negotiation
Port 5		GE		LAN	Auto Negotiation \sim	Auto Negotiation
Port 6		GE		LAN	Auto Negotiation ~	Auto Negotiation
Port 7		GE		LAN	Auto Negotiation ~	Auto Negotiation
Port 8		GE	-	LAN	Auto Negotiation ~	Auto Negotiation
Port 9		GE	WAN2	WAN	Auto Negotiation V	Auto Negotiation
Port 10		SFP		LAN	Auto Negotiation 🗸 🗸	Disable
Port 11		SFP	WAN1	WAN	Auto Negotiation 🔷	Disable
					Auto Negotiation	

Port configuration – part 2

Port	This field indicates the port number.
Port enabled	Toggle ON or OFF the port. Note: When set to disabled, this physical port is disabled and all port-based configurations do not take effect.
Port Type	This field indicates the port type. • GE: Stands for Gigabit Ethernet • SFP: Small form-factor Pluggable
Name	This indicates the port name.
Role	This indicates the port role. • LAN • WAN
Speed/Duplex	In this setting, the user can configure the duplex mode as well as the speed of the port. The speed of the port can be set to: 10M, 100M, and 1000M for Ethernet ports and 1000M, 2500M for SFP ports. The duplex setting of the port can be set to: <i>Half Duplex</i> and <i>Full Duplex</i> . When the mode is set to Auto Negotiation , the router will determine based on the settings negotiated with the device connected.
Flow Control	The user can enable or disable flow control using this option. <i>Note:</i> When the setting is set to Auto Negotiation, the router will determine based on the settings negotiated with the device connected.

Port configuration – part 2

• **PoE Configuration**

The user can also control the total power limited that the router can supply through PoE. The power supplied can also be controlled on the port level.

PoE Configuration ^

	Total Power Limit ()	Auto 12.8W 24.8W		
Port	Power Supply Mode ①	Maximum Power Supply ①	Priority	
Port 5	Active PoE(802.3af/at)	~ 5.2W	~ Low	~
Port 6	Active PoE(802.3af/at)	~ 9W	~ High	~

Port configuration – PoE configuration

Total Power Limit	 This configures the power limit which can be supplied through PoE. Auto: Automatically detect the type of the power supply and select the output power. When the DC/PoE+ input is detected, the total power limit is 12.8W 12.8W: This can be selected if the power adaptor output values which correspond to the following values: 24VDC 1A 24.8W: This can be selected if power adaptor output values which corresponds to the following values: 24VDC 1.5A.
Port	This field indicates the port number.
Power Supply Mode	 This option configures the power supply mode. Active PoE (802.3af/at) 48V Passive PoE Off Note: When the 48V passive PoE mode is selected, the router will always supply power. It is not safe for non-POE powered devices (PD) to access this port. Please ensure that the connected PD devices support 48V passive PoE.
Maximum Power Supply	Configures the maximum power supplied by the router. 5.2W 9W 12.8W Note: If the power supply mode is Active PoE (802.3af/at) or 48V passive PoE , ensure that the sum of the maximum power supplied to all ports is less than the total power limit.
Priority	 Specify the priority of the port in terms of the power supply. High Low

Port configuration – PoE configuration

WAN

The WAN ports can be connected to a DSL modem or a router. WAN port support also sets up static IPv4/IPv6 addresses and configure PPPoE.

On this page, the user can modify the setting for each WAN port, and also can delete or even add another WAN, Adding a WAN port will reduce the LAN ports number. In the case where there is more than one WAN port, load balancing or backup (Failover) can be configured.

If a GWN router is added to either GDMS Networking or GWN Manager, the **WAN Speed Test** feature will be available to users. Please for more details check GWN Management Platforms – User Guide (WAN Speed Test).

WAN										
Add										
WAN Name	Status	Port	Connection Type	IPv4 Address	IPv4 Status	IPv6 Address	IPv6 Status	VPN Connection Type	VPN IP Address	Operations
WAN2		Port3 (GE)	IPv4: DHCP IPv6: -	192.168.5.99	Connected	Local IPv6: - Global IPv6: -	Disconnected		-	C Ū
WAN4		Port4 (GE)	IPv4: DHCP IPv6: -		Disconnected	Local IPv6: - Global IPv6: -	Disconnected			ľ



Click on _____ to add another WAN port or click on the "edit icon" to edit the previously created ones.

WAN > Edit WAN		
Basic Information 🥎		
Enable		
"WAN Name	WAN1	1~64 characters
*Port	Port 3 (GE) ~	
IPv4 Settings 🔿		
Connection Type	Obtain IP automatically (DHCP) \sim	
Static DNS		
VPN		
IPv6 Settings 🗸		
Advanced Settings 🔿		
*Maximum Transmission Unit (MTU)①	1500	Default 1500, range 576~1500
WAN Connection Detection ①		
	This function is effective only when the device has multiple WAN ports enabled. If disabled, the interface will always be online and will not update the connection status due to routing tracking errors. You can go to (<u>Policy Routing > Policy Pool</u>) to customize the policy routing rules.	
	Cancel Save	

Add or Edit WAN

Please refer to the following table for network configuration parameters on the WAN port.

	Basic Information
Enable	Click to enable or disable the WAN
WAN Name	Enter a name for the WAN port
Port	Select from the drop-down list the port to be used as a WAN.
	IPv4 Settings
Connection Type	 Obtain IP automatically (DHCP): When selected, it will act as a DHCP client and acquire an IPv4 address automatically from the DHCP server. Enter IP Manually (Static IP): When selected, the user should set a static IPv4 address, IPv4 Subnet Mask, IPv4 Gateway and adding Additional IPv4 Addresses as well to communicate with the web interface, SSH, or other services running on the device. Internet Access with PPPoE account (PPPoE): When selected, enter the PPPoE account and password. PPPoE Service Name is optional and specifies the service identifier required by some ISPs to connect to specific network services. Leave blank unless provided by your ISP. The default setting is "Obtain IP automatically (DHCP)".
Static DNS	Toggle ON or OFF to enable or disable static DNS
Preferred DNS Server	Enter the preferred DNS Server, ex: 8.8.8.8
Alternative DNS Server	Enter the altenative DNS Server, ex: 1.1.1.1

VPN	Toggle ON or OFF to enable or disable VPN
VPN Connection Type	 L2TP: Layer Two Tunneling Protocol (L2TP) is an extension of the Point-to-Point Tunneling Protocol (PPTP) used by internet service providers (ISPs) to enable virtual private networks (VPNs). PPTP: Point-to-Point Tunneling Protocol (PPTP) is a network protocol that enables the secure transfer of data from a remote client to a private enterprise server by creating a virtual private network (VPN) across TCP/IP-based data networks.
Username	Enter the username to authenticate into the VPN server.
Password	Enter the password to authenticate into the VPN server.
Server Address	Enter the IP address or the FQDN of the VPN server.
MPEE Encryption (if PPTP is selected)	When PPTP is chosen as the VPN Connection Type , the user can choose to toggle on or off the MPEE Encryption.
ІР Туре	 Dynamic IP: The IP will be assigned statically using DHCP. Static IP: The IP will be assigned statically.
IP Address	If IP Type is set to Static IP , specifies the static IP address.
Subnet Mask	If IP Type is set to Static IP , specifies the subnet mask.
Default Gateway	If IP Type is set to Static IP , specifies the default gateway.
VPN Static DNS	Enable this option to use the statically assigned DNS server addresses.
Preferred DNS Server	If VPN Static DNS is enabled, specifies the preferred DNS server.
Alternative DNS Server	If VPN Static DNS is enabled, specifies the alternative DNS server.
Maximum Transmission Unit (MTU)	This configures the value of the maximum transmit unit. The valid range for this value is 576 - 1460. The default value is 1430. <i>Note: Please do not change this value unless it's necessary.</i>
	IPv6 Settings
IPv6	Enable this option to use IPv6 on this specific WAN port.
Connection Type	 Obtain IP automatically (DHCPv6) Enter the IP manually (static IPv6) Internet Access with PPPoE account (PPPoE): must enabled and configured on IPv4 then the user must enter the PPPoE credentials (PPPoE Account, PPPoE Password) and PPPoE Service name is optional.
IPv6 Address/Prefix Length	When the Connection Type is set to <i>Static IP</i> , the user can enter the static IP address and prefix length. <i>Note: This option appears only when the</i> Connection Type <i>is set to Static IPv6</i> .

IPv6 PD/Prefix Length	When the Connection Type is set to Static IP, the user can enter the IPv6 PD and prefix length. <i>Note: This option appears only when the</i> Connection Type <i>is set to Static IPv6.</i>
Default Gateway	Enter the IP address of the default gateway Note: This option appears only when the Connection Type is set to Static IPv6.
Static DNS	Enable this option to enter statically assigned DNS. <i>Note:</i> This option appears only when the Connection Type is set to DHCPv6.
Preferred DNS Server	Enter the IP address of the preferred DNS server. Note: This option appears only when the Connection Type is set to Static IPv6.
Alternative DNS Server	Enter the IP address of the alternative DNS server Note: This option appears only when the Connection Type is set to Static IPv6.
IPv6 Relay to VLAN	Once enabled, relay IPv6 addresses to clients on the LAN side. Note: This function will take effect only "IPv6 Relay from WAN" is enabled on VLAN.
	Advanced Settings
	Configures the maximum transmission unit allowed on the wan port.
Maximum Transmission Unit (MTU)	 When using Obtain IP automatically (DHCP), the valid range that can be set by the user is 576-1500 bytes. The default value is 1500. Please do not change the default value unless you have to. When using PPPoE, the valid range that can be set by the user is 576-1492 bytes. The default value is 1492. Please do not change the default value unless you have to. When IPv6 is enabled on the WAN, the minimum MTU is 1280.
WAN Connection Detection	Enables detection of WAN status when multiple WAN ports are active. If disabled, the WAN is always considered online, which can cause routing errors. Enabling this feature allows Policy Routing to switch to a standby WAN when the primary connection fails. Customize rules in Policy Routing > Policy Pool .
Tracking IP Type	Select system Default, or select Custom to specify a custom tracking IP e,g. 8.8.88.
Tracking IP	Enter the tracking IP if Tracking IP Type set to custom, click on Plus icon to add more.
VLAN Tag	Toggle ON or OFF to enable or disable VLAN Tag
	Enter the VLAN Tag ID with the priority
VLAN Tag ID	Notes: • Priority is 0~7 with 7 being the highest priority. Default is 0. • Multiple WANs can use the same VLAN ID.
Bridge mode	Toggle ON to enable Bridge Mode, which allows the WAN port to act as a bridge between specific VLANs.
VLAN Tag ID/Port/Priorit y	Enter the VLAN Tag ID and assign a port for traffic bridging.Set the priority for the VLAN traffic (0-7), where 7 represents the highest priority.
Multiple Public IP Address	Toggle ON or OFF to enable or disable Multiple Public IP Address <i>Note: Please use with Port Forward function, so that you can access to router via public IP address.</i>
Public IP	Enter a public IP address

Triple play

Triple Play feature the user to benefit from multi-service plan (depends on ISP provider), and with a single WAN connection each service e.g: Internet, Voice (VoIP) and IPTV can be separated using VLANs and a specific port.

Navigate to **Network Settings** \rightarrow **WAN** \rightarrow **Edit/Add WAN**, then scroll down and search for Bridge Mode, please refer the figure below:

> Add WAN				
VLAN Tag				
*VLAN Tag ID	VLAN Tag ID Enter VLAN Tag ID	Priority ① 0		
Bridge Mode				
*VLAN Tag ID/Port/Priority()	VLAN Tag ID	Port ①	Priority (1)	
	34	LAN1 (GE) \times	4	•
	35	LAN2 (GE) $ imes$	3	¢
	35 36	LAN2 (GE) × LAN3 (GE) ×	6	

Triple Play

LAN

To access the LAN configuration page, log in to the GWN700x WebGUI and go to **Network Settings** \rightarrow **LAN**. VLAN configuration such as adding VLANs or setting up a VLAN port can be found here on this page, as well as the ability to add Static IP Bindings, local DNS Records and Bonjour Gateway.

LAN	LAN						
VLAN	VLAN Port Settings	Static IP Binding	Local DNS Records	Bonjour Gateway			
Add	Delete						
VLAN	I ID	Name	IPv4 Address				
1		Default LAN	192.168.80.1				
20		Guests	190.168.20.1				

LAN configuration

VLAN

GWN700x router integrates VLAN to enhance security and add more functionalities and features. VLAN tags can be used with SSIDs to separate them from the rest, also the user can allow these VLANs only on specific LANs for more control and isolation and they can be used as well with policy routing.

• Add or Edit VLAN

To Add or Edit a VLAN, Navigate to **Router Interface** \rightarrow **Network Settings** \rightarrow **LAN**. Click on + Add button or click on \angle Edit button.

LAN > Edit VLAN		
* VLAN ID	2	
Name	Guests	0~64 character
Forwarding Destination Group ①	All ×	
Enable Captive Portal		
	① It is not recommended to use it together with SSID-Portal authentication after it is enabled. If used with GWN AP (version not less than 1.0.25.20), please go to (<u>Captive Fortal > Policy</u>) to set the AP device that requires ByPass.	
* Captive Portal Policy	Wired Captive Portal \sim	

Add or Edit VLAN – Part 1

IPv4 Settings \land					
VLAN Port IPv4 Address					
* IPv4 Address	20.0.0.1				
Subnet Mask	255.255.255.0				
DHCP Service					
* IPv4 Address Allocation Range	20.0.0.2	- 20.0	0.0.254		
Release Time(m)	120			Default 120, range 60-2880	
DHCP Option	Option ()	Туре	Service 🕕	Content (1)	
	43	ASCII	 Custom 	128	
			Custom		Add
			ACS URL		
Preferred DNS Server	8.8.8.8		ProvisioningC		
Alternative DNS Server	1.1.1.1		Firmware Serv		
Alternative Dito Server			VLAN ID		
IPv4 Routed Subnet ()			VLAN Priority Manager Serv		
Interface	WAN1 (WAN)		Manager Serv		
IPv6 Settings 🔿					
VLAN Port IPv6 Address					
	Cancel	Save			

Add or Edit VLAN – Part 2

VLAN ID	Enter a VLAN ID Note: VLAN ID range is from 2 to 4094.
Name	Enter the VLAN name
Forwarding Destination Group	By default, "All" is selected, and the interfaces set in the default rule of the policy pool (WAN or VPN) are selected by default and cannot be unchecked here, and subsequent new interfaces are automatically included.
Enable Captive Portal	Toggle this option to activate Captive Portal authentication for devices connected through this VLAN. It is not recommended to enable this alongside SSID-Portal authentication. If using a GWN AP with firmware version 1.0.25.20 or later, ensure to configure ByPass for the AP under Captive Portal > Policy to avoid conflicts.
Captive Portal Policy	Select the Captive portal policy from the drop-down list or click on "Add Policy " to add a new one.
	VLAN Port IPv4 Address
IPv4 address	Enter IPv4 Address
Subnet Mask	Enter Subnet Mask
DHCP Server	By default it's "Off", choose "On" to specify the IPv4 address Allocation Range
IPv4 Address Allocation Range	Enter the start and the end of the IPv4 address Allocation Range.
Release Time(m)	The default value is 120, and the valid range is 60~2880.
DHCP Option	Select the option, type, service and content for each DHCP option. Click on "Plus" or "Minus" icons to add or delete an entry.
	 Option: The range is 2-254, exclude 6, 50-54, 56, 58, 59, 61, 82 Type: three options are possible: ASCII, HEX and IP address Service: When the option is 43 and the type is an ASCII string, the service can be selected. DHCP Option 43 is typically used for vendor-specific configurations and can vary depending on the device. Content: "Hexadecimal String", please enter XX:XX:XX format or a valid even-bit hexadecimal string. "ASCII string" or "Decimal", the content limit is 1-255 characters. Here are some commonly configured

	 services: ACS URL: Auto-Configuration Server URL for TR-069 protocol, allowing remote management. Provisioning Code: Used for specifying a unique identifier for automatic provisioning.
	 VLAN ID: Can be set to assign a specific VLAN ID to a device. Bootstrap URL: URL for devices to pull initial configuration files. Time Servers: Configure specific time server addresses for devices. TFTP Servers: Define TFTP server addresses for firmware or configuration files.
	 Network Policy Settings: Define policies that might be needed by VoIP or IP phones for network access.
Preferred DNS Server	Enter the Preferred DNS Server
Alternative DNS Server	Enter the Alternative DNS Server
IPv4 Routed Subnet	Once enabled, clients under the VLAN will be allowed to access the Internet using their real IP addresses.
Interface	Select the WAN interface from the drop-down list
	VLAN Port IPv6 Address
IPv6 Address Source	Select from the drop-down list the WAN port
Interface ID	Toggle ON or OFF the interface ID
Customize Interface ID	Enter the interface ID
IPv6 Preferred DNS Server	Enter the IPv6 Preferred DNS Server
IPv6 Alternative DNS Server	Enter the IPv6 Alternative DNS Server
IPv6 Relay form WAN	Once enabled, clients will get IPv6 addresses directly from the WAN side. Note: This function will take effect only "IPv6 Relay to VLAN" is enabled on the WAN side.
	Select from the drop-down list the IPv6 address assignment
IPv6 Address	• Disable
Assignment	• SLAAC
	Stateless DHCPv6 Stateful DHCPv6

Add/edit VLAN

Note

Find below the number of VLANs which can be created in each model:

- GWN7001: 16 VLANs
- GWN7002: 16 VLANs
- GWN7003: 32 VLANs

VLAN Port Settings

The user can use LAN ports to allow only specific VLANs on each LAN port and in case there are more than one VLAN then there is an option to choose one VLAN as the default VLAN ID (PVID or Port VLAN Identifier). Click on \checkmark to edit the VLAN Port Settings or click on $\boxed{11}$ to delete that configuration and bring back the default settings which is by default VLAN 1.

AN					
VLAN	VLAN Port Settings	Static IP Binding	Local DNS Records		
LAN	PVID	Allowe	l VLANs		Operation
Port2 (SFP)	1	1,7			1
Port4 (GE)	1	1,7			1 🔟
Port5 (GE)	1	1,7			1
ort6 (GE)	1	1,7			<u> </u>
			Port 4 (GE) *Allowed VLANs 1 2 7	×	
			*PVID	~	
			Cancel Save		

VLAN Ports

Allowed VLANs	Choose the VLANS to be allowed on this port.
PVID	Select the Port VLAN Identifier or the default VLAN ID

VLAN Port Settings

Static IP Binding

The user can set IP static binding to devices in which the IP address will be bound to the MAC address. Any traffic that is received by the router which does not have the corresponding IP address and MAC address combination will not be forwarded.

To configure Static IF	' Binding, please na	avigate to Network	Settings → LAN -	→ Static IP Binding,	refer to the fig	ure and table
below:						

LAN > Static IP Binding		
*VLAN	Default	×
Binding Mode	MAC Address Client ID	
Binding Devices	Input manually	~
* MAC Address	C0 : 74 : AD : 88 : 88 : 88	
Device Name	Test PC	1~64 characters
* IP Address	192.168.7.99	
	Cancel Save	

Static IP Binding

VLAN	Select the VLAN from the drop-down list.
Binding Mode	select the binding mode, either using the client MAC address or Client ID.
Binding Devices	Select the device MAC address from connected devices list. Note: only available bindind mode is set to MAC Address.
Client ID Type	Select the client ID type, either based on: MAC Address ASCII Hex Note: only available bindind mode is set to Client ID.

MAC Address	Enter the MAC Address Note: only available bindind mode or Client ID Type is set to MAC Address
ASCII	Enter the ASCII Note: only available Client ID Type is set to ASCII
Hex	Please enter XX:XX:XX format or a valid even-digit hexadecimal number string, the first two digits need to enter the type value. Note: only available Client ID Type is set to Hex
Device Name	Enter a name for the device
IP Address	Enter the static IP address based on the VLAN selected previously.

Static IP Binding

Local DNS Records

Local DNS Records is a feature that allows the user to a DNS records into the router which can be used to map the domain name to an IP address. This feature can be used when the user needs to access a specific server using a domain name instead of an IP address when they do not want to include the entry in public DNS servers. To add a local DNS record, please navigate to **Network Settings** \rightarrow **LAN** \rightarrow **Local DNS Records**, then click "Add"

	Add Local DNS Reco	rds
Domain () 1~256 character		
www.mycor		
∗IP Address		
44.7.5.66		
Status		
	Cancel Save	
	Calicei	

Add Local DNS Records

- Enter the domain name in "Domain"
- Then, enter the IP address to which the domain name will be mapped to.
- Toggle on the "Status" for the mapping to take effect.

Bonjour Gateway

The Boujour service is a zero-configuration network that enables automatic discovery of devices and services on a local network. For example: it can be used on a local network to share printers with Windows® and Apple® devices.

Once enabled, Bonjour services (such as Samba) can be provided to Bonjour supporting clients under multiple VLANs. Once enabled, configure the services of the VLANs and proxies that need to intercommunicate.

To start using Bonjour Gateway, Toggle ON or OFF the service first, then select the VLAN and the services as shown below:

LAN				
VLAN	VLAN Port Settings	Static IP Binding	Local DNS Records	Bonjour Gateway
	Bonjour	Gateway		
	*VLAN ①		All VLANs \times	
	*Servcies		Please Select S	ervcies Q
			Any	
			AirPlay	
			AirPrint	
			chromeCas	st
			FTP	
			HTTP	
			iChat	
			Samba	
			SSH	

Bonjour Gateway

IGMP

When IGMP Proxy is enabled, the GWN router can issue IGMP messages on behalf of the clients behind it, then the GWN router will be able to access any multicast group.

To start using IGMP Proxy:

- 1. Toggle ON IGMP Proxy first.
- 2. Select the WAN interface to be used from the drop-down list (*Note: IGMP proxy cannot be enabled on a WAN port with bridge mode enabled*)
- 3. Select the version, be default is Auto.

The user can also enable IGMP Snooping. Once enabled, multicast traffic will be forwarded to the port belonging to the multicast group member. This configuration will be applied to all LAN ports.

IGMP			
General Settings	IGMP Multicast Group Table		
	IGMP Proxy		
	IGMP Proxy	Once enabled, IGMP proxy are allowed to access any multicast group	
	* Interface ①	WAN2 (WAN)	
	IGMP Version	Auto ~	
	Query Interval (secs)	125	Default 125, range 1~1800
	IGMP Snooping		
	IGMP Snooping	Once enabled, multicast traffic will be forwarded to the port belonging to the multicast group member. This configuration will be applied to all LAN ports	
		Cancel Save	

IGMP – General Settings

On the IGMP Multicast Group Table, all the active multicast groups will be displayed here.

IGMP		
General Settings	IGMP Multicast Group Ta	ble
Refresh		
Multicast Group A	ddress	Interface
224.0.0.1		Port 6,Port 5,Port 4,Port 3,Port 1,Port 2

IGMP – IGMP Multicast Group Table

Network Acceleration

Network acceleration allows the router to transfer data at a higher rate when Hardware acceleration is enabled. This ensures a high performance.

Network Acceleration	
Hardware Acceleration	Once enabled, QoS, rate limit, traffic statistic, and content security will not take effect. Please proceed with caution.
	Cancel
	Hardware Acceleration

Once enabled, QoS, rate limit, traffic statistic, and content security will not take effect. Please proceed with caution.

CLIENTS

Clients page keeps a list of all the devices and users connected currently or previously to different LAN subnets with details such as the MAC Address, the IP Address, the duration time, and the upload and download information etc.

The clients' list can be accessed from GWN700x's **Web GUI** \rightarrow **Clients** to perform different actions for wired and wireless clients.

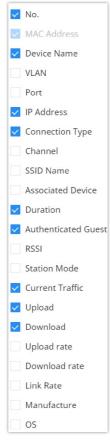
- Click on "Clear offline clients" to remove clients that are not connected from the list.
- Click on "Export" button to export clients list to local device in a EXCEL format.
- Click on "Status Detection" toggle to enable/disable the online and offline status.

Please refer to the figure and table below:

Clear	offline clients Expo	Status Dete	ection 🚺 🔹 Online	: 2 • Offline: 0					
All Co	nnection T	~ /	All VLANs 🗸	All associated devic	~ Q MAC / IP	Address / Device Name			
No.	MAC Address	Device Name	IP Address	Connection Type	Duration 🗘	Authenticated Guest	Current Tr ≑	Uplo Operations	=
	• C0:74:AD:E3:EA:28	Grandstream	IPv4:192.168.80.158 IPv6:-	Wired	5min	No	33.71KB	16.98 🛈 🗹	
2	• C0:74:AD:BA:24:FC	Grandstream	IPv4:192.168.80.37 IPv6:-	Wired	5h 1min	No	778.51KB	474.2 (1) 🗹	



The users also have the option to customize this page by adding or removing desired columns, check the figure below for the available options:



Client page options

MAC Address	This section shows the MAC addresses of all the devices connected to the router.
Device Name	This section shows the names of all the devices connected to the router.
VLAN	Displays the VLAN the client connected to.
IP Address	This section shows the IP addresses of all the devices connected to the router.
Connection Type	 This section shows the medium of connection that the device is using. There are two mediums which can be used to connect: Wireless: Using an access point with the router. Wired: Using an ethernet wired, either connected directly to one of the router's LAN ports, or through a switch.
Channel	If device is connected through an access point, the router will retrieve the information of which channel the device is connected to.
SSID Name	If device is connected through an access point, the router will retrieve the information of which SSID the device is connected to.
Associated Device	In case of an access point or an access point with the router, this section will show the MAC address of the device used
Duration	This indicates how long a device has been connected to the router.
RSSI	RSSI stands for <i>Received Signal Strength Indicator</i> . It indicates the wireless signal strength of the device connected to the AP paired with the router.

Station Mode	This field indicates the station mode of the access point.
Total	Total data exchanged between the device and the router.
Upload	Total uploaded data by the device.
Download	Total downloaded data by the device.
Current Rate	The real time WAN bandwidth used by the device.
Link Rate	This field indicates the total speed that the link can transfer.
Manufacturer	This field indicates the manufacturer of the device.
OS	This field indicates the operating system installed on the device.



• Edit Device

under the operations column click on "**Edit**" icon to set the name of the device, and assign a VLAN ID and static address to the device. It's also possible to limit bandwidth for this exact device and even assign a schedule to it from the list. Refer to the figure below:

Clients > Edit Client		
Device Name	Ain	1~64 characters
Bandwidth Limit		
Maximum Upload Bandwidth	10 Mbps	 The range is 1–1024, if it is empty, there is no limit
Maximum Download Bandwidth	20 Mbps	The range is 1~1024, if it is empty, there is
Bandwidth Schedule ()		no limit
* Schedule	Office hours	~
Static IP		
* VLAN	Default	~
* IP Address	192.168.80.11	Range 192.168.80.2~192.168.80.254
ii Adarcas	Cancel Save	
	Edit Device	

• Delete Device

To delete a device, go to the **Operations** column and click the button in then click "**Delete**". Please note that you can only delete the devices which are offline, the devices online cannot be deleted.

• View Client Information and Report

Click on a device to open the full report of the traffic used by the device. The report will contain the total data uploaded and downloaded, as well as the statistics used by each application on the device.

	(Ain)					
verview Device Info						
ently 1H 12H 1I	D 1W					
ipeed		Total 🕈 12.03MB 🌢 134.73MB	APP Traffic Statistics			
6258bps	\frown					
46.88Kbps		· · · ·				
168.75Kbps 190.63Kbps					YouTube	62.24
312.5Kbps					AmazonAWS	13.52
34.38Kbps					 WireGuard Google 	8.829
56.25Kbps					TLS	4.237
IPP List					All APP Groups	Q. Search Name
	App Group	Percentage	Total 0	Upload ‡		Q. Search Name
Name	App Group Media Streaming Services	Percentage 62.24%	Total 0 62.85MB	Upload ÷ † 1.24MB	Dor	
Name YouTube					Do	wnload ‡
Name YouTube AmazonAWS	Media Streaming Services	62.24%	62.85MB	🕈 1.24MB	Dor 4	wnload 0 61.61MB
Name YouTube AmazonAWS WireGuard Google	Media Streaming Services Web Services	62.24%	62.85MB 13.66MB	 ↑ 1.24MB ↑ 2.01MB 	Dor 4 4	wnload 0 61.61MB 11.64MB
Name YouTube AmazonAWS WireGuard	Media Streaming Services Web Services Tunneling and Proxy Services	62.24% 13.52% 8.82%	62.85MB 13.66MB 8.9MB	 ↑ 1.24MB ↑ 2.01MB ↑ 1.11MB 	Dor 4 4	wnload © 61.61MB 11.64MB 7.79MB
Name YouTube AmazonAWS WireGuard Google TLS	Media Streaming Services Web Services Tunneling and Proxy Services Web Services	62.24% 13.52% 8.82% 4.23%	62.85MB 13.66MB 8.9MB 4.27MB	 ↑ 1.24MB ↑ 2.01MB ↑ 1.11MB ↑ 1.53MB 	Dor 4 4 4	wnload © 61.61MB 11.64MB 7.79MB 2.74MB
Name YouTube AmazorAWS WireGuard Google	Media Streaming Services Web Services Tunneling and Proxy Services Web Services Web Services	62.24% 13.52% 8.82% 4.23% 2.5%	62.85MB 13.66MB 8.9MB 4.27MB 2.53MB	 ↑ 1.24MB † 2.01MB † 1.11MB † 1.53MB † 101.38KB 	Do'	wnload * 61.61MB 11.64MB 7.79MB 2.74MB 2.43MB
Name YouTube AmazonAWS WireGuard Google TLS GoogleCloud	Media Streaming Services Web Services Tunneling and Proxy Services Web Services Web Services Infrastructure	62.24% 13.52% 8.82% 4.23% 2.5% 2.17%	62.85MB 13.66MB 8.9MB 4.27MB 2.53MB 2.19MB	 ↑ 1.24MB ↑ 2.01MB ↑ 1.11MB ↑ 1.53MB ↑ 101.38KB ↑ 79.61KB 	Do'	wnload © 61.61MB 11.64MB 2.79MB 2.43MB 2.43MB 2.11MB

Device Overview

To see information related to the device, please click on **Device Info** tab.

Clients > Clients (DESK	FOP-IVU4H2Q)
Overview Device Info	
MAC Address	an one shares
Device Name	DESKTOP-IVU4H2Q
IPv4 Address	192.168.80.64
IPv6 Address	
Connection Type	Wired
Channel	-
SSID Name	-
Associated Device	C0:74:AD:BF:AF:50
Duration	22min
RSSI	
Station Mode	
Network Traffic	756.46MB ↑ 363.09MB ↓ 393.38MB
Current Rate	↑ 48.19Kbps ↓ 434.4Kbps
Link Rate	
Manufacture	
OS	WINDOWS

Device Info

VPN

VPN stands for "Virtual Private Network" and it encrypts data in real time to establish a protected network connection when using public networks.

VPN allows the GWN700x routers to be connected to a remote VPN server using PPTP, IPSec, L2TP, OpenVPN® and WireGuard® protocols, or configure an OpenVPN® server and generate certificates and keys for clients.

GWN700X routers support the following VPN functions:

- **PPTP:** Client and server
- IPSec: Site-to-site and client-to-site
- OpenVPN®: Client and server
- L2TP: Client
- WireGuard®: Server

For more details on how to configure each VPN protocol separately, please refer to the below guides:

1. OpenVPN®

- OpenVPN® Site-to-Site Guide
- OpenVPN® Client-to-Site Guide

2. **L2TP**

• L2TP Client Guide

3. PPTP Guide

• PPTP Client-to-Server Guide

4. WireGuard®

- WireGuard Site-to-Site Guide
- WireGuard Client-to-Server Guide

5. IPSec

- IPSec Site-to-Site Configuration Guide
- IPSec Client-to Site Configuration Guide

VPN page can be accessed from the GWN700x **Web GUI** \rightarrow **VPN**.

Setup Wizard

The main purpose of the Setup Wizard is to help users quickly and efficiently configure VPNs like **WireGuard®**, **IPSec**, **OpenVPN®**, **PPTP**, and **L2TP**. It allows you to configure VPN connections with minimal manual input by automating most of the necessary steps and parameters. This makes it particularly useful for users who may not be familiar with more advanced networking settings.

- **Easy Deployment**: The wizard simplifies VPN deployment, supporting various networking scenarios, including both **client-to-site** and **site-to-site** connections.
- **Predefined Configuration**: Users can select from predefined VPN options, such as WireGuard®, IPSec, OpenVPN®, etc., based on their needs. Each type of VPN comes with different available scenes and configurations.

Purpose: The primary goal of this wizard is to make VPN setup **faster** and **easier** by automating many of the common settings. This reduces the likelihood of misconfigurations and ensures a smoother setup experience, especially for users who may not have in-depth knowledge of VPN protocols.

	Recommen
🔞 WireGuard®	
Secure modern VPN tunnel technology, using the most advanced encryption technology. If solution.	you connect to terminal devices such as mobile phones and computers, we recommend this
Lightweight, small memory usage	Faster and low latency than OpenVPN
Easy to deploy, supporting a variety of networking scenarios	Configuration generation and quick export
IPSec	
Standardized network security protocol, providing a point-to-point security that can be implemented in various operating systems and network devices.	A popular and widely used VPN protocol that uses encryption and authentication to create a secure tunnel between users and servers.
Highly secure and flexible	Compatible with multiple platforms such as Windows, Mac. Android, IOS, etc.
With GDMS Networking, one-stop automatic networking. links can be automatically rebuilt after WAN IP changes.	Certificate management can effectively manage the timeliness of access users
Improve data transmission performance and efficiency through hardware acceleration and optimized configuration	Multiple authentication methods such as User, SSL (certificate), suitable for various networking scenarios
Other	ypes
PPTP VFN protocol with wide compatibility.	L2TP It is an extension of the PPTP protocol used by Internet service providers (ISPs) and does not provide any encryption itself.
Supports multiple operating platforms such as Windows, macOS, Linux and mobile platforms	A traditional VPN is canceling support for many different operating systems



Relation to Manual Configuration: It's important to note that the VPN Setup Wizard mirrors the **same configuration process** as manually configuring VPNs, but in a more user-friendly way. Advanced users can still manually configure VPNs if needed, but for most users, the wizard offers a more accessible method. The wizard is tailored for each VPN type. For instance:

- WireGuard®: Prioritizes fast, low-latency connections with a simple and secure setup.
- IPSec: Provides robust encryption and secure communication for both site-to-site and client-to-site scenarios.
- **OpenVPN**®: Allows more customizable security options, such as user-based certificate management and SSL encryption.
- PPTP/L2TP: While legacy protocols, these are supported for backward compatibility with older devices and systems.

By following this wizard, users can rapidly configure the required VPN connections without needing to navigate complex settings manually, making it an ideal solution for businesses looking to enhance security without complexity.

• WireGuard® Setup Wizard

Setup Wizard > WireGuard®				
Select Interface	Select Scene	Configure Protocol	Configuration Overview	Finish
	Select W	ireGuard® Ac	-	
*Name	WireGard®			1~64 characters
*Interface	WAN2 (WAN)		~	
*Local IP Address	192.168.49.1			
*Subnet Mask 🛈	255.255.255.0			Only support input range 255.255.255.0-255.255.255 supported
		Back Next		

WireGuard® Example

• IPSec Setup Wizard

Select Scene Configure Protocol	Configuration Overview Finish
Site-to-Site	·
Site	Site

IPSec Example

• OpenVPN ® Setup Wizard

	Select Scene	Configure Protocol	Configuration Overview	Finish	
Client-to-Site			Site-to-Site		
Clients		Site	Site		Site
	OpenVPN® Tunnel			OpenVPN@ Tunnel	,

• PPTP Setup Wizard

	Select Scene	Configure Protocol	Configuration Overview		
Client-to-Site		<u>~</u>	Site-to-Site		
Clients		Site	Site		Site
	PPTP Tunnel			PPTP Tunnel	
	PPTP Tunnel		بماليم	PPTP Tunnel	
		TT	TT		



• L2TP Setup Wizard

Select Scene Configure Protocol	Configuration Overview Finish
Site-to-Site	
Site	Site
	ii

L2TP Example

WireGuard®

WireGuard[®] is a free, open-source VPN solution that offers high performance, ease of use, and robust security for encrypting virtual private networks. The GWN700x series routers support WireGuard[®] VPN with features like automatic client generation and QR code scanning for easy setup on mobile devices and other devices with camera support. WireGuard[®] can be configured to create Peers for Site-to-Site connections or to establish clients for terminal devices, such as mobile phones and computers.

To start using WireGuard[®] VPN, please navigate to **Web UI** \rightarrow **VPN** \rightarrow **WireGuard**[®] **page**. Click on "**Add**" button to add a WireGuard[®] server as shown below:

WireGuard®						
WireGuard®	Peers	Remote Clients				
				1		
				No data, please add.		
				Add		

Add WireGuard®

Please refer to the figure and table below when filling up the fields.

WireGuard® > Edit WireGuard®		
*Name	wireGuard	1~64 characters
Status		
* Interface	WAN2 (WAN)	Y
* Monitoring Port ()	51820	Default 51820, range 1024~65535
* Local IP Address	192.168.5.143	
* Subnet Mask	255.255.255.0	only support input range 255.255.255.0- 255.255.255.255 is supported
* Destination ()	All ×	~
* Private Key	kOWantd5KA8CL+h0C20OOWRP7AqiYsXCCWre6gq6H0=	44 bits
Public Key	Cone-click generation HnWFB0FPIAY7/Z1/2GqbHbLHER+AN+xza+xioxzjmBs= Copy	
* Maximum Transmission Unit (MTU) ③	1420	Default 1420, range 576~1440
	Cancel Save	

Add/Edit WireGuard®

Name	Specify a name for Wireguard® VPN.
Status	Toggle ON or OFF to enable or disable the Wireguard® VPN.
Interface	Select from the drop-down list the WAN port.
Monitoring Port	Set the local listening port when establishing a WireGaurd® tunnel. <i>Default:</i> 51820
Local IP Address	Specify the network that WireGuard® clients (Peers) will get IP address from.
Subnet Mask	Configures the IP address range available to the Peers.
Destination	Select the Destination(s) from the drop-down list. <i>Note: When selecting "All", subsequent new interfaces will be automatically included.</i>
Private Key	Click on "One-Click Generation" text to generate a private key.
Public Key	The public key will be generated according to the private key. Click on " Copy " text to copy the public key.
Maximum Transmission Unit (MTU)	This indicates the size of the packets sent by the router. Please do not change this value unless necessary. By default is 1450.

Add/Edit WireGuard®

Once finished configuring WireGuard[®], click on " **Add client**" icon to generate clients very quickly and easily as shown in the figures below:

WireGua	rd® 💾								
WireGuar	rd® Peers	Remote Client	S						
Add	Delete								
Na Na	ame	Enable	Ports	WireGuard® Address	Uptime	Upload	Download	Current Rate	Operations
🔽 Wi	reGuard		WAN1 (WAN)	192.168.6.223	6min	1.2GB	↓ 29.77MB	TX:70.73Kbps RX:0bps	C B Ū

Enter a name and toggle status **ON** then click on "Save" button.

VireGuard® > Create Client		
① It can automatically generate client configuration files for mo	bile phones, computers and other endpoints, and then obtain configurations fro	om the remote client list by scanning the QR code or directly downloadir
*Name	Client	1~64 characters, only support input in numbers, letters and special characters, does not support \$&#; ["/- ⇔\()
Enable * IP Address	172.29.222.3	Range 172.29.222.1-172.29.222.254
Pre-Shared Key	Once enabled, the pre-shared key is automatically generated	
* Client Allowed IPs 🛈	IP Subnet v 0.0.0/0	 Prefix Length range 0-32 Add 4
	① The IP address range in the configuration file will not take effect	
Preferred DNS Server	8.8.8	
Alternative DNS Server		
	Cancel Save	

WireGuard® Add client – part 1

Now, the user can either download the configuration file and share it, or download QR code for devices like mobile phones to scan.

	or mobile phones, computers and other terminals, and then obtain the configuration from the peer list	by scanning the QK code of downloading it of
*Name	pper4	1~64 characters
Status	Generate successfully	
* IP Address	⊘ The Peer configuration has been generated successfully, and you can visit the Peer page to view it later	Range 192.168.5.1~192.168.5.254
Pre-Sharec *Allowed IP	Each profile can only be used by one terminal at a time	•
Preferred	Image: Second system Image: Second system Image: Second	Add 🚯

WireGuard® Add clients – part 2

For more details, refer to this guide: WireGuard® Site-to-Client.

Peers

On the Peers tab, users can create Site-to-Site connections by clicking the 'Add' button to configure new WireGuard peers.

/ireGuard® Peers	Remote Clients					
Add Delete					All WireGuard	de v Q Name
V Name	Enable	WireGuard®	Endpoint Address : Port	Last Handshake	Actual Endpoint Address : Port	Operations
✓ Wireguard® Peer1		WireGuard				C Ū

WireGuard® – Peers tab

for more details, refer to this guide: WireGuard® Site-to-Site.

Please refer to the figure below when filling up the fields.

WireGuard® > Edit Peer							
* Name	Peer1						
Status							
*WireGuard	wireGuard						
* Public Key	HnWFB0FPIAY7/Z1/2GqbHbLHER+AN+xza+	44 bits					
Pre-Shared Key		أبيز	44 bits				
	COne-click generation						
*Allowed IP Address()	*Allowed IP Address() 192.168.70.0 / 24						
	192.168.80.0 / 24						
Endpoint Address 🕥	Endpoint Address () 192.168.5.143						
Endpoint Port()	Range 1~65535						
*Persistent Keepalive(Sec)①	25			Default 25, range 1~65535			
	Cancel Save						

WireGuard® – add/edit peer

Remote Clients

The **Remote Clients** tab displays a list of all connected WireGuard[®] clients. Each client connection is shown with relevant details such as:

- Name: The client's configured name.
- Enable: Toggle to enable or disable the connection for the client.
- WireGuard®: Displays the WireGuard® instance the client is connected to.
- Last Handshake: Shows when the last successful handshake with the client occurred.
- Actual Endpoint Address : Port: Displays the client's current IP address and port.

Operations include:

- View connection details.
- Download client configuration file or QR code.
- Edit or delete the client configuration

To view connected clients, navigate to **VPN** \rightarrow **WireGuard** $^{\textcircled{B}}$ \rightarrow **Remote Clients**.

ireGuard® 💾							
WireGuard® Peers	Remote Clients						
Delete				A	ll WireGuard® ~	Q Name	
Vame	Enable	WireGuard®	Last Handshake	Actual Endpoint Address :	Port Op	erations	Ξ
Peer1		Wireguard	15s ago	192.168.5.254:55645	4	u ev e ü	
					Total: 1		10 / page

WireGuard® – Remote Clients

The user can download the config file after adding the client.

Peer_peer2.c	onf	» 📔 🧾 All Bookmarks
230 B • Done		D 💽 admin 🗸
	\mathbf{i}	
. v All Wire	iuard®	Q
tual Endpoint dress : Port	Upload	Dowr Operations
2.168.5.52:5224	↑ 49.52KB	↓ 16 🛃 ເ 🗍
	† 0B	♦ 0E 🕁 🖫 🗹 🔟
2.168.5.127:550	🕇 113.7KB	♦64 ⊻ ఔ ८ Ш́
	† 0B	↓oe 🗹 🔟
	Total: 4	< 1 > 10 / page ∨

WireGuard® - download client config

Or scanning the QR code for devices with camera support.

			All Generat	ion \vee 🛛 All WireC	Guard® ~	۵
Gene Mode	QR Code	×	ndshake	Actual Endpoint Address : Port	Upload	Dowi Operations
Auto			30	192.168.5.52:5224 7	† 50.96KB	↓16 业 醌 亿 前
Auto					† 0B	↓0E 🕹 🕮 🗹 🔟
Auto			50	192.168.5.127:550 18	115.07KB	<mark></mark>
Add N					† 0B	↓ 0E 🗹 🔟
	Download QR code 🕁				Total: 4	< 1 > 10 / page
	Mode Auto Auto	Auto Auto Auto Auto Auto	Gene Model Auto Auto Auto	Gene QR Code × dtshake Auto Image: Code Image: Code Image: Code Auto Image: Code Image: Code Image: Code	Gen Mode QR Code × atshale Actual Endpoint Address : Port Auto Image: Code 0 192.168.552:5224 Auto Image: Code - Auto Image: Code 192.168.5127:550 Auto Image: Code 18 Add N Image: Code - Add N Image: Code 18	Gene Actual Endpoint Upload Auto Image: Constraint of the second

WireGuard[®] – scan client config

IPSec

IPSec or Internet Protocol Security is mainly used to authenticate and encrypt packets of data sent over the network layer. To accomplish this, they use two security protocols – ESP (Encapsulation Security Payload) and AH (Authentication Header), the former provides both authentications as well as encryption whereas the latter provides only authentication for the data packets. Since both authentication and encryption are equally desirable, most of the implementations use ESP.

IPSec supports two different encryption modes, they are Tunnel (default) and Transport mode. Tunnel mode is used to encrypt both payloads as well as the header of an IP packet, which is considered to be more secure. Transport mode is used to encrypt only the payload of an IP packet, which is generally used in gateway or host implementations.

IPSec also involves IKE (Internet Key Exchange) protocol which is used to set up the Security Associations (SA). A Security Association establishes a set of shared security parameters between two network entities to provide secure network layer communication. These security parameters may include the cryptographic algorithm and mode, traffic encryption key, and parameters for the network data to be sent over the connection. Currently, there are two IKE versions available – IKEv1 and IKEv2. IKE works in two phases:

Phase 1: ISAKMP operations will be performed after a secure channel is established between two network entities.

Phase 2: Security Associations will be negotiated between two network entities.

IKE operates in three modes for exchanging keying information and establishing security associations – Main, Aggressive and Quick mode.

• **Main mode:** is used to establish phase 1 during the key exchange. It uses three two-way exchanges between the initiator and the receiver. In the first exchange, algorithms and hashes are exchanged. In the second exchange, shared keys are generated using the Diffie-Hellman exchange. In the last exchange, verification of each other's identities takes place.

• **Aggressive mode**: provides the same service as the main mode, but it uses two exchanges instead of three. It does not provide identity protection, which makes it vulnerable to hackers. The main mode is more secure than this.

• **Quick mode**: After establishing a secure channel using either the main mode or aggressive mode, the quick mode can be used to negotiate general IPsec security services and generate newly keyed material. They are always encrypted under the secure channel and use the hash payload that is used to authenticate the rest of the packet.

IPSec Site-to-Site

To build an IPSec secure tunnel between two sites located in two distant geographical locations, we can use the sample scenario below:

The branch office router needs to connect to the Headquarters office via an IPSec tunnel, on each side we have a GWN700x router. Users can configure the two devices as follows:

The branch office router runs a LAN subnet 192.168.1.0/24 and the HQ router runs a LAN subnet 192.168.3.0, the public IP of the branch office router is 1.1.1.1 and the IP of the HQ router is 2.2.2.2.

Go under **VPN** \rightarrow **IPSec** \rightarrow **Site-to-Site** then click on + add to add a VPN Client.

Add VPN Client				
*Name 🛈	Branch Office			
Connection Type	IPSec v			
*Remote Server Address	3.3.3.3			
Interface 🛈	• WAN			
IKE Version	IKEv2 ~			
*IKE Lifetime (s) 🛈	28800			

Add VPN Client – IPSec

○ Phase 1

Phase 1 ^		
Negotiation Mode	Main Aggressive	
*Pre-shared Key①		1~64 characters
Encryption Algorithm	AES-256 ~	
Hash Algorithm	SHA2-256 ~	
DH Group	Group14 ~]
Local ID 🕕		
Remote ID 🛈		
Reconnect ①		
*Number of Reconnect①	10	The default value is 10, and the valid range is 0-10. Value 0 means that it has been
		trying to negotlate connection.
DPD ()		
*DPD Delay Time (sec)	30	Default 30, range 10~900
*DPD Idle Time (sec)	120	Default 120, range 10~900
DPD Action 🛈	● Hold Clear	



○ Phase 2

Phase 2 🔨				
*Local Subnet①	IP Address	/ Mask Length		
			Add	•
*Local Source IP Address 🛈				
*Remote Subnet①	IP Address	/ Mask Length		
			Add	Ð
*IPSec SA Lifetime (sec)	3600			Default 3600, range 600~ <u>86400</u>
Security Protocol	• ESP			
ESP Encryption Algorithm	AES-256		~	
ESP Hash Algorithm	SHA2-256		~	
Encapsulation Mode	 Tunnel Mode 			
PFS Group	Disabled		~	
	Cancel Save			

Add VPN Client – Phase 2

After this is done, press "Save" and do the same for the HQ Router. The two routers will build the tunnel and the necessary routing information to route traffic through the tunnel back and from the branch office to the HQ network.

Note:

After the connection is established, the incoming packets from the remote subnet are automatically released, and it is not necessary to manually configure the firewall forwarding rules from WAN to LAN to release traffic.

• Create the remote user credentials:

To creates the remote user account which will be required to be entered on the client side and authenticated on the server side, please refer to the **Remote Users** section.

IPSec Client-to-Site

Go under **VPN** \rightarrow **IPSec** \rightarrow **Client-to-Site** then fill in the following information:

IPSec > Add Client-to-Site			
*Name			1~64 characters
Status			
Interface	WAN2 (WAN)	Ý	
*Pre-shared Key		3 ₉₇₆ 6	1~64 characters, only support input English, numbers, characters @ ! \$ %
*Encryption Algorithm	3DES \times AES-128 \times AES-192 \times AES-256 \times	~	
*Hash Algorithm	MD5 \times SHA-1 \times SHA2-256 \times	~	
*DH Group	Group2 × Group5 × Group14 × Group19 × Group20 × Group21 ×	~	

Branch Office IPSec Configuration

OpenVPN®

OpenVPN® is a virtual private network solution that offers establishing a secure connection to a distant host, VPN provides the possibility to reach hosts which are located on local area network and be logically located in that same local area network, hence the name Virtual Private Network. The connection between the client and the server is authenticated using username and password or/and TLS encryption.

Typically, users can set a client-to-server connection, the client being a computer, and the server being a GWN router or a GCC device. The user can also set site-to-site VPN connection using OpenVPN® to interconnect two sites securely. In the following sections, you can find explanation for all the configuration fields for OpenVPN®.

OpenVPN® Client

There are two ways to use the GWN700x as an OpenVPN® client:

1. Upload client certificate created from an OpenVPN® server to GWN700x.

2. Create client/server certificates on GWN700x and upload the server certificate to the OpenVPN® server.

Go to Go to $VPN \rightarrow OpenVPN$ $\ \ \rightarrow OpenVPN$ Clients and follow the steps below:

Click on + Add button. The following window will pop up.

*Name			1~64 characters
Status			
Protocol	O UDP C TCP		
Interface	WAN2 (WAN)	~	
Destination	WAN2 (WAN)	~	
*Local Port ①	1194		Default 1194, range 1~ <u>65535</u>
*Remote OpenVPN® Server①			Enter an IPv4 address or domain name
*OpenVPN® Server Port①	1194		Default 1194, range 1~ <u>65535</u>
Authentication Mode	SSL	~	
Encryption Algorithm	AES-256-CBC	v	
Digest Algorithm	SHA256	v	
TLS Identity Authentication			
Routes	IP Address / Mask Length		
		Add	•
Deny Server Push Routes			
IP Masquerading			
LZO Compression ()	On Off Adaptive		
Allow Peer to Change IP 🛈			
*CA Certificates	Please Select CA Certificates	~	
*Client Certificate	Please Select Client Certificate	~	
Client Private Key Password		> _{ref}	0~64 characters
	Cancel Save		
	© 2023 Grandstream Networks, Inc. Grandstream Software License Agre	emer	¢

OpenVPN® Client

Click save after completing all the fields.

Name	Enter a name for the OpenVPN® Client.	
Status	Toggle on/off the client account.	
Protocol	Specify the transport protocol used. • UDP • TCP Note: The default protocol is UDP.	
Interface	Select the WAN port to be used by the OpenVPN® client.	
Destination	Select the WANs, VLANs and VPNs (clients) destinations that will be used by this OpenVPN® client.	
Local Port	Configures the client port for OpenVPN®. The port between the OpenVPN® client and the client or between the client and the server should not be the same.	
Remote OpenVPN® Server	Configures the remote OpenVPN® server. Both IP address and domain name are supported.	
OpenVPN® Server Port	Configures the remote OpenVPN® server port	
Authentication Mode	 Choose the authentication mode. SSL User Authentication SSL + User Authentication PSK 	

Encryption Algorithm	Choose the encryption algorithm. The encryption algorithms supported are: • DES • RC2-CBC • DES-EDE-CBC • DESX-CBC • DESX-CBC • BF-CBC • RC2-40-CBC • RC2-64-CBC • RC2-64-CBC • AES-128-CBC • AES-192-CBC • AES-256-CBC • SEED-CBC
Digest Algorithm	Select the digest algorithm. The digest algorithms supported are: • MD5 • RSA-MD5 • SHA1 • RSA-SHA1 • DSA-SHA1-old • DSA-SHA1-old • DSA-SHA1-2 • DSA • RIPEMD160 • RSA-RIPEMD160 • MD4 • RSA-MD4 • ecdsa-with-SHA1 • RSA-SHA256 • RSA-SHA384 • RSA-SHA384 • RSA-SHA512 • SHA224 • SHA224 • whirlpool
TLS Identity Authentication	Enable TLS identity authentication direction.
TLS Identity Authentication Direction	 Select the indentity authentication direction. Server: Indentity authentication is performed on the server side. Client: Identity authentication is performed on the client side. Both: Identity authentication is performed on both sides.
TLS Pre-Shared Key	Enter the TLS pre-shared key.
Routes	Configures IP address and subnet mask of routes, e.g., 10.10.1.0/24.
Deny Server Push Routes	If enabled, client will ignore routes pushed by the server.
IP Masquerading	This feature is a form of network address translation (NAT) which allows internal computers with no known address outside their network, to communicate to the outside. It allows one machine to act on behalf of other machines.
LZO Compression	Select whether to activate LZO compression or no, if set to "Adaptive", the server will make the decision whether this option will be enabled or no.

	LZO encoding provides a very high compression ratio with good performance. LZO encoding works especially well for CHAR and VARCHAR columns that store very long character strings.
Allow Peer to Change IP	Allow remote change the IP and/or Port, often applicable to the situation when the remote IP address changes frequently.
CA Certificates	Click on "Upload" and select the CA certificate Note: This can be generated in System Settings \rightarrow Certificates \rightarrow CA Certificate
Client Certificate	Click on "Upload" and select the Client Certificate. Note: This can be generated in System Settings \rightarrow Certificates \rightarrow Certificate
Client Private Key Password	Enter the client private key password. Note: This can be configured in VPN \rightarrow Remote User



OpenVPN® Server

To use the GWN700x as an OpenVPN® server, you will need to start creating an OpenVPN® certificates and remote users.

To create a new VPN server, navigating under **Web UI** → **VPN** → **OpenVPN® page** → **OpenVPN® Servers tab.**

OpenVPN® > Add OpenVPN® S	erver			
*Name				1~64 characters
Status				
Protocol	• UDP O TCP			
Interface	WAN1 (WAN)		~	
Destination	WAN1 (WAN)		~	
*Local Port①	1194			Default 1194, range 1~ <u>65535</u>
Server Mode ()	SSL		~	
Encryption Algorithm	AES-256-CBC		~	
Digest Algorithm	SHA256		~	
TLS Identity Authentication				
Allow Duplicate Client Certificates ①				
Redirect Gateway				
Push Routes ①	IP Address	/ Mask Length	1	
			Add	i 🔁
LZO Compression	● On 🔷 Off 🔿	Adaptive		
	Cancel Save			

Create OpenVPN® Server

Click **Save** after completing all the fields.

Refer to the table below:

Name	Enter a name for the OpenVPN® server.			
Status	Toggle ON or OFF to enable or disable the OpenVPN® Server.			
Protocol	Choose the Transport protocol from the dropdown list, either TCP or UDP. <i>The default protocol is UDP</i> .			
Interface	Select from the drop-down list the exact interface (WAN).			
Destination	Select from the drop-down list the destination (WAN or VLAN).			

Local Port	Configure the listening port for OpenVPN® server. The default value is 1194.			
Server Mode	 Choose the server mode the OpenVPN® server will operate with. 4 modes are available: SSL: Authentication is made using certificates only (no user/pass authentication). Each user has a unique client configuration that includes their personal certificate and key. This is useful if clients should not be prompted to enter a username and password, but it is less secure as it relies only on something the user has (TLS key and certificate). User Authentication: Authentication is made using only CA, user and password, no certificates. Useful if the clients should not have individual certificates. Less secure as it relies on a shared TLS key plus only something the user knows (Username/password). SSL + User Authentication: Requires both certificate and username / password. Each user has a unique client configuration that includes their personal certificate and key. PSK: Used to establish a point-to-point OpenVPN® configuration. A VPN tunnel will be created with a server endpoint of a specified IP and a client endpoint of specified IP. Encrypted communication between client and server will occur over UDP port 1194, the default OpenVPN® port. Most secure as there are multiple factors of authentication (TLS Key and Certificate that the user has, and the username/password they know). 			
Encryption Algorithm	Choose the encryption algorithm from the dropdown list to encrypt data so that the receiver can decrypt it using same algorithm.			
Digest Algorithm	Choose digest algorithm from the dropdown list, which will uniquely identify the data to provide data integrity and ensure that the receiver has an unmodified data from the one sent by the original host.			
TLS Identicy Authentication	This option uses a static Pre-Shared Key (PSK) that must be generated in advance and shared among all peers. This feature adds extra protection to the TLS channel by requiring that incoming packets have a valid signature generated using the PSK key.			
TLS Identity Authentication Direction	Select from the drop-down list the direction of TLS Identity Authentication, three options are available (Server, Client or Both) .			
TLS Pre-Shared Key	If TLS Identicy Authentication is enabled, enter the TLS Pre-Shared Key.			
Allow Duplicate Client Certificates	Click on " ON " to allow duplicate Client Certificates			
Redirect Gateway	When redirect-gateway is used, OpenVPN® clients will route DNS queries through the VPN, and the VPN server will need to handle them.			
Push Routes	Specify route(s) to be pushed to all clients. Example: 10.0.0.1/8			
LZO Compression Algorithm	Select whether to activate LZO compression or no, if set to "Adaptive", the server will make the decision whether this option will be enabled or no.			
Allow Peer to Change IP	Allow remote change the IP and/or Port, often applicable to the situation when the remote IP address changes frequently.			
CA Certificate	Select a generated CA from the dropdown list or add one.			
Server Certificate	Select a generated Server Certificate from the dropdown list or add one.			
IPv4 Tunnel Network/Mask Length	Enter the network range that the GWN70xx will be serving from to the OpenVPN® client. <i>Note: The network format should be the following 10.0.10.0/16.</i>			

• Create the remote user credentials:

To creates the remote user account which will be required to be entered on the client side and authenticated on the server side, please refer to the **Remote Users** section.

PPTP

A data-link layer protocol for wide area networks (WANs) based on the Point-to-Point Protocol (PPP) and developed by Microsoft enables network traffic to be encapsulated and routed over an unsecured public network such as the Internet. Point-to-Point Tunneling Protocol (PPTP) allows the creation of virtual private networks (VPNs), which tunnel TCP/IP traffic through the Internet.

PPTP Clients

To configure the PPTP client on the GWN700x, navigate under **VPN** \rightarrow **PPTP** \rightarrow **PPTP** Clients and set the followings:

1. Click on "**Add**" button.

РРТР								
PPTP Clients PPT	P Servers							
Add Delet							All Interfaces \lor	Q. Search Name
Name	Status	Connection Status	Interface	Server Address	Duration	Upload	Download	Current Operations
PPTP_Client1		Disconnected	WAN1 (WAN)	192.168.5.143	0s	† 0B	↓ 0B	TX:0bps RX:0bps 🖾 🔟
							Total: 1	< 1 > 10/page

PPTP page

The following window will pop up.

PPTP > Edit PPTP Client			
*Name	PPTP_Client1		1~64 characters
Status			
*Server Address	192.168.5.143		Enter an IPv4 address or domain nam
* Username	user1		1~64 characters
* Password		میرد ا	1~64 characters
MPPE Encryption	Once enabled. PPTP Acceleration w	ill not take effect	
Interface	WAN1 (WAN)		
Destination ③	All ×	5	
IP Masquerading			
* Maximum Transmission Unit	1430		Default 1430, range 576~1450
(MTU)			
(MTU)	192.168.70.0	/ 24	•
	192.168.70.0		e id e

PPTP Client Configuration

Name	Enter a name for the PPTP client.
Status	Toggle on/off the VPN client account.
Server Address	Enter the IP/Domain of the remote PPTP Server.

Username	Enter the Username for authentication with the VPN Server.
Password	Enter the Password for authentication with the VPN Server.
MPPE Encryption	Enable / disable the MPPE for data encryption. By default, it's disabled.
Interface	Choose the interfaces. Note: Set forwarding rules in firewall automatically to allow traffic forwarded from VPN to the selected WAN port. If remote device is allowed to access, please set the corresponding forwarding rules in firewall.
Destination	Choose to which destination group or WAN to allow traffic from the VPN, this will generate automatically a forwarding rule under the menu Firewall \rightarrow Traffic Rules \rightarrow Forward .
IP Masquerading	This feature is a form of network address translation (NAT) which allows internal computers with no known address outside their network, to communicate to the outside. It allows one machine to act on behalf of other machines.
Maximum Transmission Unit (MTU)	This indicates the size of the packets sent by the router. Please do not change this value unless necessary.
Remote Subnet	Configures the remote subnet for the VPN. The format should be "IP/Mask" where IP could be either IPv4 or IPv6 and mask is a number between 1 and 32. <i>example:</i> 192.168.5.0/24

PPTP Client Configuration

PPTP Servers

To add a PPTP Server, please navigate to Web UI \rightarrow VPN \rightarrow PPTP page \rightarrow PPTP Servers tab, then click on "Add" button.

PPTP > Edit PPTP Server			
	*Name	PPTPServer	1~64 characters
	Status		
	*Server Local Address	192.168.5.143	
	Client Start Address	192.168.5.2	
	* Client End Address	192.168.5.9	
	MPPE Encryption	Once enabled, PPTP Acceleration will not take effect	
	* Interface	WAN2 (WAN)	
	*Destination ①	All ×	
	LCP Echo Interval (sec) ①	20	Range 1-86400
	LCP Echo Failure Threshold ()	3	Range 1~86400
	LCP Echo Adaptive ①		
	Debug		
	* Maximum Transmission Unit (MTU)①	1430	Default 1430, range 1280~1500
	^Maximum Receive Unit (MRU)③	1430	Default 1430, range 1280~1500
		Cancel Save	

Name	Enter a name for the PPTP Server.
Status	Toggle ON or OFF to enable or disable the PPTP Server VPN.
Server Local Address	Specify the server local address

Client Start Address	specify client start IP address
Client End Address	specify client end IP address
MPPE Encryption	Enable / disable the MPPE for data encryption. By default, it's disabled.
Interface	Select from the drop-down list the exact interface (WAN port).
Destination	Select the Destination from the drop-down list (WAN or VLAN). <i>Note: When selecting "All", subsequent new interfaces will be automatically included.</i>
LCP Echo Interval (sec)	Configures the LCP echo send interval.
LCP Echo Failure Threshold	Set the maximum number of Echo transfers. If it is not answered within the set request frames, the PPTP server will consider that the peer is disconnected and the connection will be terminated.
LCP Echo Adaptive	 Once enabled: LCP Echo request frames will only be sent if no traffic has been received since the last LCP Echo request. Once disabled: the traffic will not be checked, and LCP Echoes are sent based on the value of the LCP echo interval
Debug	Toggle On/Off to enable or disable debug.
Maximum Transmission Unit (MTU)	This indicates the size of the packets sent by the router. Please do not change this value unless necessary. By default is 1450.
Maximum Receive Unit (MRU)	MRU indicates the size of the received packets. By default is 1450.
Preferred DNS Server	specify the preferred DNS server. Ex: 8.8.8.8
Alternative DNS Server	specify the alternative DNS server. Ex: 1.1.1.1

PPTP Sever

• Create the remote user credentials:

To creates the remote user account which will be required to be entered on the client side and authenticated on the server side, please refer to the **Remote Users** section.

To view the clients connected to this server, click on "Client List" icon as shown below:

РРТР									
PPIP									
PPTF	Clients PPTP Ser	vers							
A	id Delete								
	Name	Status	Interface	PPTP Server Address	Uptime	Upload	Download	Current Rate	Operations
	PPTPServer		WAN2 (WAN)	192.168.5.143	1min	🛉 12.41KB	↓ 207B	TX:1.83Kbps RX:80bps	r c
				Clients Connected To	This Server	×	/		
			IP Address	Uptime	Username				
			192.168.5.127	1min	user				
					Total: 1 <	1 >			

Clients connected to this server

L2TP

To configure the L2TP client on the GWN700x router, navigate under "**VPN** \rightarrow **VPN Clients**" and set the followings:

1. Click on + Add button and the following window will pop up.

*Name	L2TP Connection		1~64 characters			
Status						
Interface	WAN2 (WAN)					
Destination	WAN2 (WAN)	WAN2 (WAN)				
*Server Address	testvpnl2tp.vpnazure.net	Enter an IPv4 address or domain name				
*Username	vpn_user		1~64 characters			
*Password		748	1~64 characters			
IP Masquerading						
*Maximum Transmission Unit (MTU)	1430		Default 1430, range 576~1460			
Remote Subnet 🗊	IP Address / Mask Length					
		Add	i 🔁			
	Cancel Save					

L2TP Client Configuration

Name	Set a name for this VPN tunnel.
Status	Toggle on/off this L2TP account.
Interface	Select the WAN port to be used by VPN.
Destination	Select the WANs, VLANs destinations that will be using this VPN.
Server Address	Enter the VPN IP address or FQDN.
Username	Enter VPN username that has been configured on the server side.
Password	Enter VPN password that has been configured on the server side.
IP Masquerading	This feature is a form of network address translation (NAT) which allows internal computers with no known address outside their network, to communicate to the outside. It allows one machine to act on behalf of other machines.
Maximum Transmission Unit (MTU)	This indicates the size of the packets sent by the router. Please do not change this value unless necessary.
Remote Subnet	Enter the remote Subnet that has been configured on the server side.

L2TP Client Configuration

Click save after completing all the fields.

+ Add					
Name	Status	Connection Type	Interface	Server Address	Operations
L2TP	Dailing	L2TP	WAN	testvpnl2tp.vpnazure.net	😣 🗡 Ū

Remote Users

To create the VPN user accounts, please navigate to **VPN** \rightarrow **Remote Users** then click "**Add**". The account configured will be used for the client to authenticate into the VPN server. The remote client user that can be created in this section is for PPTP, IPSec, and OpenVPN.

Ac	ld Delete					All Servers	This is just an ovpn file template,
							please modify it for your specific
-	Name	Enable	Server Type	Server Name	Client Subnet	IP Addr	needs.
~	OpenVPN® re		OpenVPN®	OpenVPN®_Ser	-		区回
	OpenVPN® Re		OpenVPN®	GXV3370			比尼茴

VPN Remote Users page

If the remote user is using OpenVPN®, the configuration file can be exported as an .ovpn file. This file can then be modified as needed to fit the user's requirements.

Remote Users > Add User		
*Name		1~64 characters
Status		
Server Type	PPTP IPSec OpenVPN®	
Server Name	Please Select Server Name 🗸	
*Username		1~64 characters, only support input English, numbers, characters @ ! \$ %
*Password	- Jyd	1~64 characters, only support input English, numbers, characters @ ! \$ %
Client Subnet	IP Address / Mask Length	
	Ado	•
	Cancel Save	

Add VPN Remote Users

Name	Enter a name for the user. This name will not be used to log in.
Status	Enable or disable this account.
	Choose the type of the server.
Server Type	 PPTP IPSec OpenVPN
Server Name	Enter the server's name.
Username	Enter the username. This username will be used to log in.
Password	Enter the password.
Client Subnet	Specify the client subnet.

Add VPN Remote Users

To authenticate a remote user into the VPN server successfully, the username and password are used alongside the client certificate. To create a client certificate please refer to Certificates section.

To configure the VPN clients for each VPN server type, please refer to the respective VPN client configuration above.

ROUTING

Routing Table

The **Routing Table** page displays the routes currently configured on your Grandstream device. It shows key information such as the IP address, protocol type, outgoing interface, next hop, and administrative distance for each route.

You can toggle between **IPv4 Routing Table** and **IPv6 Routing Table** using the tabs at the top of the page. Additionally, you can filter routes based on outgoing interfaces or search for a specific next hop.

- IP Address: The destination network or IP address.
- Protocol Type: Indicates the type of routing (e.g., Direct, Static, VPN).
- Outgoing Interface: The network interface used for routing traffic to the destination.
- **Next Hop**: The IP address of the next device in the routing path.
- Administrative Distance: The trustworthiness of the route.

To view the routing table, navigate to **Routing** \rightarrow **Routing Table**.

Pv4 Routing Table IP	v6 Routing Table			
Refresh			All Outgoing Interfa	a v Q Next Hop
P Address	Protocol Type	Outgoing Interface	Next Hop	Administrative Distance
.0.0.0/0		WAN1(WAN)	192.168.6.1	0
0.0.0/24	Direct	2(VLAN)	0.0.0.0	0
72.23.250.0/24	-	Tunnel(VPN)	172.23.250.2	0
72.23.250.2/32	Direct	Tunnel(VPN)	0.0.0.0	0
92.168.6.0/24		WAN1(WAN)	0.0.0.0	0
92.168.6.0/24	Direct	WAN1(WAN)	0.0.0.0	0
92.168.80.0/24	Direct	Default(VLAN)	0.0.0.0	0

Routing Table

Policy Routes

The Policy Routes feature on the GWN700X series allows network administrators to create advanced routing rules to efficiently manage traffic across multiple WAN interfaces. This feature supports three modes: **Load Balancing**, **Backup**, and **Standby**. Each mode serves a unique purpose to enhance network performance, ensure uninterrupted connectivity, and provide granular control over traffic distribution. These policies can be applied to specific VLANs for tailored traffic management.

Note:

It is also possible to implement load balancing, backup, and standby between WAN and VPN interfaces.

Policy Pool

To create a policy pool rule, follow these steps:

- 1. Navigate to **Routing** \rightarrow **Policy Routes** in the web interface.
- 2. Open the Policy Pool tab.
- 3. Click the Add button to create a new rule.
- 4. Select the desired mode:
 - Load Balance
 - Backup
 - Standby

5. Assign the Preferred Interface(s) and configure their Weight values (1-10).

Note:

For the Weight: The default is 1 and value can be from 1~10 with 10 being the highest weight.

6. (Optional) Assign Alternate Interface(s) for Backup mode or Standby Interface for Standby mode.

Note:

The number of WAN ports depends on GWN router model.

7. Save the configuration.

Key Details:

- You can configure these routes with either WAN or VPN interfaces.
- Once created, a policy pool can be applied to specific VLANs, enabling precise traffic management per VLAN.

Policy Routes					
Policy Pool Policy Routes					
Add Delete				All Interfaces ~	Q Name
Name	Mode	Interfaces	Interface	Weight	Operations
 Standby 	Standby	2	WAN3 (WAN) Preferred	1	
🔽 🗠 Backup	Backup	2	WAN1 (WAN) Preferred	1	ľ
✓ Load Balancing	Load Balance	2	WAN1 (WAN)	1	ľŌ
✓ Default	Load Balance	2	WAN1 (WAN)	1	

Policy Pool page

Load Balance Mode

- **Purpose**: Distribute traffic evenly or proportionally across multiple WAN interfaces based on bandwidth capacity or network requirements.
- How It Works:
 - Configure weights for each WAN interface. For instance, if two WAN ports have weights of 1 and 2, traffic will be divided in a **1:2 ratio**. Similarly, setting weights to 1 and 1 will evenly distribute traffic in a **1:1 ratio** across both WAN interfaces.
 - Suitable for scenarios where bandwidth optimization and redundancy are required.

• Advantages:

- Efficiently uses all available bandwidth.
- Provides redundancy across multiple WAN connections.

Example 1: If you have WAN1 (100 Mbps) and WAN2 (50 Mbps), set weights as 2 and 1, respectively, to ensure balanced utilization proportional to bandwidth.

*Name	Load Balancing Policy		1~64 characte
Mode	Load Balance		\sim
*Interface	Interface	Weight ①	
	WAN1 (WAN)	2	•
	WAN2 (WAN)	~ 1	•

Load Balance mode – Example 1

Example 2: If you have WAN1 (100 Mbps) and WAN2 (100 Mbps), set their weights to 1 and 1, respectively, to ensure balanced utilization proportional to their bandwidth. In this configuration, the bandwidth will be evenly distributed between the two connections.

* Name	Load Balance Rule		1~64 characters
Mode	• Load Balance	Backup	
*Interface	Interface	Weight 🛈	
	WAN1 (WAN)	~ 1	•
	WAN2 (WAN)	~ 1	•
			Add 🕕
	Cancel	re	

Backup Mode

- Purpose: Provide failover support by routing traffic to alternate interfaces when all preferred WAN interfaces fails.
- How It Works:
 - In backup mode, the backup interfaces remain active and ready to handle traffic if a failure is detected **on all** preferred interfaces. However, the alternate interfaces only become active when all preferred interfaces are down.
 Once activated, traffic is distributed across the alternate interfaces based on their assigned weights.
 - The status of the interfaces is monitored using ICMP replies to a tracking IP, which determines when the interface is up or down. For more details, refer to the WAN section. If the preferred interfaces come back online, traffic will revert to the primary interface after five consecutive tracking intervals (typically 60 seconds).

• Key Features:

- Backup interfaces are always active.
- Traffic can be distributed proportionally between preferred and backup interfaces if weights are configured.

Example:

If both the preferred interfaces, **WAN1 and VPN**, are down, only then will the alternate interfaces, **WAN2 and WAN4**, become active, with traffic distributed according to their assigned weights.

Mada	Paskup				
Mode ()	Backup			\sim	
*Preferred Interface	Interface		Weight 🕕		
	WAN1 (WAN)	~	1		•
	VPN (VPN)	~	1		•
				Add	Ð
*Alternate Interface①	Interface		Weight 🛈		
	WAN2 (WAN)	~	1		•
	WAN4 (WAN)	Ý	1		•
				Add	Ð

Standby Mode

• **Purpose**: maintain a **single standby interface**, which is only activated when **all the primary interfaces fail**. This is especially useful in cases like PPPoE authentication conflicts, where multiple active sessions can cause issues.

• How It Works:

- The standby interface remains inactive until all preferred (primary) interfaces fail. A Tracking IP Address (such as 1.1.1.1 or 8.8.8.8) is configured to monitor the status of the primary interface. The router pings this IP to check if the primary interface is up or down. If the pings fail continuously, the router switches to the standby interface.
- For PPPoE, authentication occurs only when the standby interface is activated, preventing simultaneous session conflicts.
- Failback occurs when the primary interface recovers, after five consecutive successful tracking intervals (typically 60 seconds) where the router pings a configured Tracking IP Address to check if the interface is back online. For PPPoE, failback may take up to 400 seconds due to session lock delays and the time required for PPPoE authentication to complete.

• Key Features:

- Standby interface remains inactive to conserve resources, activating only when needed.
- Resolves PPPoE authentication conflicts when the same account is configured across multiple WAN ports.
- Ensures smooth failback after the primary interface recovers, with an extended failback period for PPPoE sessions.

Example:

Use Standby Mode when two WAN ports require PPPoE with the same ISP credentials to prevent conflicts and maintain redundancy. For instance, WAN2 will store the PPPoE credentials but remain inactive. If WAN1, using the same credentials, fails or goes offline for any reason, WAN2 will automatically authenticate with the saved credentials and activate, ensuring seamless connectivity.

Mode 🛈	Standby		~
*Preferred Interface	Interface	Weight ()	
	WAN1 (WAN)	✓ 1	•
* Standby Interface	WAN2 (WAN)		~
	interfaces fail.	will only take effect when all the	
	Cancel Save		
	Policy Pool – Stan	ndhv mode	

WAN Name	Enable	Port	Connection Type	IPv4 Address	IPv4 Status	VPN Connection Type	VPN IP Address	Operations	=
WAN1		Port 3 (GE)	IPv4: PPPoE IPv6: -	103.45.67.89	Connected		-	() L 🗇	
WAN2		Port 4 (GE)	IPv4: PPPoE IPv6: -		Disconnected	-		ßò	

Comparison Table

Feature/Mode	Load Balancing	Backup Mode	Standby Mode
Purpose	Distribute traffic across multiple interfaces.	Failover with active backup .	Failover with inactive standby.

Feature/Mode	Load Balancing	Backup Mode	Standby Mode
Traffic Behavior	Balanced based on weights (Ratio).	When all preferred interfaces fail or become unavailable, the alternate interfaces will automatically take over. Traffic will be distributed proportionally between the alternate interfaces based on their configured weights, ensuring seamless failover	Activate the standby interface only when all preferred interfaces have failed.
Resource Usage	Utilizes all interfaces actively.	Backup interfaces are always active, and more than one interface can be configured as a backup.	The standby interface remains inactive, and only one interface can be designated as standby.

Policy Routes Modes Comparison

Policy Route

On the second tab (Policy Routes), the user can specify which Networks (VLAN) can use which Load Balance rule (must be created first), also the user can specify the protocol type, source and destination IP and even assign a schedule for it.

To create a Policy Route, please navigate to **Routing** \rightarrow **Policy Routes page** \rightarrow **Policy Routes tab**, then click on "**Add**" button to click on "**edit icon**" to edit as shown below:

olicy Route	s								
Policy Pool	Policy Routes								
Add	Delete Mov	re to Top						Q Name	/ Policy Name
- No.	Name	Enable	IP Family	Protocol Type	Source Group	Source Address	Source Port	Destination Addr.	Operations
✓ 1	Load balancin		IPv4	All	All				‡ Ľ Ō
2	Standy policy		IPv4	All	All		-		≐ Ľ ⊡
3	Default		IPv4	All	All	-	-		

Policy Routes page

Note:

When creating multiple policy routes, the order from top to bottom determines priority. Rules with lower numbers (No.) have higher priority. Users can also move a rule to the top by selecting it and clicking the 'Move to Top' button, giving it the highest priority within the list.

Policy Routes > Add Policy Route		
*Name	Load Balancing Policy	1~64 characters
Enable		
IP Family	IPv4	
Protocol Type	All	
Source Address Type	IP Address ~	
Source Address		
Source Group 🛈	Default (VLAN)	
Destination Address Type	IP Address ~	
Destination Address		
* Policy	Standby	
Schedule	None ~	
When a fault occurs, match the next one in sequence ()		
	Cancel Save	

Add Policy Route

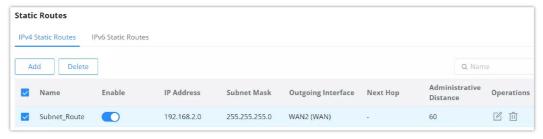
If the Source and Destination IP address field left empty, the policy route will take any IP address.

Static Routes

Static routing allows administrators to manually define routing paths instead of relying on dynamic routing protocols. This method is ideal for services requiring a consistent, unchanging route.

The **GWN700x** supports manual configuration of both IPv4 and IPv6 static routes, accessible through the Web GUI by navigating to **Routing** \rightarrow **Static Routes**.

To add a new static route, click on the **Add** button and complete the necessary fields as described.



c Routes > Edit IPv4 Static Route		
*Name	Subnet_Route	1~64 characters
Enable		
*IP Address	192.168.2.0	
* Subnet Mask	255.255.255.0	
*Outgoing Interface()	WAN2(WAN)	1
Next Hop	WAN1(WAN)	
	WAN2(WAN)	
*Administrative Distance()	Default(VLAN)	The default is 60, with a range of 1-255. is the highest priority.
	Blackhole	is the rightest priority.
	Cancel Save	

Static Routing Page

Add IPv4 Static Routing

Name	Assign a name for the route, such as 'Subnet_Route'.
Enable	Toggle this on to activate the route.
IP Address	Enter the destination network, e.g., 192.168.2.0.
Subnet Mask	Specify the subnet mask, e.g., 255.255.255.0.
Outgoing Interface	Select the interface the router should use for this route. For example, WAN1 for internet-bound traffic, or Blackhole to discard traffic to this destination.
Next Hop	Enter the IP address of the next router in the path to the destination network, if required.
Administrative Distance	Set a priority level for this route. Lower values indicate higher priority (default is 60). Use a lower value if you want this route to take precedence.

Open Shortest Path First (OSPF)

Open Shortest Path First (OSPF) is a dynamic routing protocol used in IP networks to determine the best path for data packets across the network. In Grandstream GWN routers, OSPF allows for efficient routing across large and complex networks by exchanging routing information between routers, ensuring each router knows the most optimal path to various network destinations.

The GWN routers support a robust OSPF configuration to provide flexibility, security, and scalability for enterprise-level networks. OSPF is designed to work within an Autonomous System (AS), ensuring fast convergence and optimal routing decisions based on link state information.

To view or configure OSPF settings, navigate to **Routing** \rightarrow **OSPF.**

Global Settings

The **Global Settings** tab contains important configurations to enable and fine-tune OSPF on your Grandstream GWN router. Some of the key options on this page include:

- **Router ID**: This field defines a unique IPv4 address that identifies your router within the OSPF network. It must be set for the router to participate in OSPF.
- **Always Advertise Default Route**: This toggle ensures that the router always advertises the default route (0.0.0.0/0) to other routers in the OSPF network, designating it as a gateway.
- **Metric**: The metric determines the cost of a route in OSPF. Lower values indicate a more preferred route, guiding the OSPF protocol in route selection.
- Metric Type: You can choose between:
 - **Type 1**: Considers both the OSPF metric and other route costs.
 - Type 2: Considers only the OSPF metric, typically used for external routes.
- External Route Import: This section allows you to import routes from other routing protocols such as Direct, Static, RIP, and BGP, giving you flexibility when integrating with different network setups.

OSPF					
Global Settings	Interface Settings	Area Settings	Neighbor Info		
		0	SPF		
		* R	outer ID	1.1.1.1	IPv4 Format
		A	lways Advertise Default Route		
		* M	letric	1	Default 1, range 1~16777214
		• M	letric Type	О Туре 1 💿 Туре 2	
		E	xternal Route Import		
		P	rotocol Type	🗹 Direct 🗹 Static 🔽 RIP 🔽 BGP	
				Please go to Firewall — Rule Policy/Traffic Rules to set the acceptance rules for the WAN port.	
		* D	irect Route Metric	1	Default 1, range 0~16777214
		* M	etric Type of Direct Route	○ Type 1 ● Type 2	
		* SI	tatic Route Metric	1	Default 1, range 0~16777214
		* M	letric Type of Static Route	 Туре 1 (9) Туре 2 	
		* R	IP Route Metric	1	Default 1, range 0-16777214
		• M	letric Type of RIP Route	О Туре 1 💿 Туре 2	
		* B	GP Route Metric	1	Default 1, range 0~16777214
		* M	letric Type of BGP Route	О Туре 1 💿 Туре 2	
				Cancel Save	
			OSPF – Glo	bal Settings	

Interface Settings

In this section, users can view, add, or modify OSPF configurations for each interface on the device. The interface settings allow fine-tuning of OSPF behavior by defining key parameters like intervals for OSPF hello packets, authentication types, and the cost metric for each interface.

To navigate: Routing -> OSPF -> Interface Settings

OSPF										
Globa	al Settings Interf	ace Settings	Area Settings Ne	ghbor Info						
Ad	ld Delete									
	Name	Enable	Interface	Area ID	Hello Interval (Sec)	Dead Interval (Sec)	Cost	Priority	Authentication Type	Operations
	interface vlan2		2	0.0.00	10	40	10	1	Off	CÓ (
									Total: 1 <	1 > 107 page >

OSPF – Interface Settings page

To add a new OSPF interface, they can click on the **Add** button. To edit an existing interface, click on the **Edit** icon next to the interface. Refer to the images for a visual guide.

OSPF > Edit Interface		
* Name	interface vlan2	1~64 characters
Enable		
* Interface	2(VLAN)	
* Area ID 🛈	0.0.0.0 ~	
* Hello Interval (Sec) 🛈	10	Default 10, range 1~65535
* Dead Interval (Sec) 🛈	40	Default 40, range 1~65535
*Cost()	10	Default 10, range 1~65535
* Priority 🛈	1	Default 1, range 0~255
Authentication Type ①	● Off ◯ Simple ◯ MD5	
	Cancel Save	

OSPF – Add/Edit Interface Settings

Key Configurations:

- Name: A customizable label for the interface.
- Enable: Toggle to enable or disable OSPF for this interface.
- Interface: Select the specific interface (e.g., VLAN) where OSPF should run.
- Area ID: Identifies the OSPF area the interface belongs to (default: 0.0.0.0 for backbone).
- Hello Interval (Sec): The interval between OSPF Hello packets to maintain neighbor relationships (default: 10 seconds).
- **Dead Interval (Sec)**: The interval after which a neighbor is considered down if no Hello packet is received (default: 40 seconds).
- Cost: Determines the OSPF route cost; lower values are preferred.
- Priority: Controls the interface's eligibility to become the Designated Router (DR).
- Authentication Type: Choose between No Authentication, Simple Password, or MD5 Authentication for OSPF packets.

These configurations help ensure optimal routing behavior and secure communication between OSPF-enabled devices.

Area Settings

The OSPF **Area Settings** tab allows users to configure OSPF areas to optimize routing and control traffic within different network zones. This section is essential for network segmentation and ensuring efficient routing within the Open Shortest Path First (OSPF) protocol in Grandstream GWN routers. OSPF divides networks into multiple areas to decrease routing overhead and enhance scalability.

To navigate to this page, go to **Routing** \rightarrow **OSPF** \rightarrow **Area Settings**.

To Add or Edit an Area:

- Click the Add button to create a new area.
- · Click the Edit icon next to an existing area to modify its configuration.

DSPF					
Global Settings Inte	erface Settings Area Sett	ings Neighbor Info			
Add Delete]				
< Area ID	Area Туре	No Summary	Conversion Type	Operations	
☑ 1.1.1.1	None	-	-	C Ū	
0.0.0.0	None	-	-		
			Total: 2	(1 > 10/pa	age \vee

OSPF – Area Settings page

Key Configurations in Area Settings:

- Area ID: A unique identifier for the OSPF area, defined in IPv4 format or an integer.
- Area Type: Options include:
 - None: No special designation for the area.
 - Stub: Restricts external route advertisements to minimize routing overhead.
 - NSSA (Not-So-Stubby Area): Balances between a stub and full OSPF area by allowing specific external routes.
- No Summary: Prevents summarized routes from being sent into the area, promoting more specific routing information.
- **Conversion Type**: Manages area type conversions:
 - Never: Disables conversion.
 - Always: Enables automatic conversion.

OSPF > Edit Area ID		
*Area ID	1.1.1.1	IPv4 format or an integer ranging from 1 to 4294967295
Area Type	None Stub NSSA	
No Summary 🛈		
Conversion Type	Never Always	
	Cancel Save	

OSPF – Add/Edit Area Settings

Neighbor Info

The **Neighbor Info** tab provides a summary of neighboring OSPF routers that have formed adjacencies with your Grandstream GWN router. This feature helps monitor OSPF neighbor relationships and troubleshoot connectivity between routers in a network running OSPF.

To view this information, navigate to **Routing** \rightarrow **OSPF** \rightarrow **Neighbor Info**.

Key Parameters Displayed in Neighbor Info

- Neighbor ID: The unique identifier of the neighboring router.
- **Priority**: Indicates the priority value of the neighbor, which helps in determining the designated router (DR) and backup designated router (BDR).
- Status: Shows the current state of the OSPF neighbor (e.g., Full, Init, 2-Way).
- Dead Time: The countdown before the neighbor is considered down, based on the Hello interval.
- Neighbor Address: The IP address of the neighbor.
- Interface: The interface on your router that is communicating with the neighbor.

• **Uptime**: The amount of time the OSPF neighbor relationship has been established.

This tab helps monitor OSPF relationships in real-time and identify potential routing issues.

OSPF						
USFF						
Global Settings	Interface Settings	Area Settings	Neighbor Info			
Refresh						
Neighbor ID	Priority	Status	Dead Time	Neighbor Address	Interface	Uptime
			2100			
			1			
			No data			

OSPF – Neighbor Info

RIP

Routing Information Protocol (RIP) is a distance-vector routing protocol used by routers to exchange routing information within a local network or across networks. In Grandstream GWN routers, RIP allows the configuration of both RIP Version 1 (RIPv1) and RIP Version 2 (RIPv2) to determine how routers communicate route information, maintain updated routing tables, and ensure efficient network management.

The RIP section is divided into four main tabs:

- 1. Global Settings
- 2. Interface Settings
- 3. Route Advertisement
- 4. Neighbor Info

Each tab provides specific configurations for setting up and managing RIP routing on your network.

RIP – Global Settings

The **Global Settings** tab is where the general RIP configuration is defined. You can enable RIP, choose the RIP version, and configure important parameters such as RIP Distance, Timers, and External Route Import options.

To navigate to this section: Go to **Routing** \rightarrow **RIP** \rightarrow **Global Settings**.

- **RIP**: Toggle to enable or disable RIP on the router.
- RIP Version:
 - **RIPv1**: Basic, classful routing protocol, no subnet information.
 - RIPv2: Classless routing protocol with subnet and route tags support.
- RIP Distance: Specifies the administrative distance for RIP routes, which helps in determining the reliability of the route (default is 120).
- Always Advertise Default Route: When enabled, the router will always advertise a default route to other routers.

Timer Configuration:

- Update Timer: The interval (in seconds) between route update messages.
- Invalid Timer: The duration (in seconds) after which a route is considered invalid if no update has been received.
- Garbage Collection Timer: The time after which an invalid route is removed from the routing table.

External Route Import:

You can configure the router to import external routes from the following sources:

• Direct Routes

- Static Routes
- OSPF Routes
- BGP Routes

For each protocol type, you can configure the metric values that affect the priority of the route.

RIP			
Global Settings Inte	erface Settings Route Advertisement Neighbor Info		
	RIP		
	RIP Version ()	⊖ RIPv1	
	* RIP Distance	120	Default 120, range 1~255
	Always Advertise Default Route		
	Timer		
	* Update Timer (Sec) ③	30	Default 30, range 5-2147483647
	* Invalid Timer (Sec) 🛈	180	Default 180, range 5-2147483647
	* Garbage Collection Timer (Sec)	120	Default 120, range 5~2147483647
	External Route Import		
	Protocol Type	🗹 Direct 🗹 Static 🔍 OSPF 🔽 BGP	
		Please go to Firewall — Rule Policy/Traffic Rules to set the acceptance rules for the WAN port.	
	* Direct Route Metric	1	Default 1, range 0~15
	* Static Route Metric	1	Default 1, range 0~15
	* OSPF Route Metric	1	Default 1, range 0~15
	* BGP Route Metric	1	Default 1, range 0~15
		Cancel Save	

RIP – Global Settings

RIP – Interface Settings

The **RIP Interface Settings** tab allows users to configure RIP interfaces on the GWN router. It displays a list of interfaces that can participate in the RIP routing protocol. Users can manage settings like the RIP version used for transmitting and receiving, authentication types, and other advanced options for RIP routing.

To add an interface, click the **Add** button, or to edit an interface, click the **edit icon**. See the provided images for visual guidance.

RIP									
Global Settings	nterface Settings	Route Advertisem	ent Neighbor Info						
Add Delet	e								
Name	Enable	Interface	RIP Tx Version	RIP Rx Version	RIPv2 Broadcast	Interface Suppression	Loop Protection	Authentication Type	Operations
VLAN1		2	Global Settings	Global Settings	Disabled	Disabled	Split Horizon	Off	CÓ (
								Total: 1 <	2
								iotai: 1 <	1 > 10 / page ~

RIP – Interface Settings

Key Parameters:

- Interface: Specifies the interface that RIP will run on (e.g., VLAN, physical interface).
- RIP Tx Version / RIP Rx Version: Select the RIP version for transmitting and receiving routes.
- RIPv2 Broadcast: Enable/disable broadcasting RIP version 2 messages.
- Interface Suppression: Suppresses sending RIP updates on the interface.
- Loop Protection: Protects from routing loops using the Split Horizon method.
- Authentication Type: Choose the type of authentication for RIP (e.g., MD5).
- Secret: Authentication key (password) for MD5 or simple authentication.

* * * *		1~64 characters
"Name	VLANT	1~64 characters
Enable		
*Interface	2(VLAN)	
RIP Tx Version	Use Global Settings	
RIP Rx Version	Use Global Settings	
RIPv2 Broadcast()		
Interface Suppression ()		
Loop Protection	Split Horizon ~	
Authentication Type	Off Simple MD5	
*Secret ID	1	
* Secret	•••••••	1~16 characters
	 Interface RIP Tx Version RIP Rx Version RIPv2 Broadcast () Interface Suppression () Loop Protection Authentication Type Secret ID 	Enable Image: Constraint of the second s

RIP – Add/Edit interface

RIP – Route Advertisement

The **Route Advertisement** tab in the RIP section allows users to define specific routes that need to be advertised to other routers in the network. This is essential for controlling which sub-networks are shared across the RIP protocol. Proper route advertisement ensures efficient routing and network management by determining what parts of the network can be reached through the RIP-enabled router.

Navigation: To view or modify Route Advertisement settings, navigate to **Routing** \rightarrow **RIP** \rightarrow **Route Advertisement**.

RIP		
Global Settings Interface Settings Route A	dvertisement Neighbor Info	
Add Delete		
Subnet Address	Mask Length	Operations
192.168.10.0	24	C ū
		Total: 1 < 1 > 10 / page ∨

RIP – Route Advertisement

Key Features in the Route Advertisement Tab:

- **Subnet Address / Mask Length**: Displays the list of subnets being advertised along with their corresponding subnet mask lengths.
- Add Route Advertisement: This feature allows users to add one or more subnets to advertise across the network. When adding, users need to provide both the Subnet Address and the Mask Length (e.g., /24 for Class C networks).
- **Operations**: Each route entry has options to edit or delete the advertisement.

If the user wishes to add a new route advertisement, they can click on the **Add** button and provide the required subnet address and mask length. Once configured, these routes will be shared across the network via RIP.

RIP > Add Route Advertisement			
*Subnet Address / Mask Length	10.0.0.0	/ 24)
	20.0.0.0	/ 16)
		Add 🕂)
	Cancel Save		

RIP – Add Route Advertisement

RIP – Neighbor Info

The **Neighbor Info** tab in the RIP configuration provides details about the neighboring RIP routers that communicate with the router to exchange routing information. This tab displays crucial information regarding the neighbors, which helps in managing and troubleshooting RIP routing within the network.

Navigation: To view RIP neighbor details, navigate to **Routing** \rightarrow **RIP** \rightarrow **Neighbor Info**.

Key Information Displayed:

- Interface: The network interface that is communicating with the neighbor router.
- **RIP Version Info**: Displays the version of RIP used by the neighbor router.
- Default Distance: Indicates the default administrative distance for the neighbor.
- Neighbor Address: The IP address of the neighboring RIP router.
- **Update Time**: The last time an update was received from the neighboring router.

RIP						
Global Settings	Interface Settings	Route Advertise	ement	Neighbor Info		
Refresh						
Interface	RIP Versi	on Info	Defa	ault Distance	Neighbor Address	Update Time
				1		
				1		
				No data		

RIP – Neighbor Info

Border Gateway Protocol (BGP)

The **Border Gateway Protocol (BGP)** is a key exterior gateway routing protocol used to exchange routing information between different autonomous systems (AS) over the internet. BGP plays a critical role in determining the best path for data packets as they travel across various networks. On Grandstream GWN routers, BGP is configured under the **Routing** section, offering a powerful solution for network administrators to control traffic between different AS networks.

To configure BGP on Grandstream routers, navigate to **Routing** \rightarrow **BGP**.

BGP – Global Settings

The **Global Settings** tab in BGP configuration allows the user to define the general BGP parameters essential for the protocol's operation.

Key Parameters:

- **AS (Autonomous System)**: The AS number identifies the autonomous system to which the router belongs. It is a required value with a valid range from 1 to 4,294,967,295.
- **Router ID**: A unique identifier in IPv4 format for the router. The router ID is required and helps identify this router in the BGP network.

External Route Import:

- This section allows users to configure which route types (Direct, Static, OSPF, and RIP) can be imported into the BGP routing table.
- **Protocol Type**: You can check the boxes for the route types to import, and set their respective route metrics, which determine the preference for routes. Lower metric values have higher preference.

BGP		
*AS	65001	Range 1~4294967295
* Router ID	10.0.0.1	IPv4 Format
External Route Import		
Protocol Type	🗹 Direct 🔽 Static 🔽 OSPF 🔽 RIP	
	O Please go to Firewall → Rule Policy/Traffic Rules to set the acceptance rules for the WAN port.	
* Direct Route Metric	0	Default 0, range 0~429496725
* Static Route Metric	0	Default 0, range 0~429496725
* OSPF Route Metric	0	Default 0, range 0~429496725
* RIP Route Metric	0	Default 0, range 0~429496725
	Cancel Save	
	Cancel Save	

Important Firewall Configuration Note:

For BGP to function correctly, it is essential to configure the firewall to allow communication on TCP port 179. Go to Firewall \rightarrow Rule Policy/Traffic Rules and set rules that permit traffic on this port for the WAN interface. Without this configuration, subnets will be unable to communicate across BGP peers, preventing proper route exchange and connectivity between networks. This step is crucial for establishing a stable BGP connection and enabling subnet communication between autonomous systems.

BGP – Peer

In the BGP (Border Gateway Protocol) Peer tab, users can view, add, or edit BGP peers that are configured on the router. A BGP peer is a neighboring router with which routing information is exchanged. Peers are established through their IP address and ASN (Autonomous System Number).

To add or modify a BGP peer:

- Click on the **Add** button to create a new peer.
- To modify an existing peer, click the Edit icon next to the peer you want to change.

BGP									
Glob	al Settings	Peer Route	Advertisement	Peer Info					
Ad	dd Delete								
~	Name	Enable	Remote AS	Remote Address	Connection Hold Time (Sec)	Connect Retry Time (Sec)	Keepalive Time (Sec)	MD5	Operations
	BGP Peer		65002	192.168.1.2	180	120	60	Enabled	CŌ
								Total: 1 <	-

BGP – Peer page

Key configurable fields in this tab include:

- Remote AS: The Autonomous System Number of the remote peer.
- Remote Address: The IP address of the remote BGP peer.
- Connection Hold Time: The maximum amount of time to hold a BGP connection without receiving a keepalive message.
- Connect Retry Time: The interval to retry establishing a BGP connection.
- Keepalive Time: The frequency of sending keepalive messages to ensure the peer is active.
- MD5 Authentication: Optional security for BGP connections using an MD5 password for session authentication.

BGP > Add Peer		
*Name	BGP Peer	1~64 characters
Enable		
* Remote AS	65002	Range 1~4294967295
* Remote Address	192.168.1.2	
*Connection Hold Time (Sec)①	180	Default 180, range 10~65535
* Connect Retry Time (Sec) 🛈	120	Default 120, range 3–255
* Keepalive Time (Sec) 🛈	60	Default 60, range 1~1800
MD5		
* Secret	••••••	8~64 characters
	Cancel Save	
	BGP – Add/Edit Peer	

BGP – Route Advertisement

The **Route Advertisement** tab allows users to manage BGP-advertised routes by adding or removing specific subnets. Here, you can define which networks are advertised to BGP peers.

BGP			
Global Settings Peer	Route Advertisement	Peer Info	
Add Delete			
Subnet Address		Mask Length	Operations
20.0.0.0		24	C Ū
10.0.0.0		24	C ū
			Total: 2 < 1 > 10 / page ∨

BGP – Route Advertisement page

To add or modify an advertised route, click **Add** or the **Edit** icon. The configuration will prompt you to enter the subnet address and mask length, then click **Save**.

Key configurable fields in this tab include:

Subnet Address / Mask Length: Specify the network's IP address and the corresponding subnet mask length (e.g., 10.0.0.0 / 24).

BGP > Add Route Advertisement			
*Subnet Address / Mask Length	10.0.0	1	24 😑
	20.0.0.0	1	24
			Add 🕂
	Cancel Save		

BGP – Add/Edit route advertisement

BGP – Peer Info

The **Peer Info** tab in the BGP section provides details on the active BGP peers. Here, users can monitor the status and connection of their BGP peers to ensure proper route exchange.

- BGP Version Info: Shows the BGP protocol version in use, typically version 4.
- Peer Address: Displays the IP address of the BGP peer.

- Peer AS: Shows the Autonomous System (AS) number of the peer.
- Status:
 - **Established**: Indicates a fully functional BGP connection where routes are being successfully exchanged between peers. This state confirms that the BGP connection is active and stable.
 - Active: Shows the BGP connection is active but may not have fully exchanged routes.
- Uptime: Tracks how long the peer connection has been established and active.

You can click the **Refresh** button to update the status of the peers. This allows users to verify quickly if their BGP peers are properly connected and whether routes are being exchanged as expected.

BGP				
Global Settings	Peer Route Advertisem	nent Peer Info		
Refresh				
BGP Version Info	Peer Address	Peer AS	Status	Uptim
4	192.168.3.226	1	Established	20min

BGP – Peer Info

TRAFFIC MANAGEMENT

Traffic Management – Basic Settings

The GWN700x routers are capable of identifying and analyzing the traffic exchanged between the intranet clients and remote hosts located on the Internet. To enable this feature please navigate to the GUI of the router, then click on **Traffic Management** \rightarrow **Basic Settings** and toggle on "Traffic Identification".

Basic Settings	
Traffic Identification	If enabled, the router will indentify and analyze traffic on all clients. If disabled, the traffic identification history will be cleared.

Enable Traffic Identification

Traffic Statistics

When "Traffic Identification" is enabled, the router will start identifying the traffic and generate statistics. The statistics will be represented graphically as shown in the screenshot below. The feature displays the name and the type of the service generating the traffic to easily identify which services are being used and which clients are using them.

Note

GWN7003 router supports up to a month of traffic statistics data.

App Group Percentage Total * Upload * AmazonAWS 33.54 AmazonAWS Veb Services 33.54% 261.4MB 105.3MB 222.53.MB 3 AmazonAWS Web Services 33.54% 261.4MB 2.55.MB 4 3 Specify Name App Group Percentage Total * Upload * Download * Visits * TLS Web Services 33.54% 261.4MB 2.55.3MB 227.53.MB 3 AmazonAWS Web Services 33.54% 261.4MB 2.55.MB 4 1 Spatify Media Services 3.54% 251.4MB 2.55.MB 1 1 Spatify Media Services 3.54% 251.4MB 2.55.MB 1 1 Spatify Media Services 3.54% 251.4MB 1 1 1 Spatify Media Services 3.54% 251.4MB 1 1 1 Spatify Media Services 3.54% 27.07.MB 2 2 2 3 Google Web Services 1.3%	cently 1H 12I			A	PP Traffic Statistics			
Name App Group Percentage Total * Upload * Download * Visits * TLS Web Services 42.71% 332.85MB † 105.33MB ‡ 227.53MB 3 AmazonAWS Web Services 33.54% 261.4MB ‡ 25.83MB ‡ 227.53MB 4 Slack Collborative 7.59% 59.12MB ‡ 574.17KB ‡ 58.56MB 1 Spotify Media Straining Services 7.33% \$7.11MB ‡ 2.68MB \$ 54.43MB 1 WindowsUpdate Web Services 3.54% 27.59MB \$ 33.318KB \$ 27.07MB 2 Google Web Services 2.1% 16.63MB \$ 4.97MB \$ 11.66MB 3	C	Collab Media Email	orative Streaming Services	8.56% 7.36% 0.6%	0	AmazonAWS Slack Spotify		42.71% 33.54% 7.59% 7.33% 3.54%
TLS Web Services 42.71% 332.85MB 105.33MB 227.53MB 3 AmazonAWS Web Services 33.44% 261.4MB 1.255MB 228.85MB 4 Slack Collaboration 7.59% 59.12MB 1.574.17KB 4.58.65MB 1 Spotify Media Straming Services 7.33% 57.11MB 1.26.8MB 4.54.3MB 1 WindowsUpdate Web Services 3.54% 27.59MB 1.533.13KB 4.27.07MB 2 Google Web Services 2.13% 1.6.63MB 4.4.97MB 4.11.66MB 3								
AmazonAWS Web Services 33.54% 261.4MB ‡ 2.55MB ‡ 258.85MB 4 Slack Collaborative 7.59% 59.12MB ‡ 574.17KB ‡ 58.56MB 1 Spotify Media Streaming Services 7.33% 57.11MB ‡ 2.68MB ‡ 54.43MB 1 WindowsUpdate Web Services 3.54% 27.59MB ‡ 533.13KB ‡ 27.07MB 2 Google Web Services 2.13% 16.63MB ‡ 4.97MB \$ 11.66MB 3	APP List				All App Gro	ups ~ Q Searc	h Name	
Slack Collaborative 7.59% 59.12MB † 574.17KB \$ 58.56MB 1 Spotify Media Streaming services 7.33% 57.11MB † 2.68MB \$ 54.43MB 1 WindowsUpdate Web Services 3.54% 27.59MB \$ 533.13KB \$ 27.07MB 2 Google Web Services 2.13% 16.63MB \$ 4.97MB \$ 11.66MB 3		App Group	Percentage	Total 🗘				
Spotify Media Streaming Services 7.33% 57.11MB ‡ 2.68MB \$ 54.43MB 1 WindowsUpdate Web Services 3.54% 27.59MB ‡ 533.13KB \$ 27.07MB 2 Google Web Services 2.13% 16.63MB ‡ 4.97MB \$ 11.66MB 3	Name		_		Upload 🗘	Download \hat{v}	Visits $\hat{\Rightarrow}$	
Sportify Services 7.43% 5.11MB ₹.268MB €.44.33MB 1 WindowsUpdate Web Services 3.54% 27.59MB €.533.13KB €.27.07MB 2 Google Web Services 2.13% 16.63MB €.4.97MB €.11.66MB 3	Name TLS	Web Services	42.71%	332.85MB	Upload ≑ ↑ 105.33MB	Download 🗘	Visits ÷ 3	
Google Web Services 2.13% 16.63MB ↑4.97MB ↓11.66MB 3	Name TLS AmazonAWS	Web Services Web Services	42.71%	332.85MB 261.4MB	Upload ≑ ↑ 105.33MB ↑ 2.55MB	Download ≎ ↓ 227.53MB ↓ 258.85MB	Visits ÷ 3 4	
	Name TLS AmazonAWS Slack	Web Services Web Services Collaborative Media Streaming	42.71% 33.54% 7.59%	332.85MB 261.4MB 59.12MB	Upload \$ 105.33MB 2.55MB 574.17KB	Download ≎ ↓ 227.53MB ↓ 258.85MB ↓ 58.56MB	Visits ÷ 3 4 1	
GeorgeDocs Collaborative 0.97% 6.77MP 4.09.73VD 1.6.20MD 2	Name TLS AmazonAWS Slack Spotlfy	Web Services Web Services Collaborative Media Streaming Services	42.71% 33.54% 7.59% 7.33%	332.85MB 261.4MB 59.12MB 57.11MB	Upload ≎ † 105.33MB † 2.55MB † 574.17KB † 2.68MB	Download ↓ 227.53MB ↓ 258.85MB ↓ 58.56MB ↓ 54.43MB	Visits \$ 3 4 1 1	
	Name TLS AmazonAWS Slack Spotlfy WindowsUpdate	Web Services Web Services Collaborative Media Streaming Services Web Services	42.71% 33.54% 7.59% 7.33% 3.54%	332.85MB 261.4MB 59.12MB 57.11MB 27.59MB	Upload ≎ ↑ 105.33MB ↑ 2.55MB ↑ 2.55MB ↑ 574.17KB ↑ 2.68MB ↑ 533.13KB	Download \$ \$ 227.53MB \$ 258.85MB \$ 58.56MB \$ 54.43MB \$ 27.07MB	Visits \$ 3 4 1 1 2	
	Name TLS AmazonAWS Slack Spotlfy WindowsUpdate	Web Services Web Services Collaborative Media Streaming Services Web Services	42.71% 33.54% 7.59% 7.33% 3.54%	332.85MB 261.4MB 59.12MB 57.11MB 27.59MB	Upload ≎ ↑ 105.33MB ↑ 2.55MB ↑ 2.55MB ↑ 574.17KB ↑ 2.68MB ↑ 533.13KB	Download \$ \$ 227.53MB \$ 258.85MB \$ 58.56MB \$ 54.43MB \$ 27.07MB	Visits \$ 3 4 1 1 2	

Traffic Statistics and Analysis

QoS

Quality of Service (QoS) is a feature that allows the prioritization if the latency-sensitive traffic exchanged between the WAN and the LAN hosts. This will offer more control over the usage of a limited bandwidth and ensures that all application services are not affected by the amount of the traffic exchanged.

General Settings – QoS

On this page, the user will be able to allocate a percentage of the download and the upload bandwidth to 4 classes. These classes can be assigned to applications to determine which application traffic will be prioritized, this includes the inbound and the outbound traffic. Also, it's possible to tag outbound traffic with DSCP tags for each class.

oS							
General Settings APP Class Cla	ass Rules VoIP Settings						
 Bandwidth Limit 							
 Bandwidth Limit 							
WAN2							
🕈 Upload Bandwidth	Status: O Maximum Upload Bandy	vidth: 100Mbps	Class1(High): 40%	Class2(Medium): 30%	Class3(Low): 20%	Class4(Lowest): 10%	
Download Bandwidth	Status:: 🚺 Maximum Download Bar	ndwidth: 200Mbps	Class1(High): 40%	Class2(Medium): 30%	Class3(Low): 20%	Class4(Lowest): 10%	
 Tag Outbound Traffic 	Class1(High) DSCP Tag	AF41(Low)		×			
	Class2(Medium) DSCP Tag	AF42(Medium)		~			
	Class3(Low) DSCP Tag	AF13(High)		~			
	Class4(Lowest) DSCP Tag	AF43(High)		~			
		Cancel	Save				

QoS – General Settings

To set Upload/Download bandwidth percentage for each class, click on edit button Z.

Note:

If the bandwidth value is incorrect, QoS might not work properly. Before enabling QoS, please check the upload and bandwidth rates if your connection, or contact your ISP to obtain the exact upload and download values. The total sum of the bandwidth percentages cannot exceed 100%.

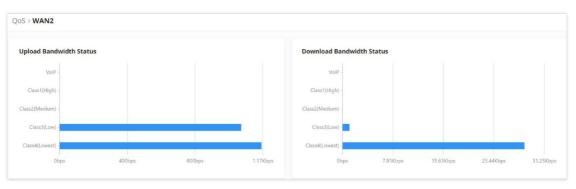
QoS > Edit Bandwidth Limit			
① If the bandwidth is incorrect, Qos cannot work properly. Before en	nabling Qos, please check the rate or contact your ISP to obtain	the exact bandw	vidth. The total proportion of bandwidth cannot exceed 100%.
Upload Bandwidth			
Status			
Maximum Upload Bandwidth	100	Mbps v	Default 100Mbps, range is 1~1024. If empty, there is no limit
*Class1(High) (%)	40		Range 1–97
*Class2(Medium) (%)	30		Range 1-97
*Class3(Low) (%)	20		Range 1~97
*Class4(Lowest) (%)	10		Range 1~97
Download Bandwidth			
Status			
Maximum Download Bandwidth	200	Mbps v	Default 100Mbps, range is 1~1024. If empty, there is no limit
*Class1(High) (%)	40		Range 1–97
	Cancel Save		

WAN Port QoS Settings

	Upload/Download Bandwidth							
Status	Toggle QoS for the WAN port on/off							
Maximum Upload/Download Bandwidth	Specify the maximum upload/download speed for the WAN port.							
Class1 (High)	Specify the bandwidth percentage allocated for Class 1.							
Class2 (Medium)	Specify the bandwidth percentage allocated for Class 2.							
Class3 (Low)	Specify the bandwidth percentage allocated for Class 3.							
Class4 (Lowest)	Specify the bandwidth percentage allocated for Class 4.							

Edit Bandwidth limit

Click on 🔟 bandwidth statistics icon to get a general overview for upload/download bandwidth status.





APP Class

GWN700X routers can prioritize the traffic of each application individually. The priority level can be set in 4 classes, class 1 having the highest priority and class 4 having the lowest priority. To access APP Class settings, please access the web GUI of the router then navigate to **Traffic Management** \rightarrow **QoS** \rightarrow **APP Class**.

The user can either set the priority for the individual applications by selecting the priority of the corresponding applications.

Gen	eral Settings APP Class	Class	Rules VoIP Setti	ngs						
_										
Eff	ciently identifiable Other	S								
Co	nfigure Classes						All App	Groups 🗸 🗸	Q Se	arch Name
_										
-	App Group	Name			Priority					
			AllCloud		Class1(High)	Uass2	(Medium)	Class3(Lov	0 0	Class4(Lowe
		\checkmark	RTSP		Class1(High)	Class2	(Medium)	Class3(Low	0	Class4(Lowe
			RTP		Class1(High)	Class7	(Medium)	Class3(Lov	0	Class4(Lowe
		_								
	Media Streaming Services	\checkmark	SD-RTN		Class1(High)	Class2	(Medium)	Class3(Lov	<i>i</i>) ()	Class4(Lowe
~		~	RTMP		Class1(High)	Class2	(Medium)	Class3(Low) ()	Class4(Low
					Class1(High)	O diana	(Medium)	Class3(Lov	a ()	Class4(Lowe
			MPEG_TS		Class I (High)		(wealum)		0 0	Class4(Lowe
		\checkmark	MpegDash		Class1(High)	Class2	(Medium)	Class3(Low	<i>(</i>) ()	Class4(Lowe
			IRC	(Class1(High)	Class2	(Medium)	Class3(Lov	0	Class4(Lowe
	Messaging		WhatsApp	0	Class1(High)	Class2	(Medium)	Class3(Lov) ()	Class4(Lowe
	Micszakink									
				Cancel	Reset	Save				

QoS – APP Class

Or, the use can select the applications and application categories and then click "**Configure Classes**" then choose the adequate priority.

QoS		
General Settings APP Class	Class Rules VoIP Settings	
Efficiently identifiable Others		
Configure Classes	Configure Classes ×	All App Groups v Q Search Name
App Group		dium) Class3(Low) Class4(Lowest)
	*Priority Class1(High) Class2(Medium) Class3(Low) 	dium) Class3(Low) Class4(Lowest)
	Class4(Lowest)	
		dium) Class3(Low) Class4(Lowest)
Media Streaming Se	Cancel OK	dium) 💿 Class3(Low) 🔿 Class4(Lowest)
		dium) Class3(Low) Class4(Lowest)
	MPEG_TS Class1(High) Class2(Medium) Oclass3(Low) Class4(Lowest)
	MpegDash Class1(High) Class2(Medium) 💿 Class3(Low) 🔿 Class4(Lowest)
	Cancel Reset Save	

QoS – Apps Class – Configure Classes

Note

App Class may take sometime to be applied since the router needs to inspect a sufficient number of packets to identify the traffic generated by the application.

Class Rules

QoS class rules are rules which sets the QoS based on source or/and destination IP addresses, and source and destination ports.

*Name		1~64 characters
Status		
IP Family	 Any IPv4 IPv6 	
Protocol Type	• TCP/UDP TCP UDP	
Source IP Address		Enter the IP address/mask length, such a "192.168.122.0/24"
Source Port 🕕		The valid range is 1-65535. You can ente single port or a port range.
Destination IP Address		Enter the IP address/mask length, such a "192.168.122.0/24"
Destination Port ()		The valid range is 1-65535. You can ente single port or a port range.
*Priority	Please Select Priority ~	
DSCP	None	

QoS – Add Class Rules

Name	Enter the name of the class. The character limit is 1-94 characters.
Status	Enable or disable the class's status.
	Choose the IP family:
IP Family	• Any: The IP addresses allowed can either be IPv4 or IPv6.
e e e e e e e e e e e e e e e e e e e	• IPv4: The IP addresses allowed are strictly IPv4.
	• IPv6: The IP addresses allowed are strictly IPv6.
	Choose the protocol type:
Protocol Type	• TCP/UDP: The QoS class will apply to both TCP and UDP traffic.
	• TCP: The QoS class will apply only to the TCP traffic.
	• UDP: The QoS class will apply only to the UDP traffic.
Source IP Address	Enter the source IP address/mask length. E.g.,"192.168.122.0/24"
	Enter a single port number, multiple port numbers, or a range of ports number.
	Example:
	- To enter a single port number, type the port number such as "3074".
Source Port	- To enter multiple port numbers, type the port numbers with a comma in between each port number, such as "3074, 5060, 10000".
	- To enter a range of port, enter the first port number in the range, then type a dash (-) and enter the last port number in the range. E.g., "10000-20000"
	Note: The valid range of port numbers that can be entered is 1-65535.
Destination IP Address	Enter the destination IP address/mask length. E.g., "192.168.122.0/24"
	Enter a single port number, multiple port numbers, or a range of ports number.
	Example:
	- To enter a single port number, type the port number such as "3074".
Destination Port	- To enter multiple port numbers, type the port numbers with a comma in between each port number, such as "3074, 5060, 10000".
	- To enter a range of port, enter the first port number in the range, then type a dash (-) and enter the last port number in the range. E.g., "10000-20000"
	Note: The valid range of port numbers that can be entered is 1-65535.
Priority	Select the class of priority.

QoS – Add Class Rules

VoIP Settings

VoIP Settings in QoS allow the user to identify and prioritize the VoIP traffic that is forwarded by the router. To configure this option, please access the web UI of the GWN router and navigate to **Traffic Management** \rightarrow **QoS** \rightarrow **VoIP Settings**, then toggle on the "**VoIP Prioritization**", after that specify the SIP UDP port, by default the port number is 5060.

QoS		
General Settings APP Class Class Rules	VoIP Settings	
VoIP Prioritization	When enabled, it will give priority to distributing traffic for VoIP SIP/RTP services and will not be restricted by other class bandwidth allocation	
SIP UDP Port	5060	Default 5060
	Cancel Save	
	VoIP Settings	

Bandwidth Limit

Bandwidth limit feature helps to limit bandwidth by specifying the maximum upload and download limit, then this limit can be applied on each IP/MAC address or applied on all IP addresses in the IP address range. Navigate to **Web UI** \rightarrow **Traffic Management** \rightarrow **Bandwidth Limit**.

Add Delete							
 Name 	Status	Range Constraint	IP Address	MAC Address	Maximum Upload Bandwidth	Maximum Download Bandwidth	Operations
Guests		IP Address	192.168.10.0/24	-	10Mbps	20Mbps	ē

Bandwidth Limit page

To add a bandwidth rule, please click on "Add" button or click on "Edit" icon as shown above.

Please refer to the figure below	Please	refer	to	the	figure	bel	ow
----------------------------------	--------	-------	----	-----	--------	-----	----

Bandwidth Limit > Add Bandwidth Limit				
*Name	Guests	1~64 characters		
Status				
Range Constraint	IP Address			
Application Mode ①	Individual Shared			
*IP Address/Mask Length	192.168.10.0	/ 24		•
			Ado	•
Maximum Upload Bandwidth	10	Mbj	05 V	The range is 1~1024, if it is empty, there is no limit
Maximum Download Bandwidth	20	The range is 1~1024, if it is empty, there is no limit		
Bandwidth Schedule				
*Schedule	Office hours		~	
	Cancel Save			

Add/edit Bandwidth rule

Application Mode: Select "Individual" to set the maximum upload bandwidth and maximum download bandwidth that can be used by each IP address, and "shared" to set the sum of the maximum upload bandwidth and maximum download bandwidth that can be used by all IP addresses in the IP address range.

AP MANAGEMENT

GWN700X routers come with an embedded controller for the GWN access points. The user can configure all the Wi-Fi related settings through the controller. When the APs are connected to the router, and they are paired with it, they will automatically inherit the configuration which has been set on the router's AP Management section.

Access Points

In this section, the user can add the access point which can be controlled using the embedded controller within the router. The user can either pair or takeover an access point in order to be able to configure it. The configuration performed on the router AP embedded controller will be pushed to the access points; thus, offering a centralized management of the GWN access points.

Note

Please note that the GWN access point that the user wishes to configure must be on the same LAN as the router.

To add a GWN access point to the GWN router, please navigate to **Web UI** \rightarrow **AP Management** \rightarrow **Access Points**.

ccess Points							Export
Pair AP Takeove	r AP Configure		Delete Reboot	Transfer • On	line: 1		
All device types \sim	Q Search MAC / Devi	ce Name					
Device Type	MAC Address	Device Name	IP Address	Firmware Versio	on SSIDs	System Up Ti	Operations
• GWN7624	C0:74:AD:90:B2:40	GWN7624	IPv4:192.168.70.171 IPv6:-	1.0.25.10	5	13min	K 550 () II
						Total: 1 <	1 > 10 / page

Access Points List

Pair AP: Use this button when pairing an AP which has not be set as a master.

Takeover AP: Use this button to take over an access point which has formerly been set as slave to a different master device. In order to pair the devices successfully, the network administrator must enter the password of the master device.

Note

While the router can create SSIDs and configure the Wi-Fi related settings, the router itself is not able to broadcast the SSID. Therefore, a GWN access point is required to broadcast the Wi-Fi signal.

Click on a paired GWN AP to view Details, Client list and debug tools. Please refer to the figures below:

Details section contains details about the paired AP like firmware version, SSID, IP address, Temperature, etc.

Access Points > C0:74	:AD:90:B2:40 (GWN	7624)	
		Firmware Version	1.0.25.10
Details		SSID	Hall (5G: c0:74:ad:90:b2:42)
Client List		IPv4 Address	192.168.70.171
Debug	\sim	IPv4 Address	192.108.70.171
		IPv6	-
		System Up Time	1h 10min
		System Time	2023-10-04 11:40
		Load Average	1min: 2.59 5min: 2.57 15min: 2.
		Temperature	41°C
		Link Speed	NET/POE:1000M FD
			NET:Disconnected
			PORT3:Disconnected
			PORT4:Disconnected
		2.4G Radio Status	Channel: 0

Paired APs – Details

Client List section lists all the connected clients trough this AP with many info like MAC Address, Device name, IP Address, bandwidth, etc.

Access Points > C0:74:AD:90:E	B2:40 (GWN	17624)								
Details		MAC Address	Device Name	IP Address	Duration $\hat{\circ}$	Total 🗘	Upload ‡	Download $\hat{\tau}$	Upload sp 🗘	Download
Client List		• E D	Ain	IPv4:192.168.70.235 IPv6:-	28s	4.16KB	2.3KB	1.86KB	18.39Kbps	↓ 14.85k
Debug	~							Total: 1	(1 >	107page ∨

Paired APs – Client list

Debug section provides the users with many debug tools to help diagnostics any issue like Ping/Traceroute, One-click Debug and SSH Remote Access.

Access Points > C0:74:AD:90:B2:40 (GWN7624)				
Details	* Tool	IPv4 Ping	~		
Client List	* Target IP Address / Hostname	8.8.8.8			
Debug ^		Start			
Ping / Traceroute	Diagnostic Result				
Core File					
One-click Debug	PING 8.8.8.8 (8.8.8.8): 56 o 64 bytes from 8.8.8.8: seq=0 64 bytes from 8.8.8.8: seq=1	0 ttl=113 time=21.727 ms			
SSH Remote Access	64 bytes from 8.8.8.8: seq=2 ttl=113 time=19.078 ms 64 bytes from 8.8.8.8: seq=3 ttl=113 time=19.874 ms				
	64 bytes from 8.8.8.8: seq=4				
	8.8.8.8 ping statistics				
		ckets received, 0% packet loss			
	round-trip min/avg/max = 19.				

Paired APs – Debug

Transfer APs to GDMS Networking/GWN Manager

GWN routers also enables to users to transfer their paired GWN APs to GDMS Networking/GWN Manager.

On the **AP Management** → **Access Points** page, select the AP or APs then click on "**Transfer**" button as shown below:

Pair AP	Takeover			Delete Reboot	Transfer • Online	2: 1		
ll device	e types v	Q Search MAC / Devic	Device Name	IP Address	Firmware Version	SSIDs	System Up Tin	Operations
• 0	5WN7624	C0:74:AD:90:B2:40	GWN7624	IPv4:192.168.70.171 IPv6:-	1.0.25.10	5	21min	C 📼 🛛 Ū

Access Points List

On the next page, select either GDMS Networking or GWN Manager then click "**Save**" button. the user will be forwarded automatically to either GDMS Networking or GWN Manager to login.

Access Points > Trans	sfer				
After successful trans	sfer, it will be taken over by Cloud/M	Aanger, and the router will delete the de	vice information synchronously		
	Transfer to	● GWN Cloud O GV	VN Manager		
	 Transferable Device 	25			
	Device Type	MAC Addres	s	Device Name	
	GWN7624	C0:74:AD:90:	B2:40	GWN7624	
					< 1 >
	 Untransferable Dev 	rices			
	Device Type	MAC Address	Device Name	Reasons	
			No device		
		Cancel Save			

Transfer AP to GDMS Networking or GWN Manager

Note:

After successful transfer, it will be taken over by Cloud/Manger, and the router will delete the device information synchronously.

SSIDs

In this page, the user can configure SSID settings. The Wi-Fi SSID will be broadcasted by the paired access points. This offers a centralized control over the SSIDs created which makes managing many GWN access points easier and more convenient.

Add Delete					Q Search for SSID Name	
SSID Name	Wi-Fi	SSID Band	Associated VLAN	Security Mode	Captive Portal	Operations
Office	Enabled	Dual-Band		WPA2	Disabled	C ū
Guests Wifi	Enabled	Dual-Band		WPA2	Disabled	C Ū



In order to add an SSID, the user should click on "Add" button, then the following page will appear:

SSIDs > Edit SSID				
	Basic Information \land			
	Wi-Fi			
	*Name	Office		1~32 characters
	Associated VLAN ()			
	SSID Band	Dual-Band 2.4G 5G		
	Access Security $ \sim$			
	Advanced \vee			
	Device Management $\ \land$			
	All Devices		All device types \sim	Q Search MAC / Device Name
	Device Name	Device Type	MAC Address	SSIDs (i)
	GWN7624	GWN7624	C0:74:AD:90:B2:40	2.4G: 2/8 5G: 2/8
	Selected: 1			< 1 >
		Cancel Save		
		Add SSID		

Basic Information		
Wi-Fi	Toggle on/off the Wi-Fi SSID.	
Name	Enter the name of the SSID.	
Associated VLAN	Toggle "ON" to enable VLAN, then specify the VLAN from the list or click on "Add VLAN" to add one.	
	Choose the Wi-Fi SSID band.	
SSID Band	• Dual-Band: Both bands will be enabled.	
	• 2.4G: Only 2.4G band is enabled.	
	• 5G: Only 5G band is enabled.	
	Access Security	
	Choose the security mode for the Wi-Fi SSID.	
	• Open	
	• WPA/WPA2	
Security Mode	• WPA2	
	• WPA2/WPA3	
	• WPA3 • WPA3-192	
	• wras-172	
	Choose the WPA key mode:	
	• PSK	
WPA Key Mode	• 802.1x	
	• PPSK without RADIUS	
	• PPSK with RADIUS	
	Choose the encryption type:	
WPA Encryption Type	• AES	
	• AES/TKIP	
WPA Shared Key	Enter the shared key phrase. This key phrase will be required to enter when connecting to the Wi-Fi SSID.	

Enable Captive Portal	Toggle Captive Portal on/off.Captive Portal Policy: Choose the created captive portal policy.	
Blocklist Filtering	Choose a blocklist for the Wi-Fi SSID.	
Client Isolation	 Closed: Allow access between wireless clients. Radio: All wireless clients will be isolated from each other. Internet: Access to any private IP address will be blocked. Gateway MAC: Private IP addresses except for the configured gateway will be blocked. 	
802.11w	 Disabled Optional: either 802.11w supported or unsupported clients can access the network. Required: only the clients that support 802.11w can access the network. 	
	Advanced	
SSID Hidden	After enabled, wireless devices will not be able to scan this Wi-Fi, and can only connect by manually adding network.	
DTIM Period	Configure the delivery traffic indication message (DTIM) period in beacons. Clients will check the device for buffered data at every configured DTIM Period. You may set a high value for power saving consideration. Please input an integer between 1 to 10.	
Wireless Client Limit	Configure the limit for wireless client, valid from 1 to 256. If every Radio has an independent SSID, each SSID will have the same limit. Therefore, setting a limit of 256 will limit each SSID to 256 clients independently.	
Client Inactivity Timeout (sec)	Router/AP will remove the client's entry if the client generates no traffic at all for the specified time period. The client inactivity timeout is set to 300 seconds by default.	
Multicast Broadcast Suppression	 Disabled: all of the broadcast and multicast packages will be forwarded to the wireless interface. Enabled: all of the broadcast and multicast packages will be discarded except DHCP/ARP/IGMP/ND. Enabled with ARP Proxy: enable the optimization with ARP Proxy enabled in the meantime. 	
Convert IP Multicast to Unicast	 Disabled: No IP multicast packets will be converted to unicast packets. Passive: The device will not actively send IGMP queries, and the IGMP snooping entries may be aged after 300s and cannot be forwarded as multicast data. Active: The device will actively send IGMP queries and keep IGMP snooping entries updated. 	
Schedule	Enable then select from the drop-down list or create a time schedule when this SSID can be used.	
Voice Enterprise	Enable voice enterprise.	
802.11r	Enable 802.11r.	
802.11k	Enable 802.11k.	
802.11v	Enable 802.11v.	
ARP Proxy	Once enabled, devices will avoid transferring the ARP messages to stations, while initiatively answer the ARP requests in the LAN.	
U-APSD	Configures whether to enable U-APSD (Unscheduled Automatic Power Save Delivery).	

Bandwidth Limit	Toggle ON/OFF Bandwidth limit Note: If Hardware acceleration is enabled, Bandwidth Limit does not take effect. Please go to Network
	Settings/Network Acceleration to disable
Maximum Upload	Limit the upload bandwidth used by this SSID. The range is 1~1024, if it is empty, there is no limit.
Bandwidth	The values can be set as Kbps or Mbps.
Maximum Download	Limit the download bandwidth used by this SSID. The range is 1~1024, if it is empty, there is no limit
Bandwidth	The values can be set as Kbps or Mbps.
Bandwidth Schedule	Toggle ON/OFF Bandwidth Schedule; if it's ON, then select a schedule from the drop-down list or click on
	"Create Schedule".
	Device Management
In this section, the user is a	ble to add and remove the GWN access points that can broadcast the Wi-Fi SSID. There is also the option to search
the device by MAC address	s or name.

Add SSID

Private Pre-Shared Key (PPSK)

PPSK (Private Pre-Shared Key) is a way of creating Wi-Fi passwords per group of clients instead of using one single password for all clients. When configuring PPSK, the user can specify the Wi-Fi password, maximum number of access clients, maximum upload and download bandwidth.

To start using PPSK, please follow the steps below:

- 1. First, create an SSID with WPA key mode set to either PPSK without RADIUS or PPSK with RADIUS.
- 2. Navigate to **Web UI** \rightarrow **AP Management** \rightarrow **PPSK** page, then click on "**Add**" button then fill in the fields as shown below:

PPSK			
	1		
	No PPSK, PPSK can be configured and managed		
	Add Import		
	PPSK page		
PPSK > Add PPSK			
* SSID Name	Guests Wifi		
*Account ()	RADIUSuser1		1-64 bits, do not support the inpu English comma
*Wi-Fi Password) _{pe} t	8-63 ASCII characters or 8-64 hex characters
* Maximum Number of Access Clients ①	1		Default 1, range 1~100
MAC Address ()	1C : 74 : AD : 11 : 22 : 33		
Maximum Upload Bandwidth	10	Mbps 、	Range 1~1024
Maximum Download Bandwidth	20	Mbps	Range 1~1024
Description	Wi-Fi for Guests		0~128 characters
	Cancel Save		

SSID Name	Select from the drop-down list the SSID that has been previously configured with WPA Key mode set to PPSK without RADIUS or PPSK with RADIUS.
Account	If the WPA key mode in the selected SSID is "PPSK with RADIUS", the account is the user account of the RADIUS server.
Wi-Fi Password	Specify a Wi-Fi password
Maximum Number of Access Clients	Confgures the maximum number of devices allowed to be online for the same PPSK account.
MAC Address	Enter a MAC Address Note: this field is only available if the Maximum Number of Access Clients is set to 1.
Maximum Upload Bandwidth	Specify the maximum upload bandwidth in Mbps or Kbps.
Maximum Download Bandwidth	Specify the maximum downlolad bandwidth in Mbps or Kbps.
Description	Specify a description for the PPSK

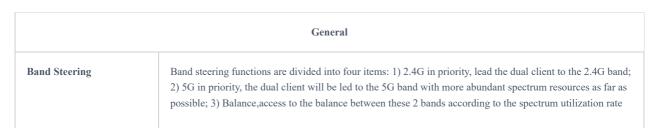
Add PPSK

Radio

Under **AP Managements** \rightarrow **Radio**, the user will be able to set the general wireless settings for all the Wi-Fi SSIDs created by the router. These settings will take effect on the level of the access points which are paired with the router.

Radio		
General		
Band Steering	Off v	
Airtime Fairness		
*Beacon Interval 🛈	100	Default 100, range 40~500
Country / Region	United States	
2.4G 🔿		
Channel Width	● 20MHz ○ 20&40MHz ○ 40MHz	
Channel	Auto Dynamically assigned by RRM	
Radio Power ①	High	
Short Guard Interval 🛈		
Allow Legacy Devices (802.11b)		
Minimum RSSI 🕥		
Minimum Rate 🛈		
Wi-Fi 5 Compatible Mode 🛈		
	Cancel Save	

Radio



	of 2.4G and 5G. In order to better use this function, proposed to enable voice enterprise via SSIDs \rightarrow Advanced \rightarrow Enable Voice Enterprise.
Airtime Fairness	Enabling Airtime Fairness will make the transmission between the access point and the clients more efficient. This is achieved by offering equal airtime to all the devices connected to the access point.
Beacon Interval	Configures the beacon period, which decides the frequency the 802.11 beacon management frames router transmits. Please input an integer, from 40 to 500.1. When router enables several SSIDs with different interval values, the max value will take effect;2. When router enables less than 3 SSIDs, the interval value will be effective are the values from 40 to 500;3. When router enables more than 2 but less than 9 SSIDs, the interval value will be effective are the values from 100 to 500;4. When router enables more than 8 SSIDs, the interval value will be effective are the values from 200 to 500.Note: mesh feature will take up a share when it is enabled.
Country / Region	This option shows the country/region which has been selected. To edit the region, please navigate to System Settings \rightarrow Basic Settings.
	2.4G & 5G
	Select the channel width.
Channel Width	 2.4G: 20Mhz, 20&40Mhz, 40Mhz 5G: 20Mhz, 40Mhz, 80Mhz
	Pick how the access points will be able to choose a specific channel.
Channel	 Auto: Dynamically assigned by RRM:
	Please select the radio power according to the actual situation, too high radio power will increase the disturbance between devices.
Radio Power	• Low • Medium
Kaulo I owei	HighCustom
	 Oynamically Assigned by RRM Auto
Short Guard Interval	This can improve the wireless connection rate if enabled under non multipath environment.
Allow Legacy Devices (802.11b) (2.4Ghz Only)	When the signal strength is lower than the minimum RSSI, the client will be disconnected (unless it's an Apple device).
Minimum RSSI	When the signal strength is lower than the minimum RSSI, the client will be disconnected (unless it's an Apple device).
Minimum Rate	Specify whether to limit the minimum access rate for clients. This function may guarantee the connection quality.
Wi-Fi 5 Compatible Mode	Some old devices do not support Wi-Fi6 well, and may not be able to scan the signal or connect poorly. After enabled, it will switch to Wi-Fi5 mode to solve the compatibility problem. At the same time, it will turn off Wi-Fi6 related functions.
	Radio

Radio

Mesh

Through the controller embedded in the GWN700X routers, the user can configure a Wi-Fi Mesh using the GWN access points. The configuration is centralized and the user can view the topology of the Mesh.

• Configuration:

To configure GWN access points in a Mesh network successfully, the user must pair the access points first with the GWN router, then configure the same SSID on the access points. Once that's done, the user should navigate to **AP Management** \rightarrow **Mesh** \rightarrow **Configure**, then enable Mesh and configure the related information as shown in the figure below.

Mesh		
Configure Topology		
Mesh	Once enabled, the AP can only support up to 5 dual-band SSIDs and single-band SSIDs in the same VLAN	10
*Scan Interval (min) 🕕	5	Default 5, range 1~5
*Wireless Cascade	3	Default 3, range 1~3
Interface	5G	
	Cancel Save	
	© 2023 Grandstream Networks, Inc. Grandstream Software License Agreem	ent

Mesh Configuration

For more information about the parameters that need to be configured, please refer to the table below.

Mesh	Enable Mesh. Once enabled, the AP can only support up to 5 dual-band SSIDs and 10 single-band SSIDs in the same VLAN.
Scan Interval (min)	Configures the interval for the APs to scan the mesh. The valid range is 1-5. The default value is 5.
Wireless Cascade	Define the wireless cascade number. The valid range is 1-3. The default value is 3.
Interface	Displays which interface is going to be used for mesh.

Mesh Configuration

• Topology:

In this page, the user will be able to see the topology of the GWN access points when they are configured in a Mesh network. The page will display information related to the APs like the MAC address, RSSI, Channel, IP Address, and Clients. It will show as well the cascades in the Mesh.

Mesh					
Configure Topology					
				Q Se	earch MAC / Name
Route / AP	RSSI	Channel	IP Address	Clients	Operations
^ C0:74:AD:62:C0:D4	-	5G:36	192.168.80.108	1	
C0:74:AD:50:FA:10	-60	5G:36	192.168.80.25	1	Ð

Mesh Topology

Switch Management

The **Switch Management** feature allows administrators to monitor, configure, and manage multiple switches through the GWN router interface. With this feature, users can easily add switches to the management platform, take control of their configurations, upgrade firmware, and view performance metrics.

Key Features:

• Switch Discovery: Automatically discover available switches connected to the network for easy management.

- **Take over Device**: Add and take over switches for centralized management, allowing you to configure and monitor them directly from the GWN interface.
- **Upgrade, Reboot, and Export**: Perform administrative tasks like upgrading switch firmware, rebooting devices, and exporting a list of managed switches.
- Detailed Monitoring: View performance metrics, such as traffic statistics and PoE port details, for each switch.
- **Comprehensive Configuration**: Global switch settings and individual port configurations are available, enabling you to fine-tune your network based on specific needs.

This feature streamlines network management by providing a unified platform to control all switches in the environment, enhancing visibility, and reducing the complexity of managing multiple devices.

Switches

Take over Device (add switch)

• Take over a switch

To manage a switch for the first time in your GWN network, follow these steps to "take over" and configure it.

Steps to Take over a Switch:

1. Navigate to: Switch Management → Switches. This will bring you to the Switches table. If no devices have been added yet, you will see a prompt stating "No data. Please select at least one device to manage."

Switches	
	No data. Please select at least one device to manage.
	Take over Device

Switch Management

2. Discover Available Switches:

Click on the **Take over Device** button. A new window will open showing all the switches in your network that are available for management. For each switch, you'll see:

- Device Model
- MAC Address
- IP Address (IPv4/IPv6)

• Firmware Version

If the firmware version is outdated, an upgrade may be required before taking over the switch.

The following switches GWN7801(P)/7802(P)/7 GWN7811(P)/7812P/78 GWN7806(P)/7816(P)/7	803(P) 1.0.5.34+ 13(P)/7830/7831 1.0.7.50+	κ, it is recommended to upgrade first before t	aning them over for management.
			Q MAC / IP Address
Device Model	MAC Address	IP Address	Firmware Version
GWN7803P	C0:74:AD:BA:24:FC	IPv4:192.168.80.37 IPv6:-	1.0.9.15
GWN7813P	C0:74:AD:CC:DF:18	IPv4:20.0.0.132 IPv6:-	1.0.7.71
GWN7813P	C0:74:AD:DF:CC:94	IPv4:192.168.80.211 IPv6:-	1.0.7.68
elected: 3			

Discover Available Switches

3. Select the Switch:

Tick the checkbox next to the switch you want to take over. You can select multiple switches if desired. Click **Save** once your selection is made.

4. Enter the Login Password:

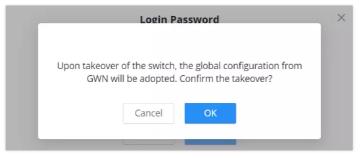
For security, a password prompt will appear. Enter the **Login Password** of the switch to confirm and complete the takeover.

	Login Password	×
* Login Password	1	
•••••	~	
	Cancel	

Enter the Login Password

5. Confirm the Takeover:

A confirmation dialog will appear indicating that the global configuration from the GWN router will be adopted on the switch. Click **OK** to proceed.



Confirm the Takeover

6. Review the Managed Switches:

Once successfully added, the switch will appear in the Switches table with the following details:

- Device Model
- MAC Address
- Device Name
- IP Address
- Firmware Version
- System Up Time

You will also see a status for how many switches are **Online** and **Offline**.

litches									🖾 Expo
① Existing	device Takeover failure, <u>Vie</u>	w details							
Take over D	Device Upgrade	Delete • Onlin	e: 2 🔹 Offline: 0		All Status	 All device model 	5 v	Q. MAC / IP Add	ress / Device Name
No.	Device Model 🗘	MAC Address	Device Name	IP Address	Firmware Version		\$	Clients ≑	Operations
1	 GWN7813P 	C0:74:AD:CC:DF:18	GWN7813P	IPv4:20.0.0.132 IPv6:-	1.0.7.71	1h 55min		3	0 2 0 1
2	 GWN7813P 	C0:74:AD:DF:CC:94	GWN7813P	IPv4:192.168.80.21 IPv6:-	1 1.0.7.68	57min		2	0 2 0 0
								Total: 2 <	1 > 10 / page

Review the Managed Switches

• Delete (Remove) a switch

To remove a switch from the GWN router:

- 1. Navigate to: **Switch Management** \rightarrow **Switches**.
- 2. **Delete a Single Switch:** in the **Operations** column of the Switches table, click the **Delete** icon next to the switch you wish to remove.

No.	Device Model 🗘	MAC Address	Device Name	IP Address	Firmware Version	System Up	Clients ≑	Operations
1	 GWN7813P 	C0:74:AD:CC:DF:18	GWN7813P	IPv4:20.0.0.132 IPv6:-	1.0.7.71	2h 10min	2	0 C U
2	 GWN7813P 	C0:74:AD:DF:CC:94	GWN7813P	IPv4:192.168.80.211 IPv6:-	1.0.7.68	1h 13min	2	0 6 0 0

Delete (Remove) a switch - part 1

3. **Delete Multiple Switches:** alternatively, select multiple switches by checking the boxes next to their names, then click the **Delete** button at the top of the table.

Take	e over De	vice Upgrade	Delete • Onlin	e: 2 🔹 Offline: 0		All Status ~	All	device models ~	Q. MAC / IP Add	ress / Device Name
~	No.	Device Model ≑	MAC Address	Device Name	IP Address	Firmware Version	¢	System Up Time	Clients 🗘	Operations
~	1	 GWN7813P 	C0:74:AD:CC:DF:18	GWN7813P	IPv4:20.0.0.132 IPv6:-	1.0.7.71		2h 10min	2	0 ₪ ∪ ₫
~	2	 GWN7813P 	C0:74:AD:DF:CC:94	GWN7813P	IPv4:192.168.80.21 IPv6:-	1.0.7.68		1h 13min	2	0 2 0 1
									Total: 2 <	1 > 10 / page

Delete (Remove) a switch – part 2

4. **Confirmation:** confirm the deletion in the prompt that appears.

Confirm to d	lelete this device?
Cancel	Delete
1.0.7.71	́ С ∪ ⊡́
1.0.7.68	0 C U Ū

Delete (Remove) a switch – part 3

Upgrade, Reboot and Export

- Upgrade switches
- 1. Navigate to: **Switch Management** → **Switches.**
- 2. In the Switches table, select the switches you want to upgrade by checking the boxes.
- 3. Click Upgrade.

- 4. A prompt will appear: "Send request to the selected device successfully, and the device will attempt to upgrade."
 Note: Do not disconnect the network or power supply during the upgrade process.
- 5. Click **Send** to initiate the upgrade.

witches										🖻 Expor
① Existing	device Takeover failure, <u>V</u>	iew details								
Take over [Device Upgrade	Delete	• Online: 2 • Offline: 0	All Status	~	A	Il device models	~	Q MAC / IP Add	
✓ No.	Device Model	MAC A			re		System Up Time	4 5	Clients 🗘	Operations
v 1	 GWN7813P 	C0:74:A	Send request to the selected device su and the device will attempt to up				2h 55min		2	0 C U Ō
2	• GWN7813P	C0:74:A	Note: During the download and installatic disconnect the network connection and the o supply, the device will not be connected to t during the installation.	device power			1h 58min		2	0000
			Cancel Send						Total: 2 <	1 > 10 / page



• Reboot switch

- 1. Navigate to: Switch Management \rightarrow Switches.
- 2. In the Switches table, identify the switch you want to reboot.
- 3. Click the Reboot icon (power symbol) located under the Operations column.
- 4. A confirmation message will appear asking: "Confirm to restart this device?"
- 5. Click **Reboot** to restart the switch.

DE	xisting dev	ice Takeover failure, <u>Vie</u>	w details						
ake	over Devi	ice Upgrade	Delete • Onlin	e: 2 Offline:	D	All Status ~	All device models	Confirm to resta	drass / Davies Mame
	No.	Device Model ≑	MAC Address	Device Name	IP Address	Firmware Version		Cancel	Reboot
	1	GWN7813P	C0:74:AD:CC:DF:18	GWN7813P	IPv4:20.0.0.132 IPv6:-	1.0.7.71	3h	2	0 00
	2	• GWN7813P	C0:74:AD:DF:CC:94	GWN7813P	IPv4:192.168.80.211 IPv6:-	1.0.7.68	2h 3min	2	0 2 0 1
									_

Reboot switches

• Export switches list

- 1. Navigate to: Switch Management \rightarrow Switches.
- 2. In the Switches table, click the Export button located at the top-right corner.
- 3. The switch list will be downloaded as an Excel (.xls) file, containing details such as Device Model, MAC Address, IP Address, Firmware Version, and System Up Time.

						26 ==	-	ist_2024102412045 I — 1.4 KB).xls			👤 adr	min ~
witches						Show all d	ownlo	ads				🖸 Exp	oort
(i) Existing of	device Takeover failure, <u>Vie</u>	w details											
Take over D	evice Upgrade	Delete • Onlir	ne: 2 🔹 Offline: 1	D	All Status	~	All	device models	~	Q MAC / IP Add	ress / Device	Name	
No.	Device Model 🗘	MAC Address	Device Name	IP Address	Firmv Versie		÷	System Up Time	Å. V	Clients ≑	Operation	15	
v 1	 GWN7813P 	C0:74:AD:CC:DF:18	GWN7813P	IPv4:20.0.0.132 IPv6:-	1.0.7.7	71		3h 5min		2	0 2	Ů Ū	
2	 GWN7813P 	C0:74:AD:DF:CC:94	GWN7813P	IPv4:192.168.80.211 IPv6:-	1.0.7.6	68		2h 8min		2	0 2	<u>ت</u> ن	

Export switches

Switch Details

Switches > CO:7	4:AD:CC:DF:18 (GWI	N7813P)							
Performance	Info Port	Debug							
Traffic Statistic	s PoE Ports								
Clear All					Statistical Inter	val 10second	 ✓ All Pc 	orts ×	
Port	Receive Rate	InOctets	InPackets	InErrPackets	Transmit Rate	OutOctets	OutPackets	OutEr	Operations
1/0/1	0bps	OB	0	0	0bps	OB	0	0	\Diamond
1/0/2	0bps	OB	0	0	0bps	OB	0	0	\Diamond
1/0/3	0bps	OB	0	0	0bps	OB	0	0	\Diamond
1/0/4	0bps	OB	0	0	0bps	OB	0	0	\diamond

Switch – Performance – Traffic Statistics

witches > C0:74	4:AD:CC:DF:18 (GW	(N7813P)					
Performance	Info Port	Debug					
Traffic Statistics	PoE Ports						
						All Ports \times	
Port	Power Status	Current (mA)	Current power (mW)	PD Class	Temperature (°C)	Power-Off Schedule	Operations
1/0/1	Off	0	0.0		40.9	None	Ô
1/0/2	Off	0	0.0	,	37.9	None	\$
1/0/3	Off	0	0.0	-	37.5	None	\$
1/0/4	Off	0	0.0	-	39.4	None	\$
1/0/5	Off	0	0.0		44.6	None	\$

Switch – Performance – PoE Ports

Switches > C0:74:AD:CC:DF:18 (GWN7813P) > 1/0/1		
Port	1/0/1	
Power Supply Standard	802.3at	~
Power Supply Mode 🛈	Auto Close Force	
Limited Power Mode ①	Class Mode User Mode	
Priority	Highest Second Highest O Lowest	
Power-Off Schedule ①	None	~
	Cancel Save	

Switch – Performance – Edit PoE

• Info

Switches > C0:74	AD:CC:DF	:18 (GWN7	813P)	
Performance	Info	Port	Debug	
	De	vice Info		
	Dev	rice Name		GWN7813P
	Dev	rice Model		GWN7813P
	Upt	Uptime		3h 25min
	Dev	Device System Time		2024-10-18 18:21
				Show more information \sim
	Pol	E Power Su	pply Inform	nation
	PoE	Ports Numbe	er	24
	Tota	al PoE Power	Supply	360W
	PoE	Reserved Po	wer	20W
	Cor	Ifigured Powe	r	OW
				Show more information \checkmark

Switch – Info

• Port

The Port Configuration page enables you to manage and fine-tune the behavior of each port. You can adjust network settings, security controls, VLAN profiles, and more for each individual port. This helps tailor each port's function to the specific needs of your network.

Performance	Info	Port	Debug					
	10Gbps	1000Mbps	100Mbps/10Mbps	Link Down 📕 Abno	rmal Shutdown 🗌 S	hutdown 🗲 PoE Pow	er: UP 🗇 Aggregate @	Mirror
	2 4	6	8 10 12	14 16	18 20	22 24		
	1 3	5	7 9 11	13 15	17 19	21 23 25	26 27 SFP+ SFP+ SFP+	28
								SFP+
Port	Desc	ription	Enable	Link Aggregation	Port Profile	Clients Count	Link Rate	Upload rate
1011			Enabled	None	All VLANs	0	Auto Negotiation	0bps
	-							Ohme
1/0/1			Enabled	None	All VLANs	0	Auto Negotiation	0bps
1/0/1			Enabled	None	All VLANs All VLANs	0	Auto Negotiation	0bps

Switch Port – part 1

Port Details

- Port Enable/Disable: Switches the port on or off.
- **Description**: Option to label the port for easier management.
- Link Aggregation (LAG): Assigns the port to a LAG group to increase throughput or redundancy.
- Port Profile: Selects from existing VLAN profiles or allows profile override for custom configurations.
- Port Mirroring: Mirrors traffic from one port to another for monitoring.
- Trust DHCP Snooping: Improves DHCP security by only allowing trusted DHCP traffic.

Switches > C0:74:AD:CC:DF:1	18 (GWN7813P)			
Performance Info	Port Debug			
10 2 1	Gbps ■ 1000Mbps ■ 100Mbps/10 4 6 8 10 3 5 7 9		 4 PoE Power: UP ↓ Aggregate Mirror 24 25 stPh 26 stPh 27 stPh 28 stPh 	
	Port 1			
	Description	Port_1_Description	0–64 characters, only support input in numbers, letters and special characters.	
	Port Enable		does not support "\7,/	
	Link Aggregation ()	LAG1(0/8) ~		
	LAG Port Profile	All VLANs ~		
	Trust DHCP Snooping()			

Switch Port – part 2

Port Profile Override This section allows custom configuration when the default port profile doesn't fit the requirements.

- Native VLAN: Specifies the VLAN for untagged traffic.
- Allowed VLAN: Defines which VLANs are permitted to pass through.
- Voice VLAN: Prioritizes voice traffic for QoS (Quality of Service).
- Speed Settings: Options include Auto-Negotiation, Full-Duplex, Half-Duplex, and more.
- Flow Control: Determines whether the port will use flow control to manage traffic congestion.

Security Options

• Storm Control:

• Prevents traffic floods (e.g., broadcast, multicast storms) that can degrade network performance by limiting the number of broadcast or multicast packets allowed.

• Port Isolation:

• Restricts communication between devices on the same switch. When enabled, the port can only communicate with uplink ports and is isolated from other local ports for improved security.

• Port Security:

• This feature limits the number of MAC addresses allowed on a port, preventing unauthorized devices from connecting.

• 802.1X Authentication:

• Provides network access control by authenticating devices attempting to connect to the network via this port. Commonly used in environments where device identity and security are important, such as enterprise networks.

	Once enabled, "Port Profile" will be invalid, and the following custo
Port Profile Override	configuration will be applied.
General <u>^</u>	
Native VLAN	1 (Default)
Allowed VLAN	1 (Default)
Voice VLAN	
Speed	Auto Negotiation
Duplex Mode 🛈	Auto Negotiation Full Half
Flow Control	Auto Negotiation Off On When duplex mode is "Half-duplex", the traffic control does not take effect
Security \land	
Port Isolation	

• Debug

For the **Debug** function there are two primary functions:

1. Ping/Traceroute:

- Select a diagnostic tool from the dropdown menu:
 - IPv4 Ping
 - IPv6 Ping
 - IPv4 Traceroute
 - IPv6 Traceroute
- Enter the target IP address or hostname.
- Click **Start** to initiate the diagnostic.
- The diagnostic results will display packet transmission details, round-trip times, and packet loss, as shown.

Switches > C0:74:	AD:CC:D	F:18 (GWN7	/813P)	
Performance	Info	Port	Debug	
Ping / Traceroute	SSH F	emote Acces	s	
	То	bl		IPv4 Ping
	* Tai	get IP Addre	ss / Hostname	IPv4 Ping
	Tu	Bern Maare	557 Hostname	IPv6 Ping
				IPv4 Traceroute
				IPv6 Traceroute
		iagnostic Re	esult	
	F	ING 1.1.1.1	(1.1.1.1): 56	data bytes
			. ,	0 ttl=51 time=40.000 ms
				1 ttl=51 time=30.000 ms
				2 ttl=51 time=140.000 ms
	6	4 bytes fro	m 1.1.1.1: seq=	3 ttl=51 time=30.000 ms
		1.1.1.1	ping statistics	
	4	packets tr	ansmitted, 4 pa	ckets received, 0% packet loss
	r	ound-trip m	in/avg/max = 30	.000/60.000/140.000 ms

Switch Debug - Ping/Traceroute

2. SSH Remote Access:

- Enter the SSH password to start remote access.
- A notification will confirm the remote session, which will terminate automatically after 48 hours.
- To manually end the session, click Stop SSH Remote Access.

Switches > C0:7 4	AD:CC:DI	:18 (GWN78	13P)
Performance	Info	Port	Debug
Ping / Tracerout	e SSH R	emote Access	
			Remote accessing It will automatically stop in 48 hours.
			Stop SSH Remote Access

Switch Debug – SSH Remote Access

Switch Configuration

In this section, you can configure the switch details, manage VLAN interfaces, and set up RADIUS authentication.

Access the Configuration Page:

In the Switch Management -> Switches screen, click the Configuration icon next to the desired switch.

evice Takeover failure, <u>Vie</u>	w details						
Vice Upgrade	Delete • Online	e: 2 • Offline: 0		All Status ~	All device models $\ \sim$	Q. MAC / IP Add	dress / Device Name
Device Model 🗘	MAC Address	Device Name	IP Address	Firmware Version		Clients ≑	Operations
 GWN7813P 	C0:74:AD:CC:DF:18	Grandstream	IPv4:20.0.0.132 IPv6:-	1.0.7.71	7h 42min	2	O C C D
 GWN7813P 	C0:74:AD:DF:CC:94	GWN7813P	IPv4:192.168.80.21 IPv6:-	1 1.0.7.68	6h 44min	2	Configuration
	Device Model \$ GWN7813P	Device Model ÷ MAC Address • GWN7813P • C0:74:AD:CC:DF:18	Device Model ² MAC Address Device Name • GWN7813P • C0:74:AD:CC:DF:18 Grandstream	Device Model + MAC Address Device Name IP Address • GWN7813P • C0:74/AD/CC/DF:18 Grandstream IPv420.00.132 IPv45: • GWN7813P • C0:74/AD/CC/DF:18 Grandstream IPv45: IPv45:	Device Model = MAC Address Device Name IP Address Firmware Version • GWN7813P • C0:74:AD:CC:DF:18 Grandstream IPV4:20.0.0.132 IPV6: 1.0.7.71 • GWN7813P • C0:74:AD:DE:CC:04 GWN7813P IPV4:192.168.80.211 1.0.7.68	Device Model ÷ MAC Address Device Name IP Address Firmware Version System Up Time • GWN7813P • C0:74:AD:CC:DF:18 Grandstream IPv420.00.132 IPv6: 1.0.7.71 7h 42min • GWN7813P • C0:74:AD:CC:DF:18 Grandstream IPv4:192.168.80.211 1.0.7.68 6h 44min	Device Model = MAC Address Device Name IP Address Firmware Version System Up Time Clients ÷ • GWN7813P • C0:74:AD:CC:DF:18 Grandstream IPV420.0.0.132 1.0.7.71 7h 42min 2 • GWN7813P • C0:74:AD:DE:CC:B4 GWN7813P IPV4:192.168.80.211 1.0.7.68 Eh:44min 2

Switch configuration

Edit Switch Details:

The **Switches** \rightarrow **Edit** page (as seen in the second image) allows you to configure:

- Device Name and Remarks
- Device Password
- **RADIUS Authentication**: You can choose to use the **Switch Global Configuration** or define a custom RADIUS setting by selecting from the dropdown or adding a new one by clicking **Add RADIUS Authentication**.

Switches > Edit								
	Device Name	2	Grandstream GWN St	witch		0-64 characters		
	Device Rema	irks	MainSwitch			0~64 characters		
	Device Passv	vord 🛈	•••••		3 ₉₉ 6	8-32 characters, must include any two of numbers, letters and special characters		
	RADIUS Auth	entication	Use Switch Global Co	nfiguration	~			
			Cancel Save					
VLAN Interface								
Add							All Types	~
VLAN ‡	Status	Туре	IPv4 Address	IPv6	IPv6 Link Local Address	IPv6 Global Unicast Address	Operations	
2 (2)	Down	Static	20.0.0.1/24	Disabled	-	-	ľŌ	

Switch configuration – part 2

Manage VLAN Interfaces:

Scroll to the VLAN Interface section where you can:

- Add a VLAN by clicking the Add button.
- Edit existing VLAN entries by clicking the pencil icon.
- View each VLAN's status, type, and IP addresses.

Add/Edit VLAN Interface:

When adding or editing, set the VLAN ID, choose IP settings (Static IP or DHCP), and configure IPv6 if required.

Save Changes:

After making your changes, click Save to apply the configuration.

Switches > Edit VLAN Interface			
*VLAN ①	2 (2)	~	
IPv4 Address Type	Static IP DHCP		
*IPv4 Address / Prefix Length	20.0.0.1	/ 24	Prefix Length range 8~30
IРvб			
	Cancel Save		

Switch configuration – Add/Edit VLAN Interface

Configuration

In the **Global Switch Configuration** section, you can configure settings that affect all switches in your network, ensuring consistent behavior across your entire switch infrastructure. This is distinct from configuring individual switches, as it provides network-wide settings.

Configurable Options:

• RADIUS Authentication:

- Set a RADIUS profile for centralized authentication across switches.
- Voice VLAN:
 - Enable a dedicated VLAN for voice traffic, optimizing voice data flow.
- Multicast:
 - IGMP/MLD Snooping VLAN: Designate VLANs for IGMP and MLD snooping to manage multicast traffic efficiently.
 - Unknown Multicast Packet: Choose how to handle unknown multicast packets (e.g., Flood).

• DHCP Snooping Settings:

- Enable DHCP snooping to prevent unauthorized DHCP servers.
- **802.1x**:
 - Set up guest VLAN for 802.1x-based authentication, securing access to the network.
- Others:
 - Jumbo Frame: Configure the maximum frame size, useful for reducing overhead in high-throughput networks.

Each of these settings is aimed at ensuring your network operates optimally by providing controls that apply universally across all switches under management.

Configuration			
Global Switch Configuration Port Profile			
	RADIUS Authentication		
	RADIUS Profile	RADIUS_1	~
	Voice VLAN		
	VOICE VLAN		
	Voice VLAN		
	Multicast		
	IGMP Snooping VLAN	Please Select IGMP Snooping VLAN	Ŷ
	MLD Snooping VLAN	Please Select MLD Snooping VLAN	~
	Unknown Multicast Packet	Flood	~
	DHCP Snooping Settings		
	DHCP Snooping		
	802.1x		
	Guest VLAN ①		
	Others		
	* Jumbo Frame	9216	
		Const	
		Cancel Save	

Global Switch Configuration

Port Profile

In the **Port Profile** section, you can manage settings that will be applied across multiple switch ports to maintain consistency in configuration. The configuration of port profiles ensures that multiple ports can follow a unified policy or set of rules. Key elements you can configure in this section include:

- Profile Name: Assign a custom name to the port profile for easy identification.
- Native VLAN: Specify the VLAN that will be considered the default for untagged traffic.
- Allowed VLAN: Define which VLANs are allowed on the ports using this profile.
- Voice VLAN: Enable and configure a separate VLAN for voice traffic, if needed.

- $\circ~$ ${\bf Speed}:$ Set the data transmission speed for the port.
- Duplex Mode: Configure the port to operate in full, half-duplex, or auto-negotiation mode.
- Flow Control: Manage the ability to control the data flow for traffic congestion.
- Ingress & Egress: Control the flow of incoming and outgoing traffic.
- LLDP-MED: Enable LLDP-MED to facilitate auto-negotiation for voice and network devices.

• Security Settings:

- Storm Control: Prevent traffic storms on the network.
- Port Isolation: Isolate this port to limit communication with other ports.
- Port Security: Set up port-based security to restrict unauthorized devices.
- 802.1X: Enable 802.1X for port-based network access control.

Configuration			
Global Switch Configuration	Port Profile		
Add Delete			
Profile Name	Native VLAN	Allowed VLAN	Operations
Port_Profile_1	1	1-2	ſ
All VLANs	1	All VLANs	

Configuration > Edit Port Profile			
	General <u>^</u>		
	* Profile Name	Port_Profile_1	1-64 characters
	*Native VLAN	1 (Default)	
	Allowed VLAN	1 (Default) 2 (2) $ imes$	
	Voice VLAN		
	Speed	Auto Negotiation ~	
	Duplex Mode ()	Auto Negotiation O Full O Half	
	Flow Control	Auto Negotiation Off On When duplex mode is "Half-duplex", the traffic control does not take effect.	
	Ingress		
	Egress		
	LLDP-MED		
	Network Policy TLV		
	Security \land		
	Storm Control		
	Port Isolation		
	Port Security ①		
	802.1X		
		Cancel Save	

Switch - Port Profile

Add/Edit – Port profile

ACCESS CONTROL

SafeSearch

The GWN700X routers offer SafeSearch feature on Bing, Google, and Youtube. Enabling this option will hide any inappropriate or explicit search results from being displayed.

SafeSearch		
SafeSearch 🛈	Bing Google YouTube	
	Cancel Save	
	Site Control page	

EXTERNAL ACCESS

By default, all the requests initiated from the WAN side are rejected by the router GWN700x external access features allow hosts located on the WAN side to access the services hosted on the LAN side of the GWN router.

DDNS

Dynamic Domain Name System (DDNS) allows users to map a dynamic IP address to a fixed domain name, making it easier to access devices on networks where the IP address may change. This is especially useful for remote access to networked devices without requiring a static IP.

Grandstream GWN700x routers support DDNS configuration, enabling seamless remote access through a consistent domain name, regardless of IP changes. Key features include:

- Multiple Provider Support: Choose from popular DDNS providers to match your existing account.
- **Public IP Detection**: When positioned behind a NAT, the GWN700x can detect and register the public IP address for accurate DDNS updates.
- **Customizable Update Intervals**: Set the frequency of updates to ensure the DDNS server always has the current IP address.
- Interface Selection: Specify the WAN interface used for DDNS, allowing flexibility in multi-WAN environments.

These features make the GWN700x routers ideal for environments requiring reliable remote access, even in networks with dynamic IP addresses.

DDNS > Add DDNS			
Service Provider	dyndns.org	~	
Enable			
* Username			1~32 characters
*Password		Speel	1~32 characters
* Domain			Please go to dyndns.org to register to get the corresponding username, password
* Interface	WAN1 (WAN)	~	and domain
IP Source ①	WAN IP Public IP		
*Update Interval (Min)①	10		Default 10, range 1~1440
	Cancel Save		



Field	Description
Service Provider	Dropdown selection of available Dynamic DNS providers (e.g., dyndns.org, changeip.com, etc.). Note: Requires registration at the chosen provider's website to obtain the domain, username, and password for DDNS services.

Enable	Toggle to enable or disable the DDNS service for the selected provider.			
Username	Enter the username provided by the DDNS service provider. Range: 1-32 characters.			
Password	Enter the password associated with the DDNS service provider. Range: 1-32 characters.			
Domain	Enter the domain or hostname to be updated by the DDNS service.			
Interface	Select the WAN interface to associate with the DDNS update.			
IP Source	Choose between 'WAN IP' or 'Public IP' for the source of IP to send to the DDNS provider. Default: WAN IP. <i>Note:</i> Use 'Public IP' if behind a NAT to detect and use the device's public IP address for the DDNS update			
Update Interval (Min)	Set the interval in minutes for updating the IP address of the device to the DDNS server. Default: 10. Range: 1-1440. <i>Note: Increasing interval reduces frequency of updates to the DDNS server</i>			

DDNS Page

Port Forward

Port forwarding allows forwarding requested initiated from the WAN side of the router to a LAN host. This is done by configuring either the port only, or the port and the IP address in case we want to restrict the access over that specific port to one IP address. Once the router receives the requested on the IP address, the router will verify the port on which the request has been initiated and will forward the request to the host IP address and the port of the host which is configured as the destination.

Port forwarding can be used in the case when a host on the WAN side wants to access a server on the LAN side.

Navigate to **GWN700x WEB UI** \rightarrow **External Access** \rightarrow **Port Forward**:

Name		1~64 characters
Status		
Protocol Type	● TCP/UDP ○ TCP ○ UDP	
Interface	WAN2 (WAN)	~
Source IP Address ①		
Source Port 🕕		The valid range is 1-65535. You can enter single port or a port range.
Destination Group	Default	~
Destination IP Address		
Destination Port 🕕		The valid range is 1-65535. You can enter single port or a port range.
	Cancel Save	

Port Forwarding page

Refer to the following table for the Port Forwarding option when editing or creating a port forwarding rule:

Name	Enter a name for the port forwarding rule.		
Status	Toggle on/off the rule status.		
Protocol Type	Select a protocol, users can select TCP, UDP or TCP/UDP.		
Interface	Select the WAN port		
Source IP Address	Sets the IP address that external users access to this device. If not set, any IP address on the corresponding WAN port can be used		
Source Port	Set a single or a range of Ports.		
Destination Group	Select VLAN group.		
Destination IP Address	Set the destination IP address.		
Destination Port	Set a single or a range of Ports.		

Port Forwarding page

DMZ

Configuring the DMZ, the router will allow all the external access requests to the DMZ host. This is

This section can be accessed from **GWN700x Web GUI** \rightarrow **External Access** \rightarrow **DMZ**. GWN700x supports **DMZ**, where it is possible to specify a Hostname IP Address to be put on the **DMZ**.

DMZ Name	
1~64 characters	
Status	\bigcirc
Enabling the DMZ host function can fully expose the designate to the Internet.	ed device
Source Group	
Please Select Source Group	~
Destination Group	
Default	~
*DMZ Hostname IP Address	
*DMZ Hostname IP Address	
DMZ Hostname IP Address	

DMZ Page

Enabling the DMZ host function, the computer set as the DMZ host can be completely exposed to the Internet, realizing twoway unrestricted communication.

Refer to the below table for DMZ fields:

DMZ Name	Enter a name for the DMZ rule.	
Status	Toggle on/off the status of the DMZ rule.	

Source Group	Select the interface to allow access to the DMZ host.		
Destination Group	Select the VLAN on which the DMZ host belong.		
DMZ Hostname IP Address Enter the DMZ host IP address.			

DMZ Page

UPnP

GWN700x supports UPnP that enables programs running on a host to configure automatically port forwarding.

UPnP allows a program to make the GWN700x open necessary ports, without any intervention from the user, without making any check.

UPnP settings can be accessed from GWN700x Web GUI \rightarrow External Access \rightarrow UPnP.

UPnP	
UPnP	Once enabled UPnP (Universal Plug and Play), computers in the LAN can request the router to do port forwarding automatically.
Interface	WAN2 (WAN) ~
Destination Group	Default ~
	Cancel Save

UPnP Settings

UPnP	Click on " ON " to enable UPnP. Note : Once enabled UPnP (Universal Plug and Play), computers in the LAN can request the router to do port forwarding automatically
Interface	Select the interface (WAN)
Destination Group	Select the LAN Group

UPnP Settings

When UPnP is enabled, the ports will be shown in the section below. The information shown includes application name, IP address of the LAN host which has requested the opening of the port, the external port number, the internet port number, and the transport protocol used (UDP or TCP).

UPnP Port Forward				
Refresh				
Application Description	IP Address	External Port	Internal Port	Protocol Type
		1		
		No UPnP device		

UPnP – Open Ports

TURN Service

TURN stands for Traversal Using Relays around NAT and it's a network service that helps establish peer-to-peer connections between devices that are behind a NAT or Firewall. Real-time communication like video conferencing, Voice over IP, etc benefit from TURN service to establish connections between peers when the NAT or the Firewall block or modify the traffic.

Navigate to **Web UI** \rightarrow **External Access** \rightarrow **TURN Service**. The service is OFF by default, toggle Status ON to turn on the service. The default TURN Server Port is 3478, also it's possible to add or remove username and password by clicking on "minus" and "Plus" icons.

RN Service				
Status				
*Ports	All WAN ports \times		~	
*TURN Server Port	3478			Default 3478, range 1024~65535
*Username and Password	Username ①	Password 🛈		
	admin	•••••	0×	•
			Add	i 🕒
*TURN Forwarding Port ()	60000	- 60500		Default 60000~60500, range 6000~6553
	Cancel Save			
		10 .		

TURN Service

Note:

- Turn Server port is by default 3478.
- For Turn Forwarding Port: do not modify the forwarding port range unless necessary. Ensure that the ports used by other services do not conflict with the TURN forwarding ports.
- TURN service is a NAT traversal solution for UC in private network and a VoIP media traffic NAT traversal gateway for Grandstream UCM and Wave.

FIREWALL

The Firewall in GWN routers enables the user to secure the network by blocking the most common attacks and allowing for more control over the traffic.

The Firewall section provides the ability to set up input/output policies for each WAN interface and LAN group as well as setting configuration for Static and Dynamic NAT and ALG.

Firewall – Basic Settings

General Settings

• Flush Connection Reload

When this option is enabled and the firewall configuration changes are made, existing connections that had been permitted by the previous firewall rules will be terminated.

If the new firewall rules do not permit a previously established connection, it will be terminated and will not be able to reconnect. With this option disabled, existing connections are allowed to continue until they timeout, even if the new rules would not allow this connection to be established.

Basic Settings			
General Settings	DoS Defence	Spoofing Defence	Rules Policy
Flush Connection	Reload 🛈		
		Cancel Sav	/e
	Firewall Basi	ic Settings	

DoS Defense

Denial-of-Service Attack is an attack aimed to make the network resources unavailable to legitimate users by flooding the target machine with so many requests causing the system to overload or even crash or shutdown.

DoS Defence		
Log		
TCP SYN Flood Attack Defense		
UDP Flood Attack Defense		
ICMP Flood Attack Defense		
ICMP Flood Packet Threshold (packets/s)	1	Default 250, range 1~ <u>10000</u>
ICMP Flood Timeout (sec) ^①	10	Default 10, range 1~65535
ACK Flood Attack Defense		
Port Scan Detection		
Block IP Options		
Block TCP Flag Scan		
Block Land Attack		
Block Smurf		
Block Ping of Death		
Block Trace Route		
Block ICMP Fragment		
Block SYN Fragment		
Block Unassigned Protocol Numbers		
Block Fraggle Attack		
	Cancel Save	

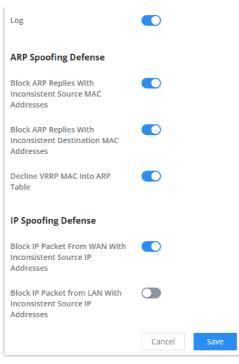
DoS Defense

DoS Defence	Toggle on/off DoS Defence
Log	When this option is enabled, all the attempts of the attacks below will be recorded in a log.
TCP SYN Flood Attack Defense	 When this option is enabled, the router will take counter measures to SYN Flood Attack. TCP SYN Flood Packet Threshold (packets/s): If the threshold of the TCP SYN packets from the Internet has exceeded the defined value, subsequent TCP SYN packets will be discarded within the specified timeout period. TCP SYN Flood Timeout (sec): If the number of TCP SYN packets received per second exceeds the threshold within the specified timeout period, attack defense will start immediately.
UDP Flood Attack Defense	 When this option is enabled, the router will take counter measures to the UDP Flood Attack. UDP Flood Packet Threshold (packets/s): If the threshold of the UDP packets from the Internet has exceeded the defined value, subsequent UDP packets will be discarded within the specified timeout period.

	• UTCP SYN Flood Timeout (sec): If the average number of received UDP packets per second reaches the threshold within the timeout period, attack defense will start immediately.
ICMP Flood Attack Defense	 When this option is enabled, the router will take counter measures to the ICMP Flood Attack. ICMP Flood Packet Threshold (packets/s): If the threshold of the ICMP packets from the Internet has exceeded the defined value, subsequent ICMP packets will be discarded within the specified timeout period. ICMP Flood Timeout (sec): If the average number of received ICMP packets per second reaches the threshold within the timeout period, attack defense will start immediately.
ACK Flood Attack Defense	 When this option is enabled the router will take counter measures to ACK Flood Attack. ACK Flood Packet Threshold (packets/s): If the threshold if the ACK packets from the Internet has exceeded the defined value, subsequent ACK packets will be discarded within the specified timeout period. ACK Flood Timeout (sec): If the average number of received ACK packets per second reaches the threshold within the timeout period, attack defense will start immediately.
Port Scan Detection	 When this option is enabled, the router will take counter measure to the port scanning attempts Port Scan Packet Threshold (packets/s): If the port packets reach the threshold, port scanning detection will start immediately.
Block IP Options	When this option is enabled, the router will ignore any IP packets with Options field.
Block TCP Flag Scan	When this option is enabled, the router will ignore any packets with unexpected information in the TCP flags.
Block Land Attack	When this option is enabled, the router will block any SYN packets which may have been spoofed and modified to set the source and the destination address to the address of the router. If this option is disabled, it might cause the router to be stuck in a loop of responding to itself.
Block Smurf	When this option is enabled, the router will drop any ICMP echo requests.
Block Ping of Death	When this option is enabled, the router will drop any abnormal or corrupted ping packets.
Block Traceroute	When this option is enabled, the router will not allow the traceroute requests initiated from the WAN side.
Block ICMP Fragment	When this option is enabled, the router will drop the ICMP packets which are fragmented.
Block SYN Fragment	When this option is enabled, the router will drop the SYN packets which are fragmented.
Block Unassigned Protocol Numbers	If enabled, the device will reject IP packets receiving IP protocol number greater than 133.
Block Fraggle Attack	If enabled, the router will drop any UDP broadcast packets initiate from the WAN side.
	DoS Defense

Spoofing Defense

Spoofing defense section offers a number of counter-measures to the various spoofing techniques. To protect your network against spoofing, please enable the following measures in order to eliminate the risk of having your traffic intercepted and spoofed. GWN routers offer measures to counter spoofing on ARP information, as well as on IP information.



Spoofing Defense

ARP Spoofing Defense

- Block ARP Replies with Inconsistent Source MAC Addresses: The router will verify the destination MAC address of a specific packet, and when the response is received by the router, it will verify the source MAC address and it will make sure that they match. Otherwise, the router will not forward the packet.
- Block ARP Replies with Inconsistent Destination MAC Addresses: The router will verify the source MAC address and when the response is received. The router will verify the destination MAC address and it will make sure that they match. Otherwise, the router will not forward the packet.
- Decline VRRP MAC Into ARP Table: The router will decline including any generated virtual MAC address in the ARP table.

IP Spoofing Defense

- Block IP Packet From WAN with Inconsistent Source IP Addresses: The router will verify the IP address of the inbound packets, the source IP address has to match the destination IP address to which the request was initially sent to. If there is a mismatch between these two IP addresses, the router will drop the packet.
- Block IP Packet from LAN With Inconsistent Source IP Address: The router will verify the IP address of the packets forwarded. If the router discovers that there is a mismatch in the packet source IP address, the packet will not be forwarded.

Rules Policy

Rules policy allows to define how the router is going to handle the traffic based on whether it is inbound traffic or outbound traffic. This is done per WAN port as well as LAN ports of the router.

Basic Settings > WAN2					
Inbound Policy	Accept	 Reject 	O Drop		
Outbound Policy	 Accept 	🔿 Reject	O Drop		
IP Masquerading					
MSS Clamping					
Log Drop / Reject Traffic					
Drop / Reject Traffic Log Limit	10		second	~	The range is 1~99999999, if it is empty, there is no limit
	Cancel	Save			

Rules Policy

- **Inbound Policy:** Define the decision that the router will take for the traffic initiated from the WAN. The options available are Accept, Reject, and Drop.
- **Outbound Traffic**: Define the decision that the router will take for the traffic initiated from the LAN side. The options available are Accept, Reject, and Drop.
- IP Masquerading: Enable IP masquerading. This will masque the IP address of the internal hosts.
- **MSS Clamping**: Enabling this option will allow the MSS (Maximum Segment Size) to be negotiated during the TCP session negotiation
- Log Drop / Reject Traffic: Enabling this option will generate a log of all the traffic that has been dropped or rejected.

Content Security

The content security feature on GWN700x routers uses DPI (Deep Packet Inspection) to allow users to filter (accept, deny or drop packets) content based on DNS, APP or URL. DNS and URL filtering uses keywords and wildcard * (which can represent any string) while APP filtering works by selecting APPs from a list organized in categories.

For more details about how to block (filter) DNS, APPs and URL, please visit the link below:

documentation.grandstream.com/knowledge-base/gwn700x-firewall-content-security

DNS Filtering

When DNS filtering is enabled, the router will filter the DNS requests initiated by the LAN hosts disallow the requests which match the queries which contains the strings and patterns specified in "Filtered DNS" field. To access DNS filtering, please access the web UI of the router then navigate to **Firewall** \rightarrow **Content Security** \rightarrow **DNS Filtering**.

ontent Security > Add DNS Filtering		
*Name		1~64 characters
Description		0~128 characters
*Filtered DNS ①	Please Enter	
	Add	•
	Cancel Save	

Add DNS Filtering

Name	Enter a name for the filtering rule.
Description	Enter a description for the filtering rule
Filtered DNS	Enter keywords and wildcard characters * (which can represent any string). Wildcard * can only be added before or after the input keyword, for example: *.imag, news*, *news*. Please enter a valid domain name, not an IP address.

Add DNS Filtering

APP Filtering

The user can restrict application(s) from accessing Internet. To restrict applications from accessing internet, please access the web UI of the router then navigate to **Firewall** \rightarrow **Content Security** \rightarrow **APP Filtering** and check the boxes of the applications then click "Save".

tent Security > Add APP Filt	ering		
Basic Information			
*Name			1~64 characters
Description			0~128 characters
Filtered Application			
All Efficiently identifiable	Others		
Collaborative			
Discord Teams	Slack GitLab	Github	Git
Database			
PostgreSQL Oracle	MySQL Redis	MongoDB Cassandra	MsSQL-TDS
E-mail			
POP3 POPS	SMTP SMTPS	IMAP IMAPS	Outlook GMail
File Transfer			
	Cancel Save		

App Filtering

Enter the name of the rule along with the description, then choose the application which will be restricted from accessing the Internet. The user can choose the applications from two categories, "Efficiently Identifiable" application and "Others". The first category can be quickly identifiable from a single network packet, while the second category require multiple packet inspection before the application is identified and blocked.

Note

As the traffic keeps being generated by the applications on the network, the router will identify efficiently. Therefore, the list will be updated continuously.

URL Filtering

The user can restrict accessing to specific URLs by configuring this option. Enter the URL(s) in "Filter URL" field.

Note

Please note that URL Filtering feature is still in beta testing phase.

Content Security > Add URL	Filtering	
*Name		1~64 characters
Description		0~128 characters
*Filtered URL①	Please Enter	
		Add 🕂
	Cancel Save	

Add URL Filtering

Name	Enter a name for the URL Filtering rule.
Description	Enter a description for the URL Filtering rule.

Add URL Filtering

Traffic Rules

GWN700x offers the possibility to fully control incoming/outgoing traffic for different protocols in customized scheduled times and take actions for specified rules such as Accept, Reject and Drop.

Traffic Rules settings can be accessed from **GWN700x Web GUI** → **Firewall** → **Traffic Rules**.

Following actions are available to configure Input, output, and forward rules for configured protocols

- To add new rule, click on "Add" button .
- To edit a rule, click on "Edit" icon .
- To delete a rule, click on "Delete" icon .

Inbound Rules

The Inbound Rules page of the Grandstream GWN router's firewall settings is used to manage and configure the incoming traffic rules for the device. These rules are crucial for controlling which types of traffic are permitted or denied when entering the network through external sources or terminals.

- Accept: To allow the traffic to go through.
- Deny: A reply will be sent to the remote side stating that the packet is rejected.
- Drop: The packet will be dropped without any notice to the remote side.

Alert:

- These inbound rules help define what external traffic can reach the internal network. Proper configuration ensures that necessary communication (such as DHCP and diagnostic pings) is allowed, while potentially harmful or unnecessary traffic can be restricted.
- The presence of a rule like Anti-lockout-Rule is crucial as it prevents administrative lockout, ensuring continued access to the router.
- Rules are sorted by priority, with a lower number indicating higher priority.

nbound R	ules Outbound Rules	Companying Dala							
nbound R	Utbound Rules	Forwarding Rule	5						
	ules are used to control the tr iority of rules is sorted by seria								
Add	Clone Delete	Move to Top						All Source Groups	
No.	Name	Enable	IP Family	Protocol Type	Source Group	Destination Port	Action	Operations	Ξ
✓ 1	WAN1_Allo Defaul		IPv4	UDP	WAN1 (WAN)	68	Accept	≐ ⊠ ⊡	
2	WAN1_Allo Defaul		IPv4	ICMP	WAN1 (WAN)		Accept	≑ ⊠ ⊡	
3	WAN1_Allo Defaul	t 💽	IPv4	IGMP	WAN1 (WAN)		Accept	≑ ⊠ ⊡	
4	WAN1_Allo Defaul	t 💽	IPv6	UDP	WAN1 (WAN)	546	Accept	≑ ⊠ ⊡	
5	WAN1_Allo Defaul	t 💽	IPv6	ICMP	WAN1 (WAN)		Accept	≐ ⊠ ⊡	
6	WAN1_Allo Defaul		IPv6	ICMP	WAN1 (WAN)		Accept	章 ☑ 亩	

Traffic Rules – Inbound Rules page

- **Clone**: You can also duplicate a rule by clicking the "**Clone**" button, allowing you to create a copy that can be easily modified as needed.
- **Move to Top:** the priority of the rules are from the top to bottom, based on the "**No.**" the lower the number, the higher the priority, and the user can priorities any rule by clicking on "**Move to Top**" button giving the rule higher priority.

Traffic Rules > Edit Inbo	und Rule		
	*Name	WAN1_Allow-DHCP-Renew	
	Enable		
	IP Family	Any IPv4 IPv6	
	Protocol Type	UDP	Ý
	*Source Group ()	WAN1 (WAN)	Ý
	Source MAC Address		
	Source Address Type	Select IPv4 Address Group	Ŷ
	Source Address	IPv4 inbound Group	v
	Source Port ()		
	Destination Address Type	Select IPv4 Address	Ŷ
	Destination Address	IPv4 Group	Ŷ
	Destination Port ①	68	
	Schedule	None	~
	Action	Accept Deny Drop	

Traffic Rules – Add/Edit Inbound Rules – Part 1

Advanced Settings (If the Rule action is 'Accept', content security acts as a blocklist and can deny or drop the requests in content security.)					
Content Security					
Content Security Action ()	Accept Deny ODrop				
DNS Filtering	DNS filter \times	~			
APP Filtering	media filter app \times	~			
URL Filtering	url filtering $ imes$	×			
	Cancel Save				

Traffic Rules – Add/Edit Inbound Rules – Part 2

Name	The descriptive name for the rule. This helps identify the rule's purpose at a glance.
Enable	Toggle switch to activate or deactivate the rule.
IP Family	Specifies whether the rule applies to IPv4, IPv6, or both.
Protocol Type	Choose the protocol type. UDP TCP ICMP IGMP All
Source Group	Indicates the source network or interface (e.g., WAN1, WAN2 or VLAN or VPN) from which traffic originates. Note: When "All " is selected, all interfaces will be included, thus this rule has the highest priority, and subsequent new interfaces are automatically included.
Source MAC Address	Option to filter traffic by the MAC address of the source device.

Source Address Type	Specifies the type of source IP address (e.g., Single IP, IP Range, Subnet or a source group like IPv4, IPv6 or FQDN Source Address.
Source Address	Specify the source IP address.
Source Port	To enter multiple port/port ranges, separate them using commas (,), for example:4,5-10.
Destination Address Type	Specifies the type of destination IP address (e.g., Single IP, IP Range, Subnet or a source group like IPv4, IPv6 or FQDN Destination Address.
Destination Address	Specify the destination IP address.
Destination Port	To enter multiple port/port ranges, separate them using commas (,), for example: 4,5-10.
Schedule	Optional field for scheduling when the rule is active (e.g., specific times or days). Note: The absolute date/time set will not take effect in the schedule.
Action	If set to "Accept", the external devices are allowed to access the router; if set to "Deny", the access of the external devices is denied and the result is returned; if set to "Drop", the access request of the external device will be directly droped.
Note: If the Rule action is 'Accept	Advanced Settings pt', content security acts as a blocklist and can deny or drop the requests in content security.
Content Security	Toggle switch to enable or disable content security filtering.
Content Security Action	Defines the action for content security (e.g., Accept, Deny, or Drop).
DNS Filtering	Specifies the DNS filtering profile used for the traffic (e.g., to block malicious domains).
APP Filtering	Selects the application filtering profile for traffic, helping to control or block certain apps.
URL Filtering	Specifies the URL filtering profile for the traffic, used to restrict or permit access to certain URLs.
	Traffic Rules – Inhound Rules

Traffic Rules – Inbound Rules

Outbound Rules

The GWN700x allows to filter outgoing traffic from the local LAN networks to outside networks and apply rules such as:

- Accept: To allow the traffic to go through.
- **Deny:** A reply will be sent to the remote side stating that the packet is rejected.
- **Drop:** The packet will be dropped without any notice to the remote side.

affic Rule										
bound Rule	es Outbound Rules	Forwarding Rule	25							
Outbour	nd rules are used to control th	e traffic that is leaving	g the router and go	ing to external networks	s or devices.					
The prio	rity of rules is sorted by serial	number. The lower th	he number, the high	her the priority.						
The prio	rity of rules is sorted by serial Clone Delete	Move to Top	he number, the high	ter the priority.					All Destination Groups	
			IP Family	Protocol Type	Source Address	Destination Group	Destination Address	Action	All Destination Groups	=

Traffic Rules – Outbound Rules

Traffic Rules > Edit Outbou	nd Rule	
	*Name	Outbound rule example
	Enable	
	IP Family	Any IPv4 IPv6
	Protocol Type	UDP/TCP ~
	Source Address Type	IP Address
	Source Address	192.168.80.6
	Source Port ①	
	* Destination Group ()	WAN2 (WAN)
	Destination Address Type	Select IPv4 Address Group
	Destination Address	IPv4 Group Guest Network
	Destination Port ①	
	Schedule	None
		① The absolute date/time set will not take effect in the schedule
	Action	🔿 Accept 💿 Deny 🔿 Drop

Traffic Rules – Add/Edit outbound Rules – Part 1

Advanced Settings (If the rule action is 'Deny' or 'Drop', content security will act as a allowlist and requests in content security will be accepted)				
Content Security				
Content Security Action 🛈	Accept Deny Drop			
DNS Filtering	DNS Filtering \times	~		
APP Filtering	App Filtering list \times	~		
URL Filtering	URL Filtering \times	~		
	Cancel Save			

Traffic Rules – Add/Edit outbound Rules – Part 2

Name	The descriptive name for the rule. This helps identify the rule's purpose at a glance.
Enable	Toggle switch to activate or deactivate the rule.
IP Family	Specifies whether the rule applies to IPv4, IPv6, or both.
Protocol Type	Choose the protocol type. UDP TCP ICMP IGMP All
Source Address Type	Specifies the type of source IP address (e.g., Single IP, IP Range, Subnet or a source group like IPv4, IPv6 or FQDN Source Address.
Source MAC Address	Option to filter traffic by the MAC address of the source device.
Source Address	Specify the source IP address.
Source Port	To enter multiple port/port ranges, separate them using commas (,), for example:4,5-10.

Destination Group	Indicates the destination network or interface (e.g., WAN1, WAN2 or VLAN or VPN). <i>Note:</i> When "All " is selected, all interfaces will be included, thus this rule has the highest priority, and subsequent new interfaces are automatically included.
Destination Address Type	Specifies the type of destination IP address (e.g., Single IP, IP Range, Subnet or a source group like IPv4, IPv6 or FQDN Destination Address.
Destination Address	Specify the destination IP address.
Destination Port	To enter multiple port/port ranges, separate them using commas (,), for example: 4,5-10.
Schedule	Optional field for scheduling when the rule is active (e.g., specific times or days). <i>Note: The absolute date/time set will not take effect in the schedule.</i>
Action	If set to "Accept", the external devices are allowed to access the router; if set to "Deny", the access of the external devices is denied and the result is returned; if set to "Drop", the access request of the external device will be directly droped.
Note: If the Rule action is 'Acce	Advanced Settings ppt', content security acts as a blocklist and can deny or drop the requests in content security.
Content Security	Toggle switch to enable or disable content security filtering.
Content Security Action	Defines the action for content security (e.g., Accept, Deny, or Drop).
DNS Filtering	Specifies the DNS filtering profile used for the traffic (e.g., to block malicious domains).
APP Filtering	Selects the application filtering profile for traffic, helping to control or block certain apps.
URL Filtering	Specifies the URL filtering profile for the traffic, used to restrict or permit access to certain URLs.
	Traffic Rules – Outbound Rules

Traffic Rules – Outbound Rules

Forwarding Rules

Forwarding rules control traffic flow between different networks (WAN, VLAN or VPN) or devices within a network, allowing administrators to manage access and enforce security policies. Each rule specifies conditions for traffic, such as source and destination groups, protocol types, and actions (e.g., **Accept**, **Deny**, or **Drop**).

Rules are prioritized by serial number—the lower the number, the higher the priority. This order ensures that high-priority rules are applied first, enabling precise control over network traffic and security. Advanced settings, like content and application filtering, offer additional layers of control for accepted traffic.

d Rules Outbound Ru	Iles Forwarding Rul	les						
prwarding rules are used to co	ntrol the traffic forwarded serial number. The lower	between different ne the number, the high	tworks or terminals with er the priority.	in a network.				
in principal and a solution of		and a second sec						
Clone Del	ete Move to Top	1			All Source Groups	~	All Destination Groups	
		_						
No. Name	Enable	IP Family	Source Group	Source Address	Destination Group	Action	Operations	Ξ
WAN1_Allo	efault	IPv6	WAN1 (WAN)	-	All	Accept	≐ □ 前	
	-							
2 WAN2_Allo D	fault	IPv6	WAN2 (WAN)	-	All	Accept	≑ └ 茴	
	Clone Dele Dele Name WAN1_Allo De	e priority of rules is sorted by serial number. The lower to Clone Delete Move to Top Io. Name Enable WAN1_Allo Default	e priority of rules is sorted by serial number. The lower the number, the high Clone Delete Move to Top Io. Name Enable IP Family WAN1_Allo Default I IPv6	e priority of rules is sorted by serial number. The lower the number, the higher the priority. Clone Delete Move to Top Io. Name Enable IP Family Source Group WAN1_Allo Default IP IPv6 WAN1 (WAN)	Clone Delete Move to Top Io. Name Enable IP Family Source Group Source Address WAN1_Allo Default IPv6 WAN1 (WAN) -	e priority of rules is sorted by serial number. The lower the number, the higher the priority. Clone Delete Move to Top All Source Groups Io. Name Enable IP Family Source Group Source Address Destination Group WAN1_Allo Default IPv6 WAN1 (WAN) - All	e priority of rules is sorted by serial number. The lower the number, the higher the priority. Clone Delete Move to Top All Source Groups Io. Name Enable IP Family Source Group Source Address Destination Group Action WAN1_Allo Default IPv6 WAN1 (WAN) - All Accept	e priority of rules is sorted by serial number. The lower the number, the higher the priority. Clone Delete Move to Top All Source Groups Val Destination Groups Io. Name Enable IP Family Source Group Source Address Destination Group Action Operations WAN1_Allo Default IPv6 WAN1 (WAN) - All Accept Image: Close Cl

Traffic Rules – Forward Rules page

Click Add to create a new forwarding rule or Edit (pencil icon) next to an existing rule to modify it.

Traffic Rules > Edit Forwarding F	ule	
	* Name	Forwarding Rule Example
	Enable	
	IP Family	Any IPv4 IPv6
	Protocol Type	UDP/TCP v
	* Source Group ①	Default (VLAN)
	Source MAC Address	
	Source Address Type	Select IPv4 Address Group
	Source Address	IPv4 Group Guest Network
	Source Port ①	
	* Destination Group ()	Guests VLAN20 (VLAN) ×
	Destination Address Type	Select IPv4 Address Group
	Destination Address	IPv4 Group Guest Network
	Destination Port ①	
	Schedule	None
		① The absolute date/time set will not take effect in the schedule
	Action ()	Accept Deny Drop

Traffic Rules – Add/Edit Forward Rules part 1

Advanced Settings (If the Rule action is 'Accept', content security acts as a blocklist and can deny or drop the requests in content security.)					
Content Security					
Content Security Action 🛈	Accept O Drop				
DNS Filtering	DNS Filtering \times	~			
APP Filtering	App Filtering list \times	~			
URL Filtering	URL Filtering \times	~			
	Cancel Save				

Traffic Rules – Add/Edit Forward Rules part 2

Name	The descriptive name for the rule. This helps identify the rule's purpose at a glance.
Enable	Toggle switch to activate or deactivate the rule.
IP Family	Specifies whether the rule applies to IPv4, IPv6, or both.
Protocol Type	Choose the protocol type. • UDP • TCP • UDP/TCP • ICMP • IGMP • All
Source Group	Indicates the source network or interface (e.g., WAN1, WAN2 or VLAN or VPN) from which traffic originates. Note: When "All " is selected, all interfaces will be included, thus this rule has the highest priority, and subsequent new interfaces are automatically included.
Source Address Type	Specifies the type of source IP address (e.g., Single IP, IP Range, Subnet or a source group like IPv4, IPv6 or FQDN Source Address.
Source MAC Address	Option to filter traffic by the MAC address of the source device.

e Port	To enter multiple port/port ranges, separate them using commas (,), for example:4,5-10. Indicates the destination network or interface (e.g., WAN1, WAN2 or VLAN or VPN).	
aation Group	Indicates the destination network or interface (e.g., WAN1, WAN2 or VLAN or VPN). Note: When "All " is selected, all interfaces will be included, thus this rule has the highest priority, and subsequent new interfaces are automatically included.	
nation Address Type	Specifies the type of destination IP address (e.g., Single IP, IP Range, Subnet or a source group like IPv4, IPv6 or FQDN Destination Address.	
nation Address	Specify the destination IP address.	
nation Port	To enter multiple port/port ranges, separate them using commas (,), for example: 4,5-10.	
ule	Optional field for scheduling when the rule is active (e.g., specific times or days). Note: The absolute date/time set will not take effect in the schedule.	
1	If set to "Accept", the external devices are allowed to access the router; if set to "Deny", the access of the external devices is denied and the result is returned; if set to "Drop", the access request of the external device will be directly droped.	
Advanced Settings Note: If the Rule action is 'Accept', content security acts as a blocklist and can deny or drop the requests in content security.		
nt Security	Toggle switch to enable or disable content security filtering.	
nt Security Action	Defines the action for content security (e.g., Accept, Deny, or Drop).	
Filtering	Specifies the DNS filtering profile used for the traffic (e.g., to block malicious domains).	
Filtering	Selects the application filtering profile for traffic, helping to control or block certain apps.	
Filtering	Specifies the URL filtering profile for the traffic, used to restrict or permit access to certain URLs.	

Traffic Rules - Forwarding Rules

Advanced NAT

NAT or Network address translation as the name suggests it's a translation or mapping private or internal addresses to public IP addresses or vice versa, and the GWN routers support both.

- SNAT : Source NAT refers to the mapping of clients IP address (Private or Internal Addresses) to a public one.
- DNAT : Destination NAT is the reverse process of SNAT where packets will be redirected to a specific internal address.

The Firewall Advanced NAT page provides the ability to set up the configuration for Static and Dynamic NAT.

SNAT

Following actions are available for SNAT.

Click on + Add to add the Port Forward rule.

- Click on to \checkmark edit a Port Forward rule.
- Click on to in delete a Port Forward rule.

*Name		1~64 characters
Status		
IP Family	IPv4	
Protocol Type	UDP/TCP v	
*Source IP Address		Enter the IP address/mask length, such as "192.168.122.0/24"
*Rewrite Source IP Address		
Source Port 🕖		The valid range is 1-65535. You can enter a single port or a port range.
Rewrite Source Port ①		The valid range is 1-65535. You can enter a single port or a port range.
*Destination Group	WAN2 (WAN)	
Destination IP Address		Enter the IP address/mask length, such as "192.168.122.0/24"
Destination Port		The valid range is 1-65535. You can enter a single port or a port range.
	Cancel Save	



Refer to the below table when creating or editing a SNAT entry:

Name	Specify a name for the SNAT entry
IP Family	Select the IP version, two options are available: IPv4 or Any.
Protocol Type	Select one of the protocols from dropdown list or All, available options are: UDP/TCP, UDP, TCP and All.
Source IP Address	Set the Source IP address.
Rewrite Source IP Address	Set the Rewrite IP. The source IP address of the data package from the source group will be updated to this configured IP.
Source Port	Set the Source Port
Rewrite Source Port	Set the Rewrite source port.
Destination Group	Select a WAN interface or a VLAN for Destination Group.
Destination IP Address	Set the Destination IP address.
Destination Port	Set the Destination Port

SNAT page

DNAT

The following actions are available for DNAT:

Click on + Add to add the Port Forward rule.

Click on to 📝 edit a Port Forward rule.

Click on to indelete a Port Forward rule.

*Name		1~64 characters
Status		
IP Family	IPv4	
Protocol Type	UDP/TCP ~	
*Source Group	WAN2 (WAN)	
Source IP Address		Enter the IP address/mask length, such as "192.168.122.0/24"
Source Port		The valid range is 1-65535. You can enter a single port or a port range.
*Destination Group	WAN2 (WAN)	
Destination IP Address		Enter the IP address/mask length, such as "192.168.122.0/24"
*Rewrite Destination IP Address		
Destination Port ①		The valid range is 1-65535. You can enter a single port or a port range.
Rewrite Destination Port ①		The valid range is 1-65535. You can enter a single port or a port range.
NAT Reflection		
	Cancel Save	

Advanced NAT – DNAT

Refer to the below table when creating or editing a DNAT entry:

Name	Specify a name for the DNAT entry
IP Family	Select the IP version, three options are available: IPv4, IPv6 or Any.
Protocol Type	Select one of the protocols from dropdown list or All, available options are: UDP, TCP, TCP/UCP and All.
Source Group	Select a WAN interface or a LAN group for Source Group, or select All.
Source IP Address	Set the Source IP address.
Source Port	Set the Source Port.
Destination Group	Select a WAN interface or a LAN group for Destination Group, or select All. Make sure that destination and source groups are different to avoid conflict.
Destination IP Address	Set the Destination IP address.
Rewrite Destination IP Address	Set the Rewrite Destination IP Address.
Destination Port	Set the Destination Port.
Rewrite Destination Port	Set the Rewrite Destination Port
NAT Reflection	Click on " ON " to enable NAT Reflection
NAT Reflection Source	Select NAT Reflection either Internal or External.

Advanced NAT – DNAT

ALG

ALG stands for **Application Layer Gateway**. Its purpose is to prevent some of the problems caused by router firewalls by inspecting VoIP traffic (packets) and if necessary modifying it.

Navigate to	Web GUI →	$\textbf{Firewall} \rightarrow$	ALG to	activate A	ALG.
-------------	-----------	---------------------------------	--------	------------	------

ALG	
SIP Protocol	Support SIP packets in both TCP and UDP.
RTSP Protocol	Support RSTP packets only in TCP.
	Cancel Save
	ALG

CAPTIVE PORTAL

Captive Portal feature on GWN700x helps to define a Landing Page (Web page) that will be displayed on Wi-Fi clients' browsers when attempting to access the Internet. Once connected Wi-Fi clients will be forced to view and interact with that landing page before Internet access is granted.

The Captive Portal feature can be configured from the GWN700x Web page under "Captive Portal".

Policy

Users can customize a portal policy on this page. Click on "**Add**" button to add new policy or click on "**Edit**" to edit previously added one.

Policy			
Add Delete			
Policy Name	Splash Page	Client Expiration	Operations
Clients policy	Internal(Clients splash page)	2d	C Ū



* Policy Name	Clients policy	1~64 character
Splash Page	Internal External	
* Client Expiration ①	2 Day 0 Hour 0 Min	
Client Idle Timeout (Min) 🛈	999	Range 5~1440
Daily Limit	When enable, the client is only allowed to access once a day.	
*Splash Page Customization	Clients splash page ~	
* Login Page ①	Redirect to the original URL ~	
HTTPS Redirection ①		
Secure Portal ①		
Pre Authentication Rule(s) 🛈	Choose Destination v	
	Ad	d 🕀
Post Authentication Rule(s)	Choose Destination ~	
	Ad	d 🕀

The policy configuration page allows for adding multiple captive portal policies which will be applied to SSIDs and contain options for different authentication types.

Policy Name	Enter a policy name.
Splash Page	• Internal • External
Client Expiration	Specify the expiration time for client network connection. Once timed out, client should re-authenticate for further network use.
Client Idle Timeout (min)	Specify the idle timeout value for guest network connection. Once timed out, guest should re- authenticate for further network use.
Daily Limit	When enable, the client is only allowed to access once a day.
Splash Page Customization	Select the customized splash page.
Login Page	Set portal authentication through the page to automatically jump to the target page.
HTTPS Redirection	If enabled, both HTTP and HTTPS requests sent from stations will be redirected by using HTTPS protocol. And station may receive an invalid certification error while doing HTTPS browsing before authentication. If disabled, only the http request will be redirected.
Secure Portal	If enabled, HTTPS protocol will be used in the communication between STA and router. Otherwise, the HTTP protocol will be used.
Pre Authentication Rule (sec)	Set pre authentication rules, allowing clients access some URLs before authenticated successfully.
Post Authentication Rule (sec)	Set post authentications to restrict users from accessing the following addresses after authenticating successfully.

Policy page

Splash Page

The splash page allows users with an easy-to-configure menu to generate a customized splash page that will be displayed to the users when trying to connect to the Wi-Fi.

On this menu, users can create multiple splash pages and assign each one of them to a separate captive portal policy to enforce the select authentication type.

The generation tool provides an intuitive "WYSIWYG" method to customize a captive portal with a very rich manipulation tool.

To add a splash page, click on "Add" button or click on "Edit" icon to edit previously added one.

Splash Page		
Add		
8:41 all 🗢 🖬		
2		
Welcome to GWN7002		
Login for free		
ScceptTerms of Use		
Clients splash page 🗾 🔟		
	© 2023 Grandstream Networks, Inc. Gra	andstream Software License Agreement

Splash Page

Users can set the following:

- **Authentication type**: Add one or more ways from the supported authentication methods (Simple Password, Radius Server, For Free, Facebook, Twitter, Google and Voucher).
- Set up a picture (company logo) to be displayed on the splash page.
- **Customize** the layout of the page and background colors.
- Customize the Terms of use text.
- Visualize a preview for both mobile devices and laptops.

Splash Page > Edit Splash Page		Clients splash	n page	Cancel	Save
Basic Components Image Text Text Text	5		Layout Background Color Background Image		~
Logging Components For Free Simple Password	Welcome to GWN7002 8		Click to u	upload Image	
RADIUS Server			Cover		¥
✓ Facebook	Login with RADIUS				
✓ Twitter	Login with Facebook				
✓ Google	Login with Twitter				
Voucher	Login with Google				
	Login with voucher				
	Accept Terms of Use				

Add/edit a Splash page

Guests

This page displays information about the clients connected via Captive portal including the MAC address, Hostname, Authentication Type, etc.

To export the list of all guests, please click on "Export Guest List" button, then an EXCEL file will be downloaded.

Export Guest List					Q	Search MAC / Hostname / SSID
MAC Address	HostName	Authentication Type	Login Time 🗦	Expire Time 🗘	Status	Operations
8:F4:08:3B:62:FD	Ain				Unauthorized	MAC Address
02:3C:5D:0E:E3:EF	Unknown device	For Free	2023-10-05 15:52:31	2023-10-07 15:52:31	Authenticated	 HostName Associated Device
					Total: 2	 SSID Used Traffic Authentication Type Login Time IP Address Expire Time Status

Guest Page

Vouchers

Voucher feature will allow clients to have internet access for a limited duration using a code that is randomly generated from platform controller.

As an example, a coffee shop could offer internet access to customers via Wi-Fi using voucher codes that can be delivered on each command. Once the voucher expires the client can no longer connect to the internet.

Note that multiple users can use a single voucher for connection with expiration duration of the voucher that starts counting after first successful connection from one of the users that are allowed.

Another interesting feature is that the admin can set data bandwidth limitation on each created voucher depending on the current load on the network, users' profile (VIP customers get more speed than regular ones etc....) and the internet connection available (fiber, DSL or cable etc....) to avoid connection congestion and slowness of the service.

Click on "Add" button to create a voucher group.

up, please add first
7

Voucher page

Please refer to the figure below when filling up the fields.

*Voucher Group Name	Guests Voucher		1-64 characters
*Quantity()	10		Range 1~100
*Max Devices()	1		Range 1~5
Byte Limit	10	MB ~	Range 1~1024
Allocation Method 🛈	Per Voucher Per Device		
*Duration()	2 Day 0 Hour 0	Min	
*Validity Time (days)	30		Range 1~365
Maximum Upload Rate	10 Mbps ~		The range is 1~1024, if it is empty, there i no limit
Maximum Download Rate	20	Mbps v	The range is 1~1024, if it is empty, there i no limit
Description	Guests voucher		0~128 characters

Add/Edit Voucher

Note:

Clients connected trough captive portals including vouchers will be listed on the Guests page under **Captive Portal** → **Guests**.

MAINTENANCE

GWN700x offers multiple tools and options for maintenance and debugging to help further troubleshooting and monitoring the GWN700x resources.

TR-069

It is a protocol for communication between CPE (Customer Premise Equipment) and an ACS (Auto Configuration Server) that provides secure auto-configuration as well as other CPE management functions within a common framework.

TR-069 stands for a "Technical Report" defined by the Broadband Forum that specifies the CWMP "CPE WAN Management Protocol". It commonly uses HTTP or HTTPS as transport for communication between CPE and the ACS. The message exchange is using SOAP (XML_RPC) for configuration and management of the device.

Important Note

Once populated, the AP you initially managed will be taken over by TR-069 (Configuration via DHCP Option 43 remains unaffected). If left blank, the ACS source address in DHCP Option 43 will be used, allowing the AP to continue being managed by you.

TR-069		
TR-069		
ACS URL		
	Once filled in, the AP you originally managed will be taken over by TR669, (Configuration via DHCP Option43 is not affected) If empty, the ACS source address in DHCP Option 43 will be used and the AP will continue to be managed by you.	
ACS Username		
ACS Password	h _{rt} i	
Periodic Inform	If enabled, the router will send connection inform packets to ACS regularly.	
* Periodic Inform Interval (sec)	86400	Default 86400
Connection Request Username ()		
Connection Request Password 🛈	hyd	
* Connection Request Port ①	7547	Default 7547, range 1~65535
CPE Cert File 🛈		
CPE Cert Key 🕥		
	Cancel Save	

TR-069 page

TR-069	Enable/disable TR-069 TR-069 is enabled by default.
ACS URL	Enter the FQDN or the IP address of the ACS server. Note: If it is empty, the ACS source address in DHCP Option 43 is preferred.
ACS Username	Enter the username.
ACS Password	Enter the password.
Periodic Inform	If enabled, the router will send connection inform packets to ACS regularly.
Periodic Inform Interval (sec)	This configures the time duration between each inform sent by the device to the ACS server. <i>Default is 86400.</i>
Connection Request Username	When ACS server sends a connection request to the router, the username that the router authenticates ACS must be consistent with the configuration of ACS side.
Connection Request Password	The password that the router authenticates ACS must be consistent with the configuration of ACS server.
Connection Request Port	The port for ACS to send connection request to the router. This port cannot be occupied by other device features. <i>Default is 7547.</i>
CPE Cert File	Enter the certificate that the router needs to use when connecting to ACS through SSL.
CPE Cert Key	Enter the certificate key that the router needs to use when connecting to ACS through SSL.

TR-069 page

SNMP

GWN700x routers support SNMP (Simple Network Management Protocol) which is widely used in network management for network monitoring for collecting information about monitored devices.

To configure SNMP settings, go to **GWN700x Web GUI** \rightarrow **Maintenance** \rightarrow **SNMP**, in this page the user can either enable SNMPv1, SNMPv2c, or enable SNMPv3, and enter all the necessary parameters.

SNMP		
SNMPv1, SNMPv2c		
*Community String	public	1~512 characters
SNMPv3		
*Username		1~128 characters
Authentication Mode	● MD5 ○ SHA	
*Authentication Key	, in the second s	8~32 characters
Encryption Mode	• DES AES128	
*Encryption Key		8~32 characters
	Cancel Save	
	© 2023 Grandstream Networks, Inc. Grandstream Software License Agreem	ent

SNMP

To configure SNMPv1 or SNMPv2, please refer to the table below:

SNMPv1, SNMPv2	Enable/disable SNMPv1 and SNMPv2
Community String	Enter the shared password of the community. Note:

SNMP – SNMPv1 or SNMPv2

To configure SNMPv3, please refer to the table below:

SNMPv3	Enable/disable SNMPv3.
Username	Enter a username.
Authentication Mode	Select the algorithm used for the authentication.
Authentication Key	Select the authentication password.
Encryption Mode	Select the encryption protocol used for the encryption of the data.
Encryption Key	Enter the encryption key.

Backup and Restore

The GWN700x configuration can be backed up (e.g., when performing a firmware update), the configuration can be uploaded to the router by clicking on "**Import**" and selecting the back up file. This will load the backed up configuration back into the router quickly.

If the user wish to modify the configuration file before importing, then a **GWN Router Configuration Tool** can be used to make the necessary modifications to the configuration file. The tool is supported on Windows[®] and Linux environments. To download the tool: GWN Router Configuration Tool, then download the Windows[®] or Linux version accordingly.

Please, visit this guide on how to use the GWN Router Configuration Tool User Guide.

If the user wants to reset the device to its initial configuration, he/she can click one "Factory Reset".

Warning

Resetting the device to its factory settings will wipe all the configuration in the router and it cannot be restored unless the user has previously backed up the configuration. Please back up the configuration before performing a factory reset if you wish to keep a copy of your configuration.

Backup & Restore
Backup
Export the current configuration file of the router to your computer or connected USB device. Once you need to restore this, you can directly import the file.
Export
Restore
The router can be restored according to the imported configuration file. If restore failed and the device cannot be used, please press and hold the Reset button on the back of the router for 5 seconds to restore the factory status.
Import
Factory Reset Configuration
After factory reset, all router's configurations will be reset to the factory settings. Please do it with caution! It is recommended that you backup the current configurations before factory reset.
Factory Reset

Backup and Restore

System Diagnostics

Many debugging tools are available on GWN700x's Web GUI to check the status and troubleshoot GWN700x's services and networks.

To access these tools navigate to "Web UI -> System Settings -> System Diagnosis"

Ping/Traceroute/NSlookup

• Ping

The **Ping** tool is used to test connectivity between the router and a specific target IP address or hostname. It sends a series of packets to the destination and measures the time taken for the packets to return, providing useful information about network latency and connectivity.

- Tool: Select "Ping" from the dropdown.
- IP Family: Choose between IPv4 or IPv6.
- Target IP Address / Hostname: Enter the IP address or hostname you want to ping.
- Interface: Select the network interface (e.g., WAN1, WAN2) through which the test will be conducted.

Click **Start** to begin the test. The **Diagnostic Result** will display the round-trip time for each packet and the overall packet loss, if any.

Ping / Traceroute / NSlookup	Core File Capture	One-click Debug External Syslog	ARP Cache Table Link Tra	cing Tabl
*Tool		Ping	v	
* IP Famil	ly	IPv4	~	
*Target I	IP Address / Hostnam	e 1.1.1.1		
Interfac	ce	WAN1 (WAN)	~	
		Start		
Diagr	nostic Result	Start		
PING	1.1.1.1 (1.1.1.1);	56 data bytes		
PING 64 by 64 by 64 by	1.1.1.1 (1.1.1.1); tes from 1.1.1.1; tes from 1.1.1.1; tes from 1.1.1.1;	56 data bytes seq=0 ttl=52 time=21.502 ms seq=1 ttl=52 time=20.980 ms seq=2 ttl=52 time=21.211 ms		
PING 64 by 64 by 64 by 64 by	1.1.1.1 (1.1.1.1); tes from 1.1.1.1; tes from 1.1.1.1; tes from 1.1.1.1; tes from 1.1.1.1;	56 data bytes seq=0 ttl=52 time=21.502 ms seq=1 ttl=52 time=20.980 ms		
PING 64 by 64 by 64 by 64 by 64 by	1.1.1.1 (1.1.1.1): ttes from 1.1.1.1: ttes from 1.1.1.1: ttes from 1.1.1.1: ttes from 1.1.1.1: ttes from 1.1.1.1: ttes from 1.1.1.1:	56 data bytes seq=0 ttl=52 time=21.502 ms seq=1 ttl=52 time=20.980 ms seq=2 ttl=52 time=21.211 ms seq=3 ttl=52 time=21.422 ms seq=4 ttl=52 time=20.994 ms		

Ping

• Traceroute

The **Traceroute** tool identifies the path that packets take from the router to a specified destination. It lists each hop (intermediate routers) along the way and measures the time taken for the packets to reach each hop.

- Tool: Select "Traceroute" from the dropdown.
- IP Family: Choose between IPv4 or IPv6.
- Target IP Address / Hostname: Enter the IP address or hostname for tracing the route.
- Interface: Choose the network interface to send the traceroute request.

Click **Start** to initiate the traceroute. The **Diagnostic Result** will display each hop along the route to the target, along with the response times for each hop.

System Diagnostics					
Ping / Traceroute / NSlookup	Core File Capture	One-click Debug	External Syslog	ARP Cache Table	Link Tracing Table
*Tool		Traceroute			~
*IP Fai	mily	IPv4			~
* Targe	et IP Address / Hostname	grandstream.c	om		
Inter	face	WAN1 (WAN)			~
		Start			
Dia	agnostic Result				
1 2 3 4 4 5 6 7 7 8 9 10 11 12 13 14 15	Ceroute to grandstream.c 192.168.6.1 0.687 ms 197.247.64.3 3.682 ms 172.20.1.53 5.172 ms 10.43.82.206 4.758 ms 10.43.250.213 21.619 m 154.54.61.129 25.420 m 154.54.485.241 100.037 154.54.485.241 100.037 154.54.490.58 100.566 m 154.24.90.58 100.566 m 154.24.30.471 101.045 38.122.244.34 99.015 m 108.175.172.10 183.994 *	IS IS IS IS IS IS IS IS IS IS	8), 25 hops max, 3	18 byte packets	

Traceroute

• NSlookup

The **NSlookup** tool is used to query DNS servers for domain name resolution. It retrieves the IP address associated with a domain name or vice versa, helping to diagnose DNS-related issues.

- Tool: Select "NSlookup" from the dropdown.
- **Domain**: Enter the domain name you want to query (e.g., "grandstream.com").

• Interface: Select the interface to use for the DNS lookup.

Click **Start** to run the query. The **Diagnostic Result** will display the DNS server queried, along with the resolved IP address or any error if the domain cannot be found.

System Diagnostics							
Ping / Traceroute / NSlooku	Core File	Capture	One-click Debug	External Syslog	ARP Cache Table	Link Traci	ing Table
*т.	ool		NSlookup			~	
* D	omain		grandstream.c	om			
Ir	nterface		WAN1 (WAN)			~	
			Start				
	Diagnostic Resul	t					
	Server: Address:	8.8.8.8 8.8.8.8#53	E.				
	Non-authoritati Name: grandst Address: 38,154	ream.com					
	Non-authoritati	ve answer:	.com: No answer				

NSlookup

Core File

When a crash event happens on the unit, it will automatically generate a core dump file that can be used by the engineering team for debugging purposes.

System Diagnost	ics						
Ping / Traceroute	Core File	Capture	External Syslog	ARP Cache Table	Link Tracing Table	Network Diagnostics	PoE Diagnostics
Refresh							
File Name					Last Moo	dified O	perations
				No Core File			
		© 2	023 Grandstream Netw	orks, Inc. Grandstream	Software License Agreemer	nt	

Core File

Capture

This section is used to capture packet traces from the GWN700x interfaces (WAN ports and network groups) for troubleshooting purposes or monitoring. It's even possible to capture based on MAC address or IP Address, once done the user can click on Start Capture and the file (CAP) will start downloading right away.

ng / Traceroute Core File Ca	pture External Syslog ARP Cache Table Link Tracing T	Table Network Diagnostics PoE Diagnostics
Capture Duration (min)	10	v
Interface	WAN2 (WAN)	~
Capture Rule	Default Rules Custom Rules	
Protocol	Please Select Protocol	\sim
MAC Address		
IP Address		
	Start Capturing	
	© 2023 Grandstream Networks, Inc. Grandstream Software License	

Capture

External Syslog

GWN700x routers support dumping the Syslog information to a remote server under Web GUI \rightarrow System Settings \rightarrow System Diagnosis \rightarrow External Syslog Tab

Enter the Syslog server Hostname or IP address and select the level for the Syslog information. Nine levels of Syslog are available: None, Emergency, Alert, Critical, Error, Warning, Notice, Information and Debug.

System Diagnostics				
Ping / Traceroute Core File Captu	e External Syslog ARP Cache Table Link Tr	acing Table Ne	etwork Diagnostics	PoE Diagnostics
Syslog Server Address				
Syslog Level	4-Warning	~		
Protocol	• UDP TCP			
Target Devices	Select All			
	C0:74:AD:BF:AF:50			
	Cancel Save			
	© 2023 Grandstream Networks, Inc. Grandstream Software L	License Agreement		

External Syslog

ARP Cache Table

GWN700X router keeps an ARP table record of all the device which have been assigned an IP address from the router. The record will keep the devices information when the device is offline. To access the ARP Cache Table, please navigate to **System Diagnostics** \rightarrow **ARP Cache Table**

P Address	120 Cancel Save		Default 120, range 5~300
P Address]		
P Address	MAC Address		
P Address	MAC Address		
192.168.5.127		HostName	Interface
	1.00.000		WAN2 (WAN)
192.168.5.154	0.000	-	WAN2 (WAN)
192.168.5.112	100 010 010	-	WAN2 (WAN)
192.168.5.75	1.00		WAN2 (WAN)
192.168.5.147	Contractor (Sector)		WAN2 (WAN)
192.168.5.1	1000000000	-	WAN2 (WAN)
192.168.5.117	100 M (0.000 M)		WAN2 (WAN)
192.168.80.2	100 x 10 x 10 x 10	Unknown device	VLAN 1

ARP Cache Table

Link Tracing Table

Link Tracing Table shows the flow of traffic by displaying the source IP address/Port (the green color) and the reply IP address/port (the blue color), also other information can be displayed like IP Family, Protocol Type, Life Time, Status, Packets/Bytes etc.

Users/Administrators can also delete the flow of certain IP addresses/Ports (Source and Destination) or then click on "**Delete**" button to clear the link tracing statistic.

Ping / Traceroute	Core File	Capture	Externa	al Syslog ARP	Cache Table	Link T	racing Table	Network [Diagnostics	PoE Diagnostics
Link Trac	king Upper Limit	0	16384					Default <u>163</u>	84,range 16384~;	32768
			Cancel	Save						
Refresh -	Source — Repl	у								
All IP families	 Please En 	ter Sou	Please	Enter Des	All Protocols	~	Please Enter S		lease Enter De	es Q 🔟
P Family	Protocol Type	Life Time	Mark	Status	Flow				Packe	ts / Bytes
Pv4	ICMP	9	255		192.168.5.99[192.168.5.99[→ 1/8 ← 1/8	
Pv4	ICMP	19	255		192.168.5.99[192.168.5.99[→ 1/8 ← 1/8	
Pv4	ТСР	299	255	ESTABLISHED	127.0.0.1[359	96]≓	127.0.0.1[5303]		→ <u>12/</u> ← <u>21/</u>	
Pv4	-	594	255		192.168.80.1[22	4.0.0.120[]		→ 4/3 ← 0/0	
Pv4	UDP	56	2		192.168.80.1[14]≓	255.255.255.255	5[14]	→ 5/2 ← 0/0	
Pv4	ICMP	29	255		192.168.5.99[192.168.5.99[→ 1/8 ← 1/8	
Pv4	ТСР	299	2	ESTABLISHED	192.168.5.147	[5776	0]≓192.168.5.9	99[443]	→ <u>11/</u> ← <u>21/</u>	
Pv4	ТСР	296	2	ESTABLISHED	192.168.5.99[56810]≓44.230.213.2	222[443]	→ <u>15/</u> ← <u>11/</u>	
								Total: 8	_	> 10 / page

Link Tracing Table

Network Diagnostics

Network diagnostics feature allows the user to quickly diagnose the connection link on a specific WAN interface.

System Diagnostics						
Ping / Traceroute Core F	ile Capture	External Syslog	ARP Cache Table	Link Tracing Table	Network Diagnostics	PoE Diagnostics
Interface		WAN2 (WAN)		~		
IP Family		Any IPv4	O IPv6			
		Start				
Diagnostic Result	:					
			No diagnostic record	d		
	C	0 2023 Grandstream Net	tworks, Inc. Grandstream	Software License Agreemer	ıt	

Network Diagnostics

PoE Diagnostics

PoE diagnostics page offers an insight about the ports and their components as well as the power used and the temperature. The information provided can be useful when the user encounters an issue with the PoE function of the GWN700X router.

Note

GWN7001 router does not support PoE.

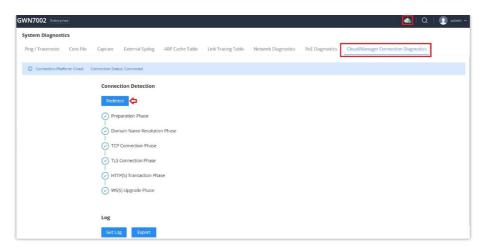
ystem Diagnost	ics						
Ping / Traceroute	Core File	Capture	External Syslog	ARP Cache Table	Link Tracing Table	Network Diagnostics	PoE Diagnosti
Diagnost	ic Result						С
Common i	nformation:						
Input	Power Supply	/ Туре	:PoE+				
PSE In	put Voltage		:51.90	V			
PSE In	put Voltage	Status	:Highe	r Than 65V			
PMAX F	ower		:12.80	W			
Over L	oad Power St	tatus	:Norma	1			
Juncti	on Temperatu	ure	:46.0	°C			
Over T	emperature S	Status	:Norma	1			
Port5	MOSFET Statu	15	:Norma	1			
Port6	MOSFET Statu	15	:Norma	1			
Port5 in	formation:						
Port5	Operation Mo	ode	:Auto	Mode			
Port5	Voltage		:51.90	V			
Port5	Current		:0.0 m	Α			
Port5	Power		:0.0 m	W			
Port5	Current Limi	it Status	:Norma	1			
Port5	Threshold Ov	/er Current T	imeout :Norma	1			
Port5	Output Power	Status	:Wrong				

PoE Diagnostics

Cloud/Manager Connection Diagnostics

If the GWN700x router is added to the GDMS Networking or GWN Manager, it will display a Cloud icon with a green check mark (as shown in the figure below) indicating it's added to either GDMS Networking or GWN Manager.

In case there is an issue with the connection, then the user can navigate to **Maintenance** \rightarrow **System Diagnosis** \rightarrow **Cloud/Manager Connection Diagnostics** and then click on "**Detection**" or "**Redetect**" button to see in what stage/step the connection has failed.



Cloud/Manager Connection Diagnostics

Note:

- The GWN700x router can detect its public IP address even when situated behind another router.
- Support GDMS Networking/GWN Manager connection detection across multiple links.

Upgrade

Under **Maintenance** \rightarrow **Upgrade**. The user has the option to upgrade the GWN router via manual upload (a bin file) or via network either HTTP/HTTPS or TFTP or even schedule to upgrade in a specific time.

Please refer to the figure below:

Upgrade			
	Current Version: 1.0.4.6		
	Upgrade via Manual Upload		
	Upload firmware file to update	Select a file to upload	Extension name: bin
	Upgrade via Network		
	Firmware Upgrade Mode	нттр	~
	* Firmware Server Path 🛈	fm.grandstream.com/gs	
	Allow DHCP Option 43 and 66 to Override Server ①		
	Check/Download New Firmware at Bootup ①		
	Upgrade Based on Schedule		
	* Schedule	Upgrade Schedule	~
		Cancel Save Detect new version	

Upgrade page

Alerts & Notifications

Alerts

Alerts page displays alerts about the network, the user can specify to display only certain types like (**System, Performance, Security or Network**) or the levels. To check the alerts which have been generated, please navigate to **Maintenance** \rightarrow **Alerts & Notifications page** \rightarrow **Alerts tab.**

The alerts can be displayed either by type or levels. However, that is not the only way to display them. The user can filter through the alert log using a date interval or search by MAC address or device name.

Alerts Types

The available types are System, Performance, Security, Network, or the user can choose to display all the types.

lerts & Notifications			Alert N	Notification Setting	s 📑 E-mail Notification Setting
Alerts E-mail Notifications					
Delete All Mark All as Read Export	Start date 🛁 End date	₿	All Alert Types 🧄 🔨	All Levels 🛛 🗸	Q Search Details / Device nam
Details			All Alert Types	Level	Time
Router WAN1(Port 4) cannot connect to network, please	check your network connection: Track	IP ping fa.	System Alert Performance Al	Warning	2023/10/06 09:01
Router(c074adbfaf50) upgraded failed: No firmware in se	erver path		Security Alert	Warning	2023/10/05 18:01
 Router WAN1(Port 4) DHCP service has detected a failure 	3		Network Alert	Emergency	2023/10/05 18:01

Alerts Types

Alerts Levels

The user can filter the alert level by the following levels: All Levels, Emergency, Warning or Notice.

lerts & N	lotifications	log Alert	Notification Settings	E-mail Notification Setting
Alerts	E-mail Notifications			
	Delete All Mark All as Read Export Start date → End date ⊟	All Alert Types 🛛 🗸	All Levels 🔷 🔨	Q Search Details / Device nam
	Details	Alert Type	All Levels	Time
•	Router WAN1(Port 4) cannot connect to network, please check your network connection: Track IP ping fa	Network Alert	Emergency Warning	2023/10/06 09:01
•	Router(c074adbfaf50) upgraded failed: No firmware in server path	System Alert	Notice	2023/10/05 18:01
•	Router WAN1(Port 4) DHCP service has detected a failure	Network Alert	Emergency	2023/10/05 18:01

Alerts Levels

Alert Notification Settings

To enable the notifications on the Alerts tab, please click on "Alert Notification Settings" button as shown below:

Alerts & N	lotifications	🕸 Alert N	lotification Setting	E-mail Notification Setting
Alerts	E-mail Notifications	-		
	Delete All Mark All as Read Export Start date Image: All date Image: All date	All Alert Types 🛛 🗸	All Levels \sim	Q Search Details / Device nam.
	Details	Alert Type	Level	Time
•	Router WAN1(Port 4) cannot connect to network, please check your network connection: Track IP ping fa	Network Alert	Warning	2023/10/06 09:01
•	Router(c074adbfaf50) upgraded failed: No firmware in server path	System Alert	Warning	2023/10/05 18:01
	Router WAN1(Port 4) DHCP service has detected a failure	Network Alert	Emergency	2023/10/05 18:01

Alert Notification Settings

The figures below show all the possible alerts notifications that the user can enable on the Alerts tab, organized into 4 categories: **System** Alert, **Performance** Alert, **Security** Alert and **Network** Alert.

Please refer to the figures below:

Alerts & Noti	fications > Alert Notification Set	ttings	
O Please se	lect the alert content that needs to be notifi	ed. For email configuration, ple	ase go to [System Settings>Email Settings]
System Alert	Performance Alert Security A	lert Network Alert	
	Admin Password Change Alert ()	System notifications	E-mail Notifications
	Upgrade Alert ①	System notifications	E-mail Notifications
	Temperature High Alert ()	System notifications	E-mail Notifications
	The time of the taken-over device is not synchronized ()		E-mail Notifications <u>Settings> Basic Settings</u>) to enable The Taken Over Device* to avoid asynchrony.
	Pairing/Unpairing/Taking Over AP Alert	System notifications	E-mail Notifications
	AP Online Alert ①	System notifications	E-mail Notifications
	AP Offline Alert	System notifications	E-mail Notifications
		Cancel Save	

Alert Notification Settings - part 1

	fications > Alert Notification S	0	ease go to [System Settings>Email Setting
System Alert	Performance Alert Security		aase go to (<u>system setungs>cmail setung</u>
	Memory Usage Alert 🛈	System notifications	E-mail Notifications
	CPU Usage Alert ①	System notifications	E-mail Notifications
	Client Throughput Alert ()	System notifications	E-mail Notifications
	WAN Port Throughput Alert ①	System notifications	E-mail Notifications
		Cancel Save	

Alert Notification Settings – part 2

Alerts & Noti	fications > Alert Notif	ication Settin	igs	
 Please se 	lect the alert content that nee	eds to be notified. I	For email configuration, ple	ase go to [System Settings>Email Settings]
System Alert	Performance Alert	Security Alert	Network Alert	
	DoS attack defense ale	rt ()	System notifications	E-mail Notifications
	ARP Spoofing Attack Al	ert①	System notifications	E-mail Notifications
	IP Spoofing Attack Aler	t①	System notifications	E-mail Notifications
			Cancel Save	

Alert Notification Settings – part 3

	lect the alert content that needs to be notif		and So to (S) statt saturble for
tem Alert	Performance Alert Security A	lert Network Alert	
	WAN Network Connection Alert	System notifications	E-mail Notifications
	WAN/LAN/USB Connection Alert	System notifications	E-mail Notifications
	VPN User Connection Alert ①	System notifications	E-mail Notifications
	VPN Client Connection Alert 🕕	System notifications	E-mail Notifications
	DHCP Failure Alert	System notifications	E-mail Notifications
	PPPoE Connection Timeout Alert	System notifications	E-mail Notifications
	Certificate Expired Alert 🕕	System notifications	E-mail Notifications
	Session Usage Alert 🛈	System notifications	E-mail Notifications

Alert Notification Settings – part 4

E-mail Notifications

On this tab, the user can setup the E-mails that will receive the notifications, once the feature is enabled, then the user can fill up the fields according to SMTP parameters. Refer to the figure below:

Alerts & No	otifications		Alert Notification Settings	E-mail Notification Settings
Alerts	E-mail Notifications			
	E-mail Notifications	After enabled, alert will be sent to receiver e-mail.		
	From E-mail Address ()			
	From Name		1~32 characters	
	*SMTP Hostname①			
	*SMTP Port ①		Range 1~65535	
	*SMTP Username ①			
	* SMTP Password ①	- Sect	1~64 characters	
	Skip Certificate Validation	Specify whether to skip certification validation. If enabled, notification email will be sent without server certificate validation.		
	* Receiver E-mail Address	GS_user1@grandstream.com	•	
		Ain@grandstream.com	•	
		Add E-mail Addres	55 () (
		Cancel Save Save and Test		

Alerts – E-mail Notifications

It's possible to add more than one receiver E-mail address as shown in the figure above.

- Click on "Minus" icon to delete the receiver E-mail address.
- Click on "Plus" icon to add the receiver E-mail address.

E-mail Notification Settings

To select what notifications will be sent to the receiver E-mail addresses, please click on "E-mail Notification Settings" button as shown below:

Alerts & M	Notifications		Alert Notification Settings	E-mail Notification Settings
Alerts	E-mail Notifications			
	E-mail Notifications	After enabled, alert will be sent to receiver e-mail.		
	From E-mail Address()			
	From Name		1~32 characters	
	*SMTP Hostname ①			
	*SMTP Port①		Range 1-65535	
	*SMTP Username ③			
	*SMTP Password ①		1~64 characters	
	Skip Certificate Validation	Specify whether to skip certification validation. If enabled, notification email will be sent without server certificate validation.		
	* Receiver E-mail Address	G51@grandstream.com	•	
		GS2@grandstream.com	•	
		Add E-mail Addres	s 🕕	

E-mail Notification Settings

The figures below show all the possible E-mail notifications that the user can send to the pre-configured receiver E-mail Addresses, organized into 4 categories: **System** Alert, **Performance** Alert, **Security** Alert and **Network** Alert.

Alerts & Notifications	s > Notification Settings	
O Please select the ale	erts to be notified by e-mail	
System Alert Perfo	ormance Alert Security Alert Network Alert	
	Admin Password Change Alert Once enabled, an alert email will be sent when the administrator password is changed	
	Upgrade Alert Once enabled, when the router /AP is upgraded, a successful/failed upgrade alert email will be sent.	
	Temperature High Alert Once enabled, an ailert email will be sent when the router /AP temperature reaches 110°C	
	Pairing/taking over/unpairing AP Alert Once enabled, an alert email will be sent when the router pairs/takes over/unpairs an AP	
	AP Online Alert Once enabled, an alert email will be sent when the AP is online	
	AP Offline Alert Once enabled, an alert email will be sent when the AP's offline time exceeds the set threshold	

E-mail Notification Settings - part 1

Alerts & Notificat	tions > Notification Settings	
① Please select the	he alerts to be notified by e-mail	
System Alert	Performance Alert Security Alert Network Alert	
_	Memory Usage Alert Once enabled, an alert email will be sent when the memory usage of the router /AP exceeds the set threshold	
	CPU Usage Alert Once enabled, an alert email will be sent when the CPU usage of the router /AP exceeds the set threshold	
	Client Throughput Alert Once enabled, an alert email will be sent when the client throughput exceeds the set threshold	
	WAN Port Throughput Alert Once enabled, an alert email will be sent when the network throughput/upload bandwidth/download bandwidth of the WAN port exceeds the set threshold	

E-mail Notification Settings – part 2

Alerts & Notific	ations > Notificatio	n Settings		
Please select	ct the alerts to be notified t	oy e-mail		
System Alert	Performance Alert	Security Alert	Network Alert	
			TCP SYN Flood Attack Alert	
			Once enabled, an alert email will be sent Once a TCP SYN Flood attack is detected/successfully defended	
			UDP Flood Attack Alert	
			Once enabled, an alert email will be sent Once a UDP Flood attack is detected/successfully defended	
			ICMP Flood Attack Alert	
			Once enabled, an alert email will be sent Once an ICMP Flood attack is detected/successfully defended	
			ACK Flood Attack Alert	
			Once enabled, an alert email will be sent Once an ACK Flood attack is detected/successfully defended against	
			IP Options Attack Alert	
			Once enabled, an alert email will be sent when the IP Option attack is detected and successfully defended	
			TCP Flag Attack Alert	
			Once enabled, an alert email will be sent Once the TCP flag attack is detected and successfully defended	
			Land Attack Alert	
			Once enabled, an alarm email will be sent Once the Land attack is detected and successfully defended	
			Smurf Attack Alert	
			Once enabled, an alert email will be sent Once a smurf attack is detected and successfully defended	
			Ping of Death Attack Alert	
			Once enabled, an alert email will be sent Once the ping of death attack is detected and successfully defended	
			Trace Route Attack Alert	
			Once enabled, an alert email will be sent Once the trace route attack is detected and successfully defended	
			ICMP Fragment Attack Alert	
			Once enabled, an alert email will be sent Once an ICMP fragment attack is detected and successfully defended	

E-mail Notification Settings – part 3

 Please select the 	alerts to be notified by e-mail	
ystem Alert Pe	rformance Alert Security Alert Network Alert	
	WAN Network Connection Alert Once enabled, an alert email will be sent when the router is connected or disconnected from the network	0
	WAN/LAN/USB Connection Alert Once enabled, an alert email will be sent when the WAWLAN/USB port of the router is connected or disconnected	0
	VPN Server Connection Alert Once enabled, an alert email will be sent when the router VPN server establishes a connection or disconnects the connection	0
	VPN Client Connection Alert Once enabled, an alert email will be sent when the router VPN client is connected or disconnected	Q
	DHCP Failure Alert Once enabled, an alert email will be sent Once the DHCP failure is detected	a
	PPPoE Connection Timeout Alert Once enabled, an alert email will be sent Once the PPPoE connection times out	0
	Certificate Expiration Alert Once enabled, an alert email will be sent Once the certificate has expired	O

E-mail Notification Settings – part 4

SYSTEM SETTINGS

Basic Settings

On the **Basic Settings** page, users can configure essential settings for the GWN700x router, including:

• **Device Name**: Assign a custom name for the router.

- **Country/Region** and **Time Zone**: Set the geographical location and time zone.
- **NTP Server**: Configure one or more NTP servers to synchronize the router's time. Click the + icon to add additional NTP servers, which is useful for ensuring time accuracy from multiple sources.
- **Synchronize Time to The Taken Over Device**: Once enabled, all devices managed by the router will directly synchronize with the router's NTP server time settings.
- **Language**: Choose the preferred display language.
- Reboot Plan: Set up a scheduled reboot if required by clicking on Create Schedule under the Reboot Plan section.
- LED Indicator: Configure the LED indicator to be Always On, Always Off, or based on a defined schedule.

Deale Castleres			
Basic Settings			
Basic Settings	Manager Server Settings		
	*Device Name	GWN7002	1~64 characters
	Country / Region	Morocco ~	
	Time Zone	(UTC) Casablanca,Monrovia	
	*NTP Server	0.pool.ntp.org	•
		1.pool.ntp.org	•
			•
		Ad	d 🕂
	Synchronize Time to The Taken Over Device 🕜		
	Language	English	
	Other Settings		
	Reboot Plan		
	LED Indicator	Always On Always Off Enabled based schedule	
		Cancel Save	
		Basic Settings	

Manager Server Settings

In the case of GWN manager (on-premise GWN management solution), the user can specify the manager server address and port, there is also the option to allow DHCP option 43 override.

Basic Settings			
Basic Settings	Manager Server Settings		
	Manager Server Settings		
	* Manage Server Address	192.168.5.122	
	*Manage Server Port	8443	Default 8443, range 1~65535
	Allow DHCP Option 43 Override		
		Cancel Save	

Manager Server Settings

Security Management

Under "Web UI \rightarrow System Settings \rightarrow Security Management" the user can change the login password and activate the web service for example web WAN port access for HTTPS port 443 as well as enabling SSH remote access.

Login Password

On this page, the user can change the password by entering the old password and then confirming the new password.

After changing the login password, the web will be forcibly logged out.

Security Manag	ement			
Login Password	Web Service SSH Service	Passwordless Remote Access		
	*Old Password		*	
	*New password	Enter new password	*	8~32 characters, must include any two of numbers, letters and special characters
	*Confirm new password	Confirm to enter new password	>	
		Cancel Save		

Security Management – Login Password

Web Service

Web Service feature allows the user to access the router's web GUI from the WAN side. The connection is established over HTTPS for enhanced security. It's also possible to specify a hostname for the GWN700x router as shown in the figure below:

Security Management		
Login Password Web Service SSH Service	Passwordless Remote Access	
*HTTPS Port ①	443	Default 443, range 1~65535, excluding 14,80,223,224,8000,8080,8443,10014
Web WAN Port Access		
*HostName	gwn700x.grandstream.com	
	Cancel Save	

Security Management – Web Service

SSH Service

This feature allows the user to access the device using SSH remotely. Enable this option and click on "**SSH Remote Access**" button and then enter the SSH remote access password (login password). Once that's done, SSH access will be provided to remote users when they enter the correct password.

Security Manage	ement					
Login Password	Web Service	SSH Service	Passwordl	ess Remote Access		
	Enable SSH			•		
	SSH Remo	ote Access		۰. ۲		
				SSH Remote Access		
				SSH Remote Access		×
		_	n Password	I		- 1
			characters			- 1
					74	- 1
						- 1
				Cancel Save		- 1
						_

Security Management – SSH Service

Passwordless Remote Access

Enabling the Passwordless Remote Access feature, accessing the device using GDMS Networking will not require entering the password to be able to access the web GUI of the router.

Note

By default is disabled.

Security Manag	ement		
Login Password	Web Service	SSH Service	Passwordless Remote Access
	Password	lless Remote Aco	cess If enabled, account password will no longer be required wher accessing remotely via GWN.Cloud. Disabled by default.
			Cancel Save

Security Management – Passwordless Remote Access

Email Settings

The *Email Settings* feature in the GWN router enables email alerts for network events and notifications. To configure email notifications, follow these steps:

1. Enable Email Notifications: Toggle the "Email Notifications" switch to enable alerts.

2. Enter Sender Information:

- From Email Address: Enter the email address from which alerts will be sent. Example: notifications@gwnrouter.com.
- $\circ~$ From Name: Specify the sender name that will appear in alert emails. Example: <code>GWN Router Alert</code> .

3. Configure SMTP Server:

- **SMTP Hostname**: Enter the SMTP server hostname. This is required for the router to connect to your email service provider. Example: smtp.example.com.
- SMTP Port: Set the SMTP port used by your email provider. Common ports are 587 (for TLS) and 465 (for SSL).
- SMTP Username: Input the email account's username. Example: your-email@example.com.
- SMTP Password: Enter the password for the SMTP username.

4. Certificate Validation:

 Skip Certificate Validation: Toggle this option only if your SMTP server does not support SSL certificates. Enabling this will send alerts without server certificate validation.

5. Set Receiver Email Address:

• Add the email addresses to which notifications should be sent. Example: admin@yourdomain.com. Multiple addresses can be added by clicking "Add E-mail Address".

6. Save Configuration:

• Click "Save" to apply the settings or "Save and Test" to test email notifications.

Note: Ensure that SMTP credentials are correct, and the SMTP server allows email relay for notifications to work properly.

Email Settings		
E-mail Notifications	After enabled, the alert will be sent to receiver e-mail.	
From E-mail Address ①	notifications@gwnrouter.com	
From Name	GWN Router Alert	1~32 characters
* SMTP Hostname ①	smtp.example.com	
*SMTP Port ()	587	Range 1~65535
*SMTP Username ()	your-email@example.com	
* SMTP Password ①	Sec. Sec.	1~64 characters
Skip Certificate Validation	Specify whether to skip certification validation. If enabled, notification email will be sent without server certificate validation.	
* Receiver E-mail Address	admin@yourdomain.com	•
	Add E-mail Address	0
	Cancel Save Save and Test	

Email Settings

File Sharing

The GWN routers have a USB port that can be used for file sharing, either using a USB flash drive or a Hard Drive, enabling clients with Windows, Mac or Linux to access files easily on the local network. There is also an option to enable a password for security reasons.

Navigate to System Settings → File Sharing.

File Sharing
① Support Inserting USB devcie. You can use the data in USB storage device by accessing shared directories.
No USB device detected
© 2023 Grandstream Networks, Inc. Grandstream Software License Agreement

File Sharing

Profiles

MAC Group

The MAC Group is a feature in GWN700x that enables the user to create a group of MAC addresses from the available ones or manually adding the MAC Address.

To create a new MAC group, Navigate under: "Profiles → MAC Group" then click on "Add" button.

$\circ~$ Add devices from the list:

Enter the name of the MAC Group, then add the devices from the list.

Name	MAC Group name		1~64 character
Available Devices Add Manually			
Device Name		MAC Address	
Grandstream		00:08:82:F6.64.8C	
DESKTOP BESIME		80.8370.54.80.29	
 M210187865 		FEE7.14.64.8F.09	
• M210 * 100		AE84.5CA54277	
Grandstream		CE78.4056.61.64	

Add MAC Group

• Add Devices Manually:

Enter the name of the MAC Group, then add the devices' MAC addresses.

MAC Group > Add MA	C Group		
*Name		MAC Group name	1~64 characters
Available Devices	Add Manually		
Device MAC Address		E0 : 74 : AD : 77 : 66 : 55 Add MAC Address +	
		Cancel Save	

Add MAC address manually

After the MAC Group is created, to take effect the user needs to apply it, for example like the SSID:

Navigate to "**Web UI** \rightarrow **AP Management** \rightarrow **SSIDs**", either click on "**Add**" button to create new SSID or click on "**Edit**" icon to edit previously created SSID, scroll down to "**Access Security**" section then look for "**Blocklist Filtering**" option and finally select from the list the previously created MAC address, the user can select one or more, or click on "**Add**" at the bottom of the list to create new one.

Please refer to the figure below:

SSIDs > Add SSID		
*WPA Shared Key		2
Enable Captive Portal		
Blocklist Filtering	Please Select Blocklist Filtering	Q
Client Isolation ①	Select All	
	MAC Group	
802.11w①	+ Add	
Advanced \checkmark		
Device Management $\ ee$		
	Cancel Save	

MAC Group – SSID example

IP Address Group

The **IP Address Group** feature allows users to manage groups of IP addresses for applying policies such as security rules, NAT, or firewall settings. Both **IPv4** and **IPv6** addresses are supported. By grouping addresses, you can manage multiple addresses with ease, improving policy efficiency and reducing errors.

To configure IP Address Groups, follow these steps: Navigate to **Profiles** \rightarrow **IP Address Group** from the main menu.

IPv4 Address

The **IPv4 Address** feature lets you add individual IPv4 addresses, subnets, or ranges for use in policies like NAT or firewall settings. Once addresses are added, you can group them for better management.

Steps to add an IPv4 Address:

- 1. Navigate to **Profiles** \rightarrow **IP Address Group** \rightarrow **IPv4 Address**.
- 2. Click Add to create a new IPv4 address.
- 3. Enter a **Name** for the address.
- 4. Select the **Type** from:
 - IP Address
 - IP Address/Mask Length
 - IP Address Range
- 5. Fill in the relevant details (e.g., IP address, subnet mask, or range).
- 6. Click **Save** to add the IPv4 address.

Pv4	Address IPv4 Addre	ss Group IPv6 Address IPv	6 Address Group	
A	dd Delete			Q. Name / IP Address
~	Name	Content	References	Operations
	IP Address Group 3	192.168.4.65-192.168.4.100	①Total 1: Ipv4 Address group	C Ū
	Block IP Addess Gro	10.0.0/24	①Total 1: <u>Ipv4 Address group</u>	
	IP Address Group 2	192.168.3.33	①Total 1: IPv4 Address Group 2	
~	SNAT Group	192.168.5.0/24	-	13 11

IP Address – IPv4 Address

Add Delete		Q Name / IP Address
Name	Edit ×	Operations
IP Address Group 3	* Name	C Ū
Block IP Addess Gro.	1~64 characters	C ū
IP Address Group 2	SNAT Group	I
SNAT Group	Туре	C ū
Sixer Group	IP Address/Mask Length v	
	 Content 	Total: 4 < 1 > 10 / pag
	IPv4 Format/Mask Length Range 1-32	and the second
	192.168.5.0 / 24	

IP Address – Add IPv4 Address

IPv4 Address Group

The **IPv4 Address Group** feature allows you to combine multiple IPv4 addresses into one group, simplifying the application of policies like SNAT or firewall rules.

Steps to create an IPv4 Address Group:

- 1. Navigate to **Profiles** \rightarrow **IP Address Group** \rightarrow **IPv4 Address Group**.
- 2. Click Add to create a new IPv4 group.
- 3. Enter a Name for the group.
- 4. Select the IPv4 addresses you wish to include in the group from the list.
- 5. Click **Save** to create the group.

Pv4 Address IPv4	4 Address Group IPv6 Address	Pv6 Address Group	
Add Delete	2		Q. Name / IP Address
- Name	Content	References	Operations
IPv4 Address G	roup 2 ①Total 1: IP Address Group 2		C ū
Ipv4 Address g	roup ①Total 2: IP Address Group 3	Block IP Addess Gro	I Ū

IP Address Group – IPv4 Address

Address Group > Edit		
*Name	IPv4 Address Group 2	1~64 characters
Add Manually		Q Name / IP Address
- Name	Content	
IP Address Group 3	192.168.4.65-192.168.4.100	
Block IP Addess Group	0 10.0.0/24	
IP Address Group 2	192.168.3.33	
SNAT Group	192.168.5.0/24	

IP Address Group – Add IPv4 Address

IPv6 Address

The **IPv6 Address** feature lets you add IPv6 addresses or networks, which can be used in settings such as firewall rules or NAT configurations.

Steps to add an IPv6 Address:

- 1. Navigate to **Profiles** \rightarrow **IP Address Group** \rightarrow **IPv6 Address**.
- 2. Click **Add** to create a new IPv6 address.
- 3. Enter a Name for the address.
- 4. Select the Type:
 - IP Address
 - IP Address/Prefix Length
- 5. Fill in the relevant IPv6 address or prefix.
- 6. Click **Save** to add the IPv6 address.

Address Group			
v4 Address IPv4	Address Group	IPv6 Address Group	
Add Delete			Q Name / IP Address
Name	Content	References	Operations
IPv6 Address 3	2001:db8::		Ľ Ū
IPv6 Address 2	2001:db8::/64	①Total 1: IPv6 Address Group SNAT	Ľ ī
IPv6 Address	2001:db8::1	①Total 1: IPv6 Address Group Firewall	Ľ Ū
			Total: 3 < 1 > 10 / page

Add Delete	Edit	×	Q Name / IP Address
Name	* Name		Operations
IPv6 Address 3	1–64 characters		C Ū
IPv6 Address 2	IPv6 Address 2	I	Ľ Ū
IPv6 Address	Туре	vall	C Ī
-	IP Address/Prefix Length \sim		
	* Content		Total: 3 < 1 > 10 / page
	IPv6 Format/Prefix Range 1-128		
	2001:db8:: / 64		

Add IPv6 Address

IPv6 Address Group

The **IPv6 Address Group** feature allows you to group multiple IPv6 addresses into one group. This makes it easier to apply policies to multiple addresses at once.

Steps to create an IPv6 Address Group:

- 1. Navigate to **Profiles** \rightarrow **IP Address Group** \rightarrow **IPv6 Address Group**.
- 2. Click Add to create a new IPv6 group.
- 3. Enter a **Name** for the group.
- 4. Select the IPv6 addresses to include from the list.
- 5. Click **Save** to create the group.

Pv4 Address IPv4 Address Group	IPv6 Address IPv6 Addr	ess Group	
Add Delete			Q Name / IP Address
Name Content		References	Operations
IPv6 Address Group ①Total 1	: IPv6 Address		
IPv6 Address Group ①Total 1	: IPv6 Address 2		C Ū
			Total: 2 < 1 > 10 / page

IPv6 Address Group

IP Address Group > Edit		
*Name	IPv6 Address Group Firewall	1~64 characters
Add Manually		Q Name / IP Address
Name	Content	
IPv6 Address 3	2001:db8::	
IPv6 Address 2	2001:db8::/64	
✓ IPv6 Address	2001:db8::1	
	Cancel Save	

Add IPv6 Address Group

IP Address Group – Example

Here's an example of how to use an IPv4 Address Group in a Source NAT (SNAT) configuration:

- 1. Navigate to **Routing** \rightarrow **SNAT**.
- 2. Click Add to create a new SNAT rule.
- 3. Select the Destination Group as WAN1 (WAN).

- 4. Under Destination Address Type, choose Select IPv4 Address Group.
- 5. Under Destination Address, select the desired IPv4 Address Group from the list.
- 6. Configure other fields such as **Destination Port** as needed.
- 7. Click Save to apply the rule.

* Destination Group	WAN1 (WAN)	~
Destination Address Type	Select IPv4 Address Group	~
Destination Address		⊗ Q
Destination Port	IPv4 Address Group 2	
	lpv4 Address group	
	+ Add IPv4 Address Group	
	IP Address Group	

FQDN (Fully Qualified Domain Name)

The FQDN feature allows you to define domain names that can be applied in traffic rules, firewall policies, or other configurations. It can also be paired with specific IP addresses, making it easier to manage domains instead of individual IP addresses.

You can create individual **FQDN Addresses** or group multiple FQDN addresses into an **FQDN Address Group** for easier management and application in rules.

FQDN – Address

An FQDN Address is a domain name entry that can optionally be associated with up to eight IP addresses. This is useful for applying domain-based traffic filtering or rules.

To create an FQDN Address:

- 1. Navigate to: Profiles → FQDN → Address
- 2. Enter the following:
 - Name: Name of the FQDN address (e.g., "Grandstream").
 - FQDN: Enter the domain (e.g., *.grandstream.com). Wildcards can be used to match subdomains.
 - Manually added IPs (optional): Add up to 8 IP addresses to be associated with the FQDN.

3. Click Save to add the FQDN entry.

Addr	Address Group				
A	dd Delete			C	۱۹ Name / Domain name / ۱۹
~	Name	Content	Associated IPs	References	Operations
~	Documentation	*.documentation.gr	①Total 1: 44.231.237.187		ľ
	FQDN	*.text.net	①Total 1: 1.1.1.1	①Total 1: FODN Ad	ddr 🗹 🔟
	Grandstream	*.grandstream.com	() Total 3: 44.231.237.187,199.60.103.225	Total 1: FQDN A	ddr 🗹 🔟

FQDN

* Name	Grandstream		1~64 characters
* FQDN 🛈	*.grandstream.com		1~256 characters
Manually added IPs 🛈	199.60.103.225		e IPv4 Forma
	179.60.13.56		•
		Add IP address	•
Resolved IPs	44.231.237.187		
	Cancel Save		

FQDN – Address Group

FQDN Address Groups allow you to group several FQDN addresses, which simplifies applying multiple FQDNs within traffic rules.

To create an FQDN Address Group:

1. Navigate to: Profiles \rightarrow FQDN \rightarrow Address Group

- 2. Provide a **Name** for the group.
- 3. Select the FQDN addresses to be included in the group.
- 4. Click **Save** to create the group.

FQDN				
Address Address Group				
Add Delete				Q Name
Vame	Content	References		Operations
FQDN Address Group	①Total 2: FQDN,Grandstream	-		r ū
			Total:	1 < 1 > 10 / page ∨
	FQL	DN – address group		
FQDN > Edit				
*Name	FQDN Address 0	Group		1–64 characters
Add Manually				Q Name / Domain name / IP A
- Name	Content	Associated IPs		
Documentation	*.documentation.gr	①Total 1: 44.231.237.187		
FQDN	*.text.net	①Total 1: 1.1.1.1		
Grandstream	*.grandstream.com	①Total 3: 44.231.237.187,199.60.103.	225,179.60	.13.56
	Cancel	Save		

FQDN – Add address group

FQDN – Example

Here is an example of applying an FQDN Address Group in a firewall rule. This will show how to use domain-based filtering within your network.

Example: Applying FQDN Address Group in a Traffic Rule

- 1. Navigate to: Firewall → Traffic Rules → Add Inbound Rule.
- 2. For Source Address Type, select FQDN Address Group.

- 3. Select the previously created FQDN Address Group (e.g., "FQDN Address Group").
- 4. Configure any other parameters as needed and click Save.

Source Address Type	Select FQDN Address Group	~
Source Address		Q
Source Port ()	FQDN Address Group	
Source Forc	+ Add FQDN Address Group	
Destination Address Type	IP Address	~

FQDN – Example

RADIUS

RADIUS is a networking protocol that provides centralized authentication, authorization, and accounting for users or devices connecting to a network. In the GWN7002, the RADIUS feature allows network administrators to integrate external RADIUS servers for handling network access.

To create a RADIUS profile:

- 1. Navigate to: Profiles \rightarrow RADIUS \rightarrow Add.
- 2. Enter the RADIUS server details:
 - Authentication Server: Enter the server address and port for authentication (default port is 1812).
 - RADIUS Accounting Server: Enter the server address and port for accounting purposes (default port is 1813).
 - RADIUS NAS ID: Input the NAS ID (Network Access Server ID).
 - Attempt Limit: Specify the number of attempts before the server denies access.
 - RADIUS Retry Timeout: Set the time to wait before retrying a connection to the server (in seconds).
 - Accounting Update Interval: Set the interval at which accounting updates will be sent (in seconds).
- 3. Save the profile.

DIUS					
Add Delet	e			Q Na	ame
Name	Authentication Server	RADIUS Accounting Server	Attempt Limit	RADIUS retry tin	nec Operations
RADIUS_1	139.59.128.75[1812]	139.59.128.76[1813]	1	10	ľŪ
				Total: 1 <	1 > 10 / p.
		RADIUS			
RADIUS > Edit R	RADIUS Authentication				
	* Name	RADIUS_1		1~64 character	75
	*Authentication Server ①	Server Address	Port	Secret	
		139.59.128.75	1812	•••••	Add 🕂
		Server Address			
	RADIUS Accounting Server ①	139.59.128.76	Port 1813	Secret	bat 😑
					Add 🕁
	RADIUS NAS ID	radius1			rs, support numbers, letters aracters ~!@#\$%&*()+=_
	* Attempt Limit 🕕	1		Default 1, rang	e 1~5
	* RADIUS retry timeout (s) ①	10		Default 10, ran	ge 1~120
	Accounting Update Interval (sec)	30		Range 30~604	800
		Cancel Save			

Add RADIUS

RADIUS – Example

Applying the RADIUS Profile to a Wi-Fi SSID:

- 1. Navigate to: AP Management \rightarrow SSIDs \rightarrow Add.
- 2. In the Access Security section, configure the following:
 - Security Mode: Select WPA2.
 - WPA Key Mode: Select PPSK with RADIUS or another option based on the required encryption method.
 - RADIUS Profile: Select the previously created RADIUS Profile from the dropdown list.

3. Save the settings.

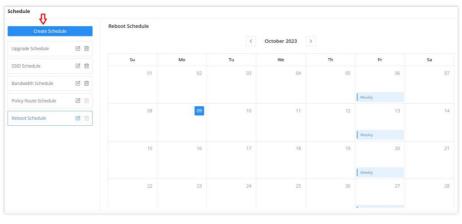
SSIDs > Add SSID		
Access Security \land		
Security Mode	WPA2	~
WPA Key Mode	PPSK with RADIUS	~
WPA Encryption Type	• AES AES/TKIP	
* RADIUS Profile	RADIUS_1	Q
Enable Captive Portal	RADIUS_1	
Disability Elization	Add	
Blocklist Filtering	Please Select Blocklist Filtering	×

RADIUS – Example

Schedule

GWN routers allow the user to create a schedule, either weekly based or an absolute date/time (specific date and an interval), then these schedules can be assigned to various services on GWN routers: Upgrade, SSID, Bandwidth limit, Policy route and reboot.

To create a schedule, navigate to **Profiles** → **Schedule**, then click on "Create Schedule" button as shown below:



Schedule page

Note:

- If both weekly and absolute schedules are configured on the same day, only the absolute schedule will take effect.
- (If no time period is selected on the scheduled date, no service on the corresponding date will be executed).

Create Scheduk	e	Edit (UTC) Casablanca, Mo								
Upgrade Schedule	13 自	 If both weekly and abco 	luce schedules are configured on the same d	ay, only the abson	ice schedule will take	enect.				
SSID Schedule	2 8		* Schedule Name		Reboot Schedul	e			1+64 characters	
Bandwidth Schedule	28	* Weekly								
Policy Route Schedule	E S		Select All	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
Reboot Schedule	E S		19:00-19:30							
			19:30-20:00							
			20:00-20:30							
			20:30-21:00							
			21:00-21:30							
			21:30-22:00							
			22:00-22:30							
			22:30-23:00							
			23:00-23:30							
			23:30-24:00							
		* Absolute Date / Tim	 (If no time period is selected on the scheil) 	fuled date, no serv	ice on the corredgion	ding date will be exc	uted.)			
			2023/10/31				23:30-24:00			1
										Add
					Cancel	Save				

Certificates

CA Certificates

In this section, the user can create a CA certificate. This certificate will authenticate the user when connected to the VPN server created on the router. This authentication will ensure that no identity is being usurped and that the data exchanged remain confidential. To create a certificate, please access the web GUI of the router and access **System Settings** \rightarrow **Certificates** \rightarrow **CA Certificates** then click "Add" and fill in the necessary information.

*Cert. Name		1~64 characters, only support input in English, numbers, characters .
Key Length	2048 ~	
Digest Algorithm	● SHA1 ○ SHA256	
*Expiration (D)		Range 1~ <u>999999</u>
SAN	None IP Address Domain	
Country / Region	United States of America \vee	
*State / Province		
*City		
*Organization		
*Organizational Unit		
*Email		
	Cancel Save	

Add CA Certificate

Cert. Name	Enter the Certificate name for the CA. Note: It could be any name to identify this certificate. Example: "CATest".
Key Length	 Choose the key length for generating the CA certificate. The following values are available: 512: 512-bit keys are not secure and it's better to avoid this option. 1024: 1024-bit keys are no longer sufficient to protect against attacks. 2048: 2048-bit keys are a good minimum. (Recommended). 4096: 4096-bit keys are accepted by nearly all RSA systems. Using 4096-bit keys will dramatically increase generation time, TLS handshake delays, and CPU usage for TLS operations.
Digest Algorithm	Choose the digest algorithm:SHA1: This digest algorithm provides a 160-bit fingerprint output based on arbitrary-length input.

	• SHA256: This digest algorithm generates an almost unique, fixed-size 256 bit hash. <i>Note: Hash is a one-way function, it cannot be decrypted back.</i>
Expiration (D)	Enter the validity date for the CA certificate in days. The valid range is 1~999999
Country / Region	Select a country code from the dropdown list. Example: "United Stated of America".
State / Province	Enter a state name or province. Example: "Casablanca".
City	Enter a city name. Example: "SanBern".
Organization	Enter the organization's name. Example: "GS".
Organizational Unit	This field is the name of the department or organization unit making the request. Example: "GS Sales".
Email	Enter an email address. Example: "EMEAregion@grandstream.com"

Add CA Certificate

Certificate

In this section, the user can create a server or a client certificate. To create a certificate please access the web UI of the router, then navigate to **System Settings** \rightarrow **Certificates** \rightarrow **Add Certificate**, click "Add", then enter the necessary information regarding the certificate.

*Cert. Name		1~64 characters, only support input in English, numbers, characters .
*CA Certificates	CERT1 ~	
Certificate Type	Server v	
Key Length	2048 ~	
Digest Algorithm	● SHA1 ◯ SHA256	
*Expiration (D)		Range 1~ <u>999999</u>
SAN	None IP Address Domain	
Country / Region	United States of America \vee	
*State / Province		
*City		
*Organization		
*Organizational Unit		
*Email		
	Cancel Save	
	Add Certificate	

Cert. Name	Enter the certificate's name.
Key Length	Choose the key length for generating the CA certificate. The following values are available:
	 512: 512-bit keys are not secure and it's better to avoid this option. 1024: 1024-bit keys are no longer sufficient to protect against attacks.

	 2048: 2048-bit keys are a good minimum. (Recommended). 4096: 4096-bit keys are accepted by nearly all RSA systems. Using 4096-bit keys will dramatically increase generation time, TLS handshake delays, and CPU usage for TLS operations. 				
Digest Algorithm	 Select the digest algorithm. SHA1: This digest algorithm provides a 160-bit fingerprint output based on arbitrary-length input. SHA256: This digest algorithm generates an almost unique, fixed-size 256 bit hash. Note: Hash is a one-way function, it cannot be decrypted back. 				
Expiration (D)	Select the duration of validity of the certificate. The number entered represents the days that have to elapse before the certificate is considered as expired. The valid range is 1 - 999999.				
SAN	Enter the address IP or the domain name of the SAN (Subject Alternate Name).				
Country / Region	Select a country from the dropdown list of countries. Example: "United States of America".				
State / Province	Enter a state name or a province. Example: California				
City	Enter a city name. Example: "San Diego"				
Organization	Enter the organization's name. Example: "GS".				
Organization Unit	This field is the name of the department or organization unit making the request. Example: "GS Sales".				
Email	Enter an email address. Example: "EMEAregion@grandstream.com"				

Add Certificate

Certificates Backup and Restore

To backup the created certificates, first select all the desired certificates, then click on "**Backup**" button and enter a password to protect it as shown below:

Certificates				Backup C Restore
CA Certificates Certificates				
Add Import Delete			/	Q Search Certificate Name
Cert. Name	Issuer	Expiration	Theme	Operations
CA_Cert	В	ackup	×	ert/emailAd 🕞 🕄 🔟
	* Password 8-32 characters, must include an characters, do not support \$8.8: 	ny two of numbers, letters and special (אר איז) איז		

Certificate Backup

To restore a certificate, click on "Restore" button, then upload the file and enter the password.

Certificates Certificates			
Add Import Delete	Restore	×	Q. Search Certificate Na
Cert. Name	After restoring, all certificates will be overwritten, and VPN clients and services the reference these certificates will be deleted	ıt	me Operations
	Restore Files Upload Only files in .bin format can be uploaded certificates20231005102907.bin ×		
	* Password 8–32 characters, must include any two of numbers, letters and special characters, do not support 54% ["/- \sim \0		

Certificate Restore

CHANGE LOG

This section documents significant changes from previous versions of the GWN700x routers user manuals. Only major new features or major document updates are listed here. Minor updates for corrections or editing are not documented here.

Firmware Version 1.0.11.6

- Added support for VLAN2. [VLAN]
- Added support for nslookup. [System Diagnostics]
- Optimized Traceroute feature. [System Diagnostics]
- Added RADIUS configuration as a profile. [RADIUS]
- Optimized dynamic route WAN action rule. [WAN]
- Optimized WireGuard® configuration. [WireGuard®]
- Optimized Feedback configuration. [Feedback]
- Optimized Client list filtering. [Client]
- After changing the login password, the web will be forcibly logged out. [Security Management]
- OpenVPN/WireGuard® local ports automatically provide an available number. [WireGuard®][OpenVPN®]
- Added support for switch management. [Switch Management]
- Added switch statistics to the dashboard. [Overview]
- Added support for dynamic routing: OSPF/RIP/BGP. [OSPF] [RIP] [BGP]
- Added VPN configuration wizard. [VPN Setup Wizard]
- Added support for 6G band. [Overview]
- Added support for captive portal on wired network. [Captive Portal]
- Added multiple language support. [Web UI Languages]
- Added FQDN and FQDN group profile. [FQDN]
- Added object grouping profile support. [Profiles]
- Added support for nslookup [NSlookup]
- Added support for TR069, settings can be found under Maintenance. [tr-069]
- Cloud/Manager connection detection support multiple links. [Manager Servers Settings]
- Added "Service Name" filed to the WAN PPPoE configuration. [WAN]
- Added the feature Email Settings. [Email Settings]
- Added support for Standby on Demand mode for PPPoE. [WAN]
- Added standby mode in policy routing. [Policy Routing]
- Added the ability to detect the public IP when the GWN700x is behind another router. [GDMS Networking]
- GDMS Networking/GWN Manager connection detection support multiple links. [GDMS Networking/GWN Manager]
- Added support for cloud configuration of DDNS IP source and update interval. [DDNS]
- Added supports for cloud configuration of exempt IP, DoS defense, and Spoofing defense.
- Added support for cloud security alerts.
- Added support to configure blackhole for static routes. [Static Routes]
- Added support for exporting .ovpn files [VPN Remote Users]
- Optimized Alert & Notifications Web UI. [Alert & Notifications]
- Added support for setting up multiple NTP servers. [NTP Server]

Firmware Version 1.0.5.36

No major change

Firmware Version 1.0.5.35

• No major change

Firmware Version 1.0.5.30

• Added the new feature of Speed test [WAN]

Firmware Version 1.0.5.7

Removed the DHCP range restriction on Static IP assignment which was added in 1.0.5.6 [Static IP Binding]

Firmware Version 1.0.5.6

- Added new feature of WAN-Bridge Mode and VLAN tag priority [WAN]
- Added new feature of disabling the router ports [Port Configuration]
- Added more services under DHCP option 43 [LAN]
- Added IGMP proxy and IGMP snooping [IGMP]
- Added new feature of IP Routed Subnet [LAN]
- Added Bonjour Gateway [Bonjour Gateway]
- Added Binding Mode and Device Name under Static IP Binding [Static IP Binding]
- Added new feature of transferring GWN APs taken over by GWN router to GWN Cloud/Manager [AP Management]
- Added Client list under Access Point for clients connected currently to the AP [Access Points]
- Added PPSK (Private Pre-Shared Key) feature [PPSK]
- Added SSID Bandwidth limit feature with schedule support [SSIDs]
- Added WireGuard® VPN [WireGuard®]
- Added new feature of exporting clients list [Clients]
- Added clients bandwidth limit feature with schedule support [Clients]
- Added Bandwidth limit feature for both wireless and wired clients [Bandwidth Limit]
- Added more social authentication (Facebook, Twitter and Google) under Captive portal [Splash Page]
- Added Vouchers feature under Captive Portal [Vouchers]
- Added new feature of exporting Guest list [Guests]
- Added support for more alerts [Alerts]
- Added new feature of naming the GWN router [Basic Settings]
- Added new feature of customizing the Hostname [Web Service]
- Added GWN.Cloud/Manager connection status detection [System Diagnostics]
- Added EEE (Energy-Efficient Ethernet) feature [Port Configuration]
- Added the option to display a month-long time period in traffic statistics (only for GWN7003) [Traffic Statistics]
- Added TURN Service feature [TURN Service]

Firmware Version 1.0.3.5

• No major changes.

Firmware Version 1.0.3.4

- Added new feature of TURN server (Beta) [TURN Service]
- Added new feature of 2.5G SFP module support [Port Configuration]
- Added QoS bandwidth statistics feature [QoS]

Firmware Version 1.0.1.6

• This is the initial release.