

# GWN7806(P)/7816(P)/7832 Switch Firmware Release Notes

# **IMPORTANT UPGRADING NOTE**

1. Once GWN7806(P)/7816(P)/7832 upgraded to 1.0.9.15, downgrading to 1.0.3.x or 1.0.1.x firmware version is not allowed.



# **Table of Content**

IMPORTANT UPGRADING NOTE	1
FIRMWARE FILE DOWNLOAD	
FIRMWARE VERSION 1.0.9.15	4
PRODUCT NAME	
DATE FIRMWARE FILE INFORMATION	
CHANGES/ENHANCEMENT	
NEW FEATURE OVERVIEW	7
FIRMWARE VERSION 1.0.3.8	43
PRODUCT NAME	
DATE	43
FIRMWARE FILE INFORMATION	-
CHANGES/ENHANCEMENT	
FIRMWARE VERSION 1.0.3.3	44
PRODUCT NAME	
DATE	44
FIRMWARE FILE INFORMATION	
CHANGES/ENHANCEMENT	
FIRMWARE VERSION 1.0.1.14	45
PRODUCT NAME	45
DATE	-
FIRMWARE FILE INFORMATION	
CHANGES/ENHANCEMENT	45



# FIRMWARE FILE DOWNLOAD

Individual firmware files are available for downloading at URL below:

https://www.grandstream.com/support/firmware



# FIRMWARE VERSION 1.0.9.15

## **PRODUCT NAME**

GWN7806(P) / GWN7816(P) / GWN7832

## DATE

8/29/2024

## FIRMWARE FILE INFORMATION

- GWN7806(P) Firmware file name: gwn7806fw.bin
   MD5 checksum: caaedf38dbc458559f734a6fcbf354be
- GWN7816(P) Firmware file name: gwn7816fw.bin
   MD5 checksum: caaedf38dbc458559f734a6fcbf354be
- GWN7832 Firmware file name: gwn7832fw.bin
   MD5 checksum: caaedf38dbc458559f734a6fcbf354be

# **CHANGES/ENHANCEMENT**

- Delete DAC cable configuration in Port Basic Settings.
- Delete 5s interval for port statistics.
- Added port groups.
- Added LLDP auto-config for Auto Voice VLAN mode in Voice VLAN.
- Added more features for STP, including ignore VLAN in BPDU, root protection and loopback protection.
- Added more OUI in Voice VLAN.
- Added IP configuration for MGMT VLAN.
- Added redirect to interface for ACE.
- Added VLAN binding to ACL function.
- Added mask for IPSG/IPv6SG.



- Added remote-ID configuration based on port for DHCP Snooping.
- Added entries fixed for DHCP/DHCPv6 Snooping.
- Added flow upgrade for upgrade via manual upgrade.
- Added more settings for logs, including minimum log level and log aggregation.
- Added Ping watchdog in diagnostics.
- Added connection diagnostics of GWN router.
- Added RSPAN, including port-based and ACL-based remotely mirroring.
- Added new SNMP Traps.
- Added 802.3bt info in LLDP.
- Added alert.
- Added management ACL, including hardware-based and software-based management ACL.
- Added Layer 3 discovery and management by GWN router.
- Added 1588v2 P2P TC.
- Added recovery function.
- Added NAS-Port-Type value 15 with alternate management VLAN.
- Added ability to shutdown port by profile group.
- Added support to ping from ports.
- Added ACL for VTY (SSH and telnet).
- Added additional Radius Access-Request Attributes.
- Added more port details such as neighbor and PoE power history info.
- Added port scheduled enabling feature.
- Added more port statistics info.
- Added loopback detection.
- Added support for QinQ.
- Added MAC-based VLAN.
- Added protocol-based VLAN.
- Added VLAN translation.



- Added untagged OUI mode for voice VLAN.
- Added gateway priority when using DHCP to get VLAN IP address.
- Added default gateway configuration under MGMT VLAN.
- Added ACL advanced settings, including mirroring, statistic and priority remapping for rule.
- Added rate limit by ACL binding to VLAN.
- Added import/export IPSG binding table for IP Source Guard.
- Added IPv6 Source Guard.
- Added mask for IPSG/IPv6SG.
- Added MAC bypass authentication.
- Added DHCPv6 Snooping.
- Added entries fixed for DHCP/DHCPv6 Snooping.
- Added upgrade by FTP and Explicit FTPS.
- Added connection diagnostics with GWN.Cloud/Manager.
- Add DST mode for time settings.
- Add HTTPS/SSH port customization.
- Add GWN Manager takeover function.
- Added support to see switch clients and other information.
- Optimized RIP/RIPng.
- Optimized CBS valid range in Queue Shaping.
- Optimized the rate limit groups from 32 to 128 in ACL.
- Optimized memory fragmentation caused by frequent configuration changes.
- Adjust the maximum length of the command line to 2000.
- Optimized searching for Web GUI.
- Optimized CPU and memory usage in Web GUI.
- Optimized device IP address display.
- Optimized trunk port settings.
- Optimized DHCP server and DHCP relay.



- Optimized DHCP option 43 settings for DHCP server.
- Optimized routing table.
- Optimized remote ID and Circuit ID for DHCP Snooping.
- Optimized EEE.
- Optimize GWN Manager settings.
- Fixed issue that high fan speed with a low load.
- Fixed issue that fans running non-stop at low temperature.
- Fixed DHCP's Option 82 is using wrong Circuit ID/Remote ID.
- Fixed the issue when using STP, connected switch reboots might cause the entire system loses internet connectivity.
- Fixed the issue that the network packets show wrong Circuit ID/Remote ID of DHCP's Option 82.
- Fixed the issue that the device fails to pair with the GWN Manager.
- Fixed issue that Polycom devices failed to assume the Voice VLAN through LLDP-MED.
- Expanded DHCP leases range up to 11520 min
- Some internal bugs fixed.

## **NEW FEATURE OVERVIEW**

Add port groups

Added port group settings to facilitate quick batch setting for port group ports.

🕜 Overview 🗸 🗸	Port Basic Settings			
Switching ^	Port Basic Settings	Port Group		
Port Basic Settings	Add Delete			
Port Statistics	ID	Description	Port Members	Operation
Loopback Detection	1	monitoring	1/0/1-1/0/4	e ii
Port Auto Recovery				
Link Aggregation				
MAC Address Table				
VLAN				



escription	0											0-128 characters
ck on port	to select/	unselect										
Port												
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 28 SFF+ SFF+ SFF+ SFF+
LAG												
LAG				2	4	6		1	10	12	14	

### Added LLDP auto-config for Auto Voice VLAN mode in Voice VLAN

If you select Auto Voice VLAN for Voice VLAN mode, you need to go to LLDP to set network policies. LLDP automatic configuration is now added to voice VLANs, making it easier and faster for users to configure them with one click.

(2) Overview	VLAN					
Switching ^	VLAN	Port Settings	Port Members	Voice VLAN OUI MAC VLAN	Protocol VLAN	
Port Basic Settings				Voice VLAN	Auto Voice VLAN ~	
Port Statistics				*Voice VLAN ID	2	
Loopback Detection				CoS/802.1p Priority	6	Valid range is 0-7
Port Auto Recovery				*DSCP	46	Valid range is 0-63
Link Aggregation						
MAC Address Table					Cancel OK	
VLAN				LLDP/LLDP MED		
Spanning Tree				Auto Config		
~ qı				LLDP Global Settings: LLDP: enabled		
😂 Multicast 🛛 🗸				Port Settings: RXTX : 1/0/1-1/0/10 TX : None	0	
🛞 Routing 🗸 🗸				RX : None Disabled: None		
L≃ Qos ∽				LLDP MED Network Policy Auto Vioce Network Policy		
🧭 Security 🗸 🗸				LLDP MED Port Settings	: enabled	
🖉 Maintenance 🗸 🗸				LLDP MED: Enabled : 1/0/1-1/0/	10	
段 System ~				Disabled : None Network Policy TLV: Enabled : 1/0/1-1/0/: Disabled : None	10	

• Added control over the processing of BPDU packets with VLANs.



Spanning Tree		
Global Settings	Port Settings VLAN Settings	PVST Port Settings
	Spanning Tree	
	Mode	PVST ~
	Ignore VLAN in BPDU	
	Path Cost	Short      Long      legacy
		Cancel OK

#### Added root protection and loopback protection for STP

Root protection and loop protection are added to the port. Note: Root protection and loop protection have one and only one can be enabled.

Port Settings →	Edit Port				
	Port	1/0/2			
	Enable Spanning Tree 🛈				
	*Priority	128			Enter a value between 0-240 that is a multiple of 16
	<b>∗</b> Path Cost ①	0			Valid range is 0-65535
	Edge Port	Auto	🔵 Enabled	O Disabled	
	Root Protection ③				
	Loop Protection ①				
	BPDU Guard				
	BPDU Fliter				
	Point-to-Point	Auto	Enabled	Disabled	
		Cancel	ОК		

Added more OUI in Voice VLAN



) Overview 🗸 🗸	VLAN			
Switching ^	VLAN Port Settings Port Members Voice VLAN O	JI MAC VLAN Protocol VLAN		
	Add Delete			
	OUI Address	Mask	Description	Operation
	00:0B:82:00:00:00	FF:FF:FF:00:00:00	Grandstream	e i
	C0:74:AD:00:00:00	FF:FF:FF:00:00:00	Grandstream	e i
	EC:74:D7:00:00:00	FE:FE:FE:00:00:00	Grandstream	e i
Link Aggregation	00:E0:BB:00:00:00	FE:FE:FE:00:00:00	3COM	I Ó
	00:03:68:00:00:00	FE:FF:FF:00:00:00	Cisco	ľ
	00:E0:75:00:00:00	FE:FF:FF:00:00:00	Veritel	ľŪ
VLAN	00:D0:1E:00:00:00	FF:FF:FF:00:00:00	Pingtel	C Ū
Spanning Tree	00:01:E3:00:00:00	FF:FF:FF:00:00:00	Siemens	C Ō
IP V	00:60:B9:00:00:00	FF:FF:FF:00:00:00	NEC/Philips	e i
Multicast N	00:0F:E2:00:00:00	FF:FF:FF:00:00:00	H3C	e i
	00:09:6E:00:00:00	FE:FE:FE:00:00:00	Avaya	ßŌ
	00:04:F2:00:00:00	FE:FE:FE:00:00:00	Polycom	ľ
	64:16:7F:00:00:00	FE:FE:FE:00:00:00	Polycom	C Ū
	00:88:83:00:00:00	FE:FE:FE:00:00:00	Cisco	C Ū

## Added IP configuration for MGMT VLAN

ôĝ System ∨

Adds the IP address configuration for the management VLAN interface and displays the result. Note: The IP address configuration of the management VLAN interface is synchronized with the configuration of the corresponding VLAN interface in the IP interface.

VLAN IP Interface			
IPv4 Interface IPv6 Interface IPv6 Router Adv	vertisements MGMT VLAN		
	MGMT VLAN	VLAN 1 ~	
	IPv4 Address Settings		
	Address Type	Static IP ( DHCP	
	*Gateway Priority	2	The valid range is 2-255. The smaller the value, the higher the priority.
	IPv6 Address Settings		
	Enable		
		Cancel	
	Management Address		
	MGMT VLAN	VLAN 1	
	Status	UP	
	IPv4		
	Address Type	Dynamic	
	IP Address	192.168.80.123	
	Mask Length	24	
	Gateway	192.168.80.1	
	IPv6		
	Enable Status	Disabled	
	Link-Local Address	-	

#### Added redirect to interface for ACE

The function of redirecting ACL rules to interfaces is added. Note: The selected interface does not contain the interface bound by the ACL.



	۴	IPv4 ACL > Add ACL			
Switching	÷		ACL Name		1-64 (haracters
	~		Rule Settings 💿		
	×		•Rule ID	1	Valid range in 1-2147483647. The smaller
	Ý				ID is matched first.
	~		Action	Allow ~	
Security	^		Protocol Type	Allow	
	E		Source IP Address	Shut Down	
			Destination IP Address	Redirect to Interface	
			Tos Type	Any	
ACL			Time Policy	None	
IP Source Gua	ird		Advanced Settings		
	uard 📧		Count		
			Count Unit	By packet      By byte	
			Mirroring		
			Priority Mapping		
			Rate Limit	Disabled ~	
				The rate limit function medic to go to "Security-#ACL#Rate Limit Settings" to Cancel OK	
Identity Authe	inticatio				

# • Optimized the rate limit groups from 32 to128 in ACL

The ACL rate limit group has been expanded from 32 groups to 128 groups.

ACL				
IPv4 ACL IPv6 ACL MAC AG	CL Port Binding to ACL VLAN Binding to	ACL Rate Limit Settings		
	Burst Threshold Group			
	Burst Byte (Bps)	8388480	Enter a value between 128-8388480 that is a multiple of 128	
	Burst Packet (pps)	10	Valid range is 1-65535	
		Cancel		
te Limit Settings				
Rate Limit Group ID		Rate Limit Type	Rate Threshold	Operation
121				C
22				Ľ
23		-	-	I
24				ß
25				C
26				C
27				Ľ
28		**		Ľ
			Total 128 < 1 11 12	13 > 10/page V Go to

### • Added VLAN binding to ACL function

Added the binding of ACLs to VLANs. Note: The binding of IPv6 ACLs to VLANs is not supported.



ACL				
IPv4 ACL IPv6 ACL MAC ACL Port Binding to ACL VLAN Bi	inding to ACL Rate Limit Settings			
Edit Unbind				
VLAN	IPv4 ACL Name		MAC ACL Name	Operation
□ 1				e e
2		_		C P
3	Edit	×		<b>E</b> <i>P</i>
4	VLAN			<b>I</b> ?
5	3			<b>I</b> ?
6				I d
7	IPv4 ACL v			<b>I</b> P
c 🗌 8				I d
9	MAC ACL			C P
10	None ~			<b>I</b> P
	Cancel		Total 1	9 < 1 2 > 10/page × Go to

# • Added mask configuration for IPSG/IPv6SG

In the quaternary binding table of IPSG and IPv6SG, the mask configuration is added for the IP address and MAC address to expand the coverage of the binding table.

5 Itouting ~	IP Source Guard			
<u>≓ Qa5</u> .~	Port Protection Quaternary Binding Table			
🧿 Security 🔷 🔨	Add Delete Refresh Import Export	Add Quanternary Binding		
Storm Control	Port IPv4 Address/Mask	*Port	Туре	Lease Time (s) Operation
Port Security	1/0/1 192.168.122.254/255.255.255.	1/0/1 ~	Static	- 10
Port Isolation		eIP Address		Table T 🖉 🛐 🖓 Millipage 🛩
ACL.				
IP Source Guard		Mask IPv4 format		
IPv6 Source Goard				
Anti Attack	e:	MAC Address The MAC address must be a stricted address.		
DAL DAL				
RADIUS		Mask FF : FF : FF : FF : FF		
TACACS+		VLAN		
(AAA)		Valid ranger is 1-4004		
802.1X				
DHCP Snaoping		Cancel Ox		
DHCPv6 Snooping				
2 Maintenance ~				



🚡 Routing 🗸 🗸	IPv6 Source Guard	
	Port Protection Quaternary Binding Table	
	Add Quanternary Binding	×
	aPort	
	16/1 ~	
	Provides Profilement and must be a valid unicast address	
	-Prefix Length	
IP Source Guard	Valid range in 1-128	
IPv6 Source Guard	MAC Address	
	The MAC address must be a wricast address.	
	Mask	
	39         :         39         :         39         :         39	
	VLAN Valid range is 1-4294	
	Cancel	
© System ∽	© 2024 Grandstream Networks, Inc. Grandstream Software Lice	License Ag

### • Added remote-ID configuration based on port for DHCP Snooping

DHCP Snooping						
DHCP Snooping Option 8	2 Port Settings	Statistics				
		Format	Normal     Private			
		•Remote ID	Add Option 82	$\times$	1-63 characters, including digits, letters and special characters except "V/,	
			Port			
			1/0/1 ~			
Option 82			VLAN			
Add Delete			None ~			
			Format			
Port	VLAN		Normal      Private		Remote ID	Operation
			■Circuit ID 1-61 characters, including digits, letters and special characters except "V/.			
			Remote ID 0-63 characters, including digits, letters and special characters except "V/			
			Cancel			

Added use of port-based configuration for remote IDs.

## • Added entries fixed for DHCP/DHCPv6 Snooping

Added the entry fixing function for DHCP/DHCPv6 Snooping. Once enabled, the dynamic binding table of the IPSG/IPv6SG is automatically restored when the device restarts. Once turned on, the curing cycle needs to be set.



ස් Routing ~	DHCP Snooping			
	DHCP Snooping Option 82 Port Settings	Statistics		
⊘ Security ^		DHCP Snooping		
		Entries Fixed for DHCP Snooping ()		
		•Fixed Duration (s)	300	Valid range is 15-86400
		VLAN	1-16,444	Valid range is 1-4094, Example: "5-8, 11" will associate VLANs 5, 6, 7, 8 and 11.
		1001	1.10,000	will associate VLANs 5, 6, 7, 8 and 11.
			Cancel OK	
	¢			
802.1X				
DHCP Snooping				
<u>^</u>				
<u>^</u>	DHCPv6 Spooping			
	DHCPv6 Snooping DHCPv6 Snooping Option Settings Port Se	tings Statistics		
			2	
		DHCPv6 Snooping	2	
l⊻ QoS ✓ Ø Security ^		DHCPv6 Snooping	٥	
∠   QqS   ✓     ⊘   Security   ∧     Storm Control   ✓		DHCPv6 Snooping C Entries Rixed for DHCPv6 Snooping © «Fixed Duration (s)	300	Vold range is 13.8600 Vold range 1.5.800
QoS Security Storm Control Port Security		DHCPv6 Snooping	300	Valut range to 15-66400 Valut range to 15-6800 Valut range 15-6000 Executive 'S-8, 11* will associate VANIs 5, 6, 7, 8 and 13.
QoS		DHCIV6 Snooping C Entries Rised for DHCIV6 snooping © «Reed Duration (s) VLAN	500	
Let     QoS     V       Storm Control     A       Port Solution     A       ACL     A		DHCIV6 Snooping C Entries Rised for DHCIV6 snooping © «Reed Duration (s) VLAN	300	
Qos     ~       Security     ~       Storm Control     ~       Port Security     ~       Port Solation     ~       ACL     Posure Guard		DHCIV6 Snooping C Entries Rised for DHCIV6 snooping © «Reed Duration (s) VLAN	500	
dods     v       otherward     <		DHCIV6 Snooping C Entries Rised for DHCIV6 snooping © «Reed Duration (s) VLAN	500	
Qoš     Qoš       Qostaruto     No       Qostaruto     No       Qostaruto     No       Postaruto     No <th></th> <th>DHCIV6 Snooping C Entries Rised for DHCIV6 snooping © «Reed Duration (s) VLAN</th> <th>500</th> <th></th>		DHCIV6 Snooping C Entries Rised for DHCIV6 snooping © «Reed Duration (s) VLAN	500	
Qodi         Quitaria         Quitaria           Quitaria         Quitaria         Quitaria		DHCIV6 Snooping C Entries Rised for DHCIV6 snooping © «Reed Duration (s) VLAN	500	
QoS         QoS         QoS           Beauring         A           Port Social (Control (Contro) (Control (Contro) (Control (C		DHCIV6 Snooping C Entries Rised for DHCIV6 snooping © «Reed Duration (s) VLAN	500	
Quist         Quist         Quist           Istam Control         Intercontrol         Intercontrol           Intercontrol         Intercontrol         Intercontro		DHCIV6 Snooping C Entries Rised for DHCIV6 snooping © «Reed Duration (s) VLAN	500	
Quist         Quist         Quist           Istam Catarda         Istam Catarda         Istam Catarda           Istam Catarda		DHCIV6 Snooping C Entries Rised for DHCIV6 snooping © «Reed Duration (s) VLAN	500	
Storm Control Port Society Port Society Port Society Port Society Port Society Port Society Port Society Port Port Society Port Port Port Port Port Port Port Port		DHCIV6 Snooping C Entries Rised for DHCIV6 snooping © «Reed Duration (s) VLAN	500	

## • Added flow upgrade for upgrade via manual upload

Considering the memory problem of the device, the upload upgrade supports streaming upgrade, and the upgrade is carried out while uploading.

## • Added more settings for logs

Increase the minimum print level of web logs. The log aggregation function is added to merge and display the same logs within a certain period.



0	IP	× .	Diagnostics				
\$		~	Logs Ping Ping Wate	chdog Traceroute Mirroring Fiber Mo	dule Copper Test O	ne-click Debugging N	Aanagement Platform Connection Dia
÷		~	Log Server Address Refresh	Clear All Export Settings			
<u>اح</u>		~	Start date -+ End date	Settings	×		
0		~	Details	Minimum Log Level ()		Level	Generated Time
2	Maintenance	~	SYSTEM-5-CPU_INFO: utilization	Notice	ų.	Notice	Jul 30 2024 19:09:29
			SYSTEM-5-MEM_INFO: utilizatio cached:38744 shared:0 AnonPa	Log Aggregation		Notice	Jul 30 2024 19:09:29
	Diagnostics	¢	DHCP_SNOOPING-5-UNTRUSTE C0:74:AD:CC:DF:C0 and opcode	*Timeout (s) Valid range is 15-3600		Notice	Jul 30 2024 18:17:53
			DHCP_SNOOPING-5-UNTRUSTE C0:74:AD:CC:DF:C0 and opcode	60		Notice	Jul 30 2024 18:17:52
			DHCP_SNOOPING-5-UNTRUSTE C0:74:AD:CC:DF:C0 and opcode	Cancel	1	Notice	Jul 30 2024 18:17:52
			DHCP_SNOOPING-5-UNTRUSTED_DR C0:74:AD:CC:DF:C0 and opcode OFFE	ROP: Untrusted deny. Packet drop: VLAN 1, interfa ER	ice Ethernet1/0/1, chaddr	Notice	Jul 30 2024 18:16:59
Ī					Total 1533 <	1 2 3 1	154 > 10/page ~ Go to
	Energy Saving Man	agent.					

### • Added Ping watchdog in diagnostics

The port Ping watchdog function is added to automatically inflate the device by automatically detecting problems such as device crashes and faults to help solve the problem of unresponsive device failures in the environment

@		Ping Watchdog > Edit Port			
			Port	1/0/1	
0			Enable		
	Multicast		●IP Address		IPv4 format
			Packet Sending Interval (s)	30	Valid range is 30-3600
0			<b>≱</b> Delay Time (s)	60	Valid range is 60-3600
æ	Maintenance		<b>₽</b> Retry Times	2	Valid range is 1-10
	Upgrade		Shutdown Interval (s)	5	Valid range is 5-30
	Diagnostics	c		Cancel	
	Backup & Restore	Í.			
	SNMP				
	RMON				

• Added RSPAN, including port-based and ACL-based remotely mirroring

Added support for remote mirroring. Remote VLANs are used to transmit mirrored packets. In general, VLAN 1 is not recommended



ogs	Ping	Ping Watchdog	Traceroute	Mirroring	Fiber Module	Copper Test	One-click Debugging	Management Platfo	rm Connection Diagnostics		
			Remot	te VLAN ()		2			Valid range is 1-4094, Example: "5-8, 11" will associate VLANs 5, 6, 7, 8 and 11.		
						Cancel	ок				
-		44	Bala					0.000	Manuface Paral		Oreceller
-	Mod		Role		Ingress Mirroring		gress Mirroring	Output Port	Monitor Port	Remote VLAN	Operation
irroring Gro Group			Role		Ingress Mirroring	E		Output Port	Monitor Port	Remote VLAN	29
-	Mod	N					- -				
-	Mod	N	-			-	-	2	-	-	29

Port-based RSPAN for remote mirroring:

Set up a mirror group. When you select RSPAN, you need to select the switch role.

If you use the source switch, you need to set the mirroring port, output port, and remote VLAN.

If you want to use the destination switch, you need to configure the source port, observation port, and remote VLAN

Diagnostics > Edit Mirroring Port		
	Group	1
	Mode	RSPAN ~
	Role	Source Switch
	No. of Concession, Name	Source Switch Destination Switch
	Port	
	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 28 Strate Strate Strate
	LAG	
		2 4 6 8 10 12 14
		1 3 5 7 9 11 13
	Egress Mirroring Click on port to select/unselect	
		Cancel OK

Flow-based (ACL)-based RSPAN: Select an image group in ACL Image



Pv4 ACL > test Rule Details > Edit Rule			
	Rule Settings ①		
	Rule ID	1	Valid range is 1-2147483647. The smaller ID is matched first.
	Action	Allow	
	Protocol Type	Any	~
	Source IP Address	Any     Custom	
	Destination IP Address	Any Custom	
	Тоѕ Туре	Any	~
	Time Policy	None	~
	Advanced Settings		
	Count		
	Mirroring		
	*Mirroring Group	Group 3	~
		Go to "Maintenance>Diagnostics>Mirroring" to configure take effect	
	Priority Mapping		
	Rate Limit	Disabled	v
		The rate limit function needs to go to "Security→ACL→Rate Limit Settings' configure the rate limit group to take effect	° to
		Cancel OK	

Then, select the corresponding port/VLAN binding ACL in the VLAN Binding ACL

Edit Unbind				
VLAN	IPv4 ACL Name		MAC ACL Name	Operation
□ 1				C C
2				C C
3	Edit	×		C C
□ 4	VLAN			C O
5	2			I O
6				20
7	IPv4 ACL test	~		20
8	1621			C C
9	MAC ACL			C C
10	None	~		
	Cancel		Total 12 < 1	2 > 10/page V Go to

Then go to Mirroring Setup Mirroring Group. If you select RSPAN, you can only use it as a source switch and you need to set the output port and remote VLAN.



Diagnostics	Edit Mirroring Port
-------------	---------------------

Group	3	
Mode	RSPAN	~
Role	Source Switch	~
Ingress Mirroring	IPv4 test sequence 1	
*Output Port ()	Please select	~
*Remote VLAN	Please select	~
	Cancel OK	

# • Added new traps in SNMP

Add more traps.

		F						
⑦ Overview	~	SNMP						
Switching	~	Global Settings	View Management	Group Management	Community Management	User Management	Notification Management	Trap Event
9I (Q	~			Authenticati	ion failed			
😂 Multicast	~			Port Up/Dow	vn 💽			
සි Routing	~			Cold Start				
I∠ QoS	~			Warm Start				
Security	~			STP Bridge				
Aaintenance	^			CPU				
Upgrade Diagnostics				Monitor				
Backup & Restore	e			Port ErrDisal	ble			
SNMP				MAC Addres	ss Notification			
RMON				Port Security				
LLDP/LLDP-MED				Logs				
Energy Saving Ma	anag			VLAN Creation	on 🕥			
Alert				VLAN Deletio	on 🕥			
ැබූ System	~			Configuratio	on Distribution			
					Car	ocel OK		

## Added 802.3bt info in LLDP

Port and neighbor information: Add 802.3 bt power supply information.

## • Added alert



Local alarms are added, including CPU usage, memory usage, MAC address exceeding the limit, and temperature.

Overview	~	Alert								
Switching	~	Alert Settings Statistics								
© IР	~									
Multicast	~	Туре	Alert Status	Log Level		Alert Threshold	Alert Waiting Time (s)	Restore Threshold		Restore Walting Time (s)
금 Routing	~	CPU Usage		Error	~	80 %	30	80	%	10
l∠ QoS	~	Memory Usage		Error	~	80 %	30	80	%	10
Security	~	Mac Address Exceeds Limit		Error	~	80 %	30	80	%	10
Le Maintenance	^	Temperature		Error	~	100 'C	30	100	°C	10
Diagnostics	¢	Power Supply Malfunction		Error	~		30			10
Backup & Restore	Ľ					Cancel	ОК			
SNMP						Cancer	UK .			
RMON										
LLDP/LLDP-MED										
Energy Saving Man	ag									
Alert										
🕄 System	×									

• Added management ACL, including hardware-based and software-based management ACL

Hardware management ACLs and software management ACLs are added. Hardware management ACL: The hardware-level management ACL is checked before the CPU is sent to reduce unnecessary resource consumption.

Overview	~	Access Control						
Switching	~	Web Service Management	SSH Remote Access	Management Platform Settings	Management ACL of Hardware-based	Management ACL of Software-base	đ	
© 1P	~			Access Control				
😂 Multicast	~				Cancel			
പ്പ് Routing	~							
L∠ QoS	~	Rule						
Security	~	<ul> <li>After rules added, the syste</li> </ul>	em will generate default drop	ped rules for each set of services and VLA?	N interfaces of the rules, with the lowest priority			
🔑 Maintenance	~							
😂 System	^	Rule ID	Service	Action	IP Address	Mask	VLAN Interface	Operation
Basic Settings	<				1980			
Access Control					1			
User Management					No Data			
Time Policy								
1588v2 TC Beta								
Management AC	CL of H	lardware-based > Ac	dd					
			*Rule ID				Valid range is 1-2147483647. The s	maller
							ID is matched first.	
			Service			~		
			Action	۲	Allow Orop			
			<b>≱</b> IP Address				IPv4 format	
			Mask①				IPv4 format	
			<b>≱</b> VLAN Interf	ace		~		
					Cancel OK			



Overview ~	Access Control		
Switching ~	Web Service Management SSH Remote Access Management Platfo	rm Settings Management ACL of Hardware-based Management ACL of Softwa	re-based
~ ¶1 ⊚			
😂 Multicast 🗸 🗸			
🛃 Routing 🗸 🗸		1.1	
Lee Qoos 🗸 🗸		- 100	
⊘ Security ~			
🔑 Maintenance 🗸 🗸			
System ^	By applying ACL for verificat	ion, users who meet the conditions are allowed to access, while those who do not mee	t the conditions are denied to access
Basic Settings			
Access Control		Add	
User Management			
Time Policy			
1588v2 TC Beta			
Management ACL of	Software-based > Add ACL		
	ACL Name		1~64 characters
	Rule Settings 💿		
	<b>∗</b> Rule ID	1	Valid range is 1-2147483647. The smaller ID is matched first.
	Action	Allow     Drop	
	IPv4 Address/Mask	Any Custom	
	IPv6 Address/Prefix Length	Any Custom	
	*Service	HTTPS SSH Telnet SNMP	
	Port. Click on port to select/unselect		
	Port		
	2 4 6 8	10 12 14 16 18 20 22 24	
			as as an as
	1 3 5 7	9 11 13 15 17 19 21 23	25 26 27 28 55P+ 55P+ 55P+ 55P+
	LAG		
		2 4 6 8 10 12 14	
		1 3 5 7 9 11 13	
		Cancel	

Software management ACL: Use firewall-like settings to control user access.

### • Added Layer 3 discovery and management by GWN router

Layer 3 discovery of switches by cross-network segments and GWN routers is added. You need to set the Layer 3 server address and port on the switch.



@	Overview	~	Access Control				
⊕		~	Web Service Management	SSH Remote Access	Management Platform Settings	Management ACL of Hardware-based	Management ACL of Software-based
		~			Allow DHCP Option 43 to Override Management Server ①		
		~			Management Server Settings		
		~				_	
		~			Management Platform	GWN Manager 💿 GWN Router	
0		~			*Management Server Address		
ور	Maintenance	~			Management Server Port	7443	
	System	^				Cancel OK	
\$		î.					
	Basic Settings	<					
	User Management						
	Time Policy						

### • Added 1588v2 P2P TC

\_\_\_\_

Added 1588v2 P2P TC function.

Note: GWN7806(P)/1X takes effect for electrical ports, and GWN7830/31 takes effect for SFP ports (the Web UI should not be open yet).

Overview ~	1588v2 TC				
⊕ Switching ~		1588v2 TC			
♥ IP		Device Class	○ E2E TC		
😂 Multicast 🗸 🗸					
금 Routing 🗸		Message Encapsulation Mode	MAC UDP UDP over IPv6		
⊯ QoS ~		•PTP Domain	0	Valid range is 0-255	
⊘ Security ~		Virtual Clock ID		0-16 characters, in hexadecimal format	
🖉 Maintenance 🗸 🗸			Cancel OK		
System ^	Port Settings				
Basic Settings	< Edit				
Access Control	Port	End	able Status		Operation
User Management	1/0/1	Di	sabled		ß
Time Policy	1/0/2	D	sabled		ľ
1588v2 TC 8eta	1/0/3		sabled		ľ
130012 10 000	1/0/4		sabled		ß
	1/0/5		sabled		C
	1/0/7		sabled		ß
	1/0/8		sabled		Ľ
	1/0/9	D	cabled		12/2

#### Added recovery function

When the device fails to boot, you can use the recovery function. For details, see the Recovery User Guide.

## • Optimize searching for WEB GUI

A secondary TAB on the left and a TAB at the top of a specific page have been added to support direct jump to a specified page.



6	GWN7801	_					Save Q   💽 adm
		~	VLAN IP Interface			IPv4 Interface	8
⊕		~	IPv4 Interface IPv6 Interface	IPv6 Router Adverti	sements	Ø IP	
0		^	MGMT VLAN		VLAN 1	IP > VLAN IP Interface > IPv4 Inter	face
Γ			IPv4 Default G	ateway			
					Cancel OK		
			Interface Settings				
		y	Add Delete			All ~ All Ty	
L	DNS		Loopback1	Status ()	Type Static	IPv4 Address	MTU Operation
		~ <	* VLAN 1	UP	Dynamic	192.168.80.201/24	1500
		~					Total 2 < 1 > 10 / pag
		~					
		~					
		~					
		~					
				0	2023 Grandstream Networks, Inc	Grandstream Software License Agreement	

### • Optimize CPU and memory usage in Web GUI

Supports viewing historical information of CPU and memory and assists in checking problems of high CPU and memory usage.

S GWN7801	_					Save	<b>Q</b>   🤇
🕜 Overview	^	System Info					
System Info		Basic Info		Resource Status			
Port Info  Switching  IP	~ ~	Device Name System Location System Contact	GWN7801 C Default Default	50%			<b>3%</b> CPU Usage
	× × ×	MAC Address System OID Part Number Serial Number	C0:74:AD:89:38:44 1.3.6.1.4.1.42379 9640004612A 20VXU28N90B93B44	40% 30% 20%		-	<b>0%</b> Memory Usage
	~ ~ ~	MGMT VLAN IPv4 Address IPv6 Global Unicast Address IPv6 Link Local Address	VLAN 1 192.168.80.201 :: fe80::c274:adff:feb9:3b44	0% 1548:10 1548:21 1548: Device Temperature <b>33'C</b>	31 15:48:41 15:48:	51 15:49:01	
		IPv4 Default Gateway IPv6 Default Gateway	192.168.80.1 fe80::96a6:7eff:fe69:7bf1	System Events			
		System Time System Uptime System Version	2023-12-23 15:48:58 UTC+8:00 0 hours. 10 minutes 1.0.5.2	🕍 Emergency	0 > 2 >	<ul><li>Critical</li><li>Error</li></ul>	
		Hardware Version Boot Version	V1.2A 3.6.9.55156	Warning     Notification	22 > 206 >	<ul><li>Information</li><li>Debug</li></ul>	

• Optimize device IP address display

Displays the IP address information of the management VLAN, including the IPv4 address, IPv6 linklocal address, and global unicast address, and also displays the switch default gateway address.



S GWN7801						S	ave 🛛 Q 🕴 🧕 admin :
Overview	^	System Info					
		Basic Info		Resource Status			
Port Info	×	Device Name System Location System Contact	GWN7801 🗹 Default Default	50%			<b>34%</b> CPU Usage
이 IP 왕 Multicast 관 Routing	* *	MAC Address System OID Part Number Serial Number	C0:74:AD:B9:3B:44 1.3.6.1.4.1.42379 9640004612A 20VXU28N90893B44	40% 30% 20%	~		60% Memory Usage
	* * *	MGMT VLAN IPv4 Address IPv6 Global Unicast Address IPv6 Link Local Address	VLAN 1 192.168.80.201 :: fe80::c274:adff.feb9:3b44	0% 15:50:17 15:50:27 15:50:37 1 Device Temperature 33°C	5:50:47 15:50	57 1551407	
		IPv4 Default Gateway IPv6 Default Gateway	192.168.80.1 fe80::96a6:7eff:fe69:7bf1	System Events			
		System Time System Uptime System Version Hardware Version	2023-12-23 15:48:58 UTC+8:00 0 hours, 10 minutes 1.0.5.2 V1.2A	<ul> <li>Emergency</li> <li>Alert</li> <li>Warning</li> </ul>	0 > 2 > 22 >	Critical     Error     Information	0>
		Boot Version	3.6.9.55156	O Notification	206 >	Debug	0 >

• Add more port details such as neighbor, PoE power history info

Supports viewing the port neighbor information, including device name, MAC address, IP address, speed, and connection duration.

Supports viewing the PoE power history to help troubleshoot PoE power supply.

S GWN7803P			Save	🔍   🚺 admin 🗸
Overview	<ul> <li>Port Info</li> </ul>			
Port info				
Switching	Click on the port above to view po	ort information		
	Basic Info		Neighbor Info	0
S Multicast	Port Name:	1/0/1	Hostname:	
	Port Description:		Device ID:	
	Port Status:	Down	iPv4 Address: -	
	Speed:	Auto	IPv6 Address:	
L∼ QoS	Duplex Mode:	Auto	Manufacturer:	
	Flow Control:	Disabled (Off)	Current Rate:	
	Jumbo Frame:	9216	Current Pkts/Bytes:	
	~		Up Time:	
	Statistics		⊘ PoE Power Supply	0
	<		CE FOR SHEEP	Ŭ,
	InOctets:	0	Interval 10 minutes ~	
	InUcastPkts:	0		
	InNUcastPkts:	0		
	OutOctets:	0	1 mW	
	OutUcastPkts:	0	6.8 mW	
	OutOCastPicts:	0		
	OutDiscards:	0	0.6 mW	
	InMulticastPkts:	0	0.4 mW	
	InBroadcastPicts:	0	6.2 mW	
	OutMulticastPkts:	0		
	OutBroadcastPkts:	0	0 mW 02:05	02:15
			Status: Shutdown	
			Power Class: class0	
			Max Power Supply: 15 W	

### Add port scheduled enabling feature

You can customize the Scheduled enable time for a port, including physical ports and LAGs.



S GWN7801			Save	Q   💽 admin 🗸
⑦ Overview ~	Port Basic Settings > Edit Port			
Switching	Port	1/0/1		
Port Basic Settings	Port Type	Copper		
Port Statistics	Description		0~128 characters	
Loopback Detection	Port Enable	Enable     Disabled		
Port Auto Recovery				
Link Aggregation	Scheduled enabled	Only-Workday ^		
MAC Address Table	1000	None Only-Workday		
VLAN	10,000,000	Add		
Spanning Tree	< Flow Control	Disabled Enabled Auto Flow Control setting will not take effect if Duplex Mode is set to "Hali".		
© IP		Cancel		
😂 Multicast 🗸 🗸				
중 Routing ~				
⊾ QoS ~				
⊘ Security ~				
S GWN7801			Save	Q   🚺 admin ~
Overview ~	Port Settings > Edit Port			

S GWN7801			Save Q   💽 admin ~
Overview ~ Port S	Settings > Edit Port		
⊕ Switching	Port	LAG1	
Port Basic Settings	Description		0-128 characters
Port Statistics	Port Enable	Enable Disabled	
Loopback Detection	Scheduled enabled	None	
Port Auto Recovery		None	
Link Aggregation		Only-Workday	
MAC Address Table	(instantion)	🕒 Add	
VLAN		Cancel OK	
Spanning Tree			
~ ¶			
😂 Multicast 🗸 🗸			

# • Add more port statistics info

Support viewing port Private MIB information.



	~	Port Statistics								
Switching	~									
Port Basic Settings			Phylickles Internal fo	P	ort:1/0/1		×			
Port Statistics		Statistics								
Port statistics	_	Clear All	Refresh	Clear						
	n	Port		Interface Ether	ike RMON	Private		tOctets	OutPackets	Operation
		1/0/1	RX_etherStats	UndersizeDropPktsRT	0			18971	35826	0 &
		1/0/2	RX_etherStats	Pkts1519toMaxOctetsRT	0					
		1/0/3	TX_etherStats	Pkts1519toMaxOctetsRT	0					
	e .	1/0/4	RX_MacDisca	dsRT	0					
		1/0/5	-							
	<	1/0/6	-							
	U. 1	1/0/7	-							
		1/0/8	-							
	×.	1/0/9								
	~	1/0/10								
	~	LAG1								
		LAG2								
	~	LAG3								
	~	LAG4								
	~	LAG5	-				-			
		LAG6								
		LAG7								

#### Add loopback detection

By enabling the interface loop detection function, detection messages are periodically sent from the interface to check whether the message is returned to the device, and then determine whether the device has a loop. After a loop is found, the port is automatically shut down to break the loop and ensure the normal operation of the network environment.

Note: If STP is enabled, STP loop protection takes precedence over interface loop protection, that is, interface loop protection will not take effect.

Overview		Loopback Deter	rtion				
		LOOPDICK Deter					
Switching	^		Loopback Detection				
Port Basic Setti	igs			Cancel			
Loopback Detec	tion	Port					
Port Auto Recov	ery	Edit	efresh				
Link Aggregatio		Port	Loopback Detection	Detection Status	Port Status	Time Left (s)	Operation
		1/0/1	Disabled	Disabled	normal	0	Ľ
	able	1/0/2	Disabled	Disabled	normal	0	ß
		1/0/3	Disabled	Disabled	normal	0	ß
	¢	1/0/4	Disabled	Disabled	normal	0	Ø
) IP	~	1/0/5	Disabled	Disabled	normal	0	ß
Multicast		1/0/6	Disabled	Disabled	normal	0	e
		1/0/7	Disabled	Disabled	normal	0	Ľ
출 Routing	~	1/0/8	Disabled	Disabled	normal	0	Z
	~	1/0/9	Disabled	Disabled	normal	0	ß
	~	1/0/10	Disabled	Disabled	normal	0	ß
	~	LAG1	Disabled	Disabled	normal	0	Ľ
3 System		LAG2	Disabled	Disabled	normal	0	12
a system		LAG3	Disabled	Disabled	normal	0	ß



## • Add QinQ

An 802.1Q tag (VLAN tag) is added to the original 802.1Q packet header. Through the double-layer tag, the number of VLANs is increased to 802.1Q.

QinQ encapsulates the user's private network VLAN Tag in the public network (service provider) network VLAN Tag, allowing the double-layer VLAN Tag message to pass through the operator's backbone network (public network). In the public network, the message is transmitted according to the outer VLAN Tag (that is, the public network VLAN Tag), shielding the user's private network VLAN Tag, thereby providing a simple L2 VPN tunnel for the user.

5	GWN7801					Save	Q	admin ~
@			Port Settings > Edit					
<b>#</b>	Switching		Port	1/0/1				
			*Link Type	Trunk				
	Port Statistics		*PVID	Hybrid Access	Valid range is 1-4094			
			Accept Frame Type	Trunk				
	Link Aggregation		TPID	QinQ				
	MAC Address Table	:	VLAN Translation					
				Cancel OK				
0								
\$	Multicast							
ð								
k								
ß								

S GWN7801							Sa	re Q   👤 admi
	~	VLAN						
Switching	^	VLAN	Port Settings Por	t Members Voice VLAN	OUI MAC VLAN Pro	tocol VLAN		
	ngs	Port	Link Type	Tagged VLAN	Trunk Allowed VLANs	Untagged VLAN	PVID	Operation
		1/0/1	Trunk			1	1	Ľ
	rtion	1/0/2	Trunk				1	C
		1/0/3	Trunk		Edit Port Member	×	1	C
	very	1/0/4	QinQ	Port			1	C
	n	1/0/5	Trunk	1/0/4			1	C
	able	1/0/6	Trunk	Link Type			1	Ľ
	ubic	1/0/7	Trunk	QinQ			1	ľ
		1/0/8	Trunk	<b> ↓</b> Untagged VLAN			1	Ľ
	K	1/0/9	Trunk	1			1	Ľ
	<b>_</b>	1/0/10	Trunk	PVID			1	C
		LAG1	Trunk	QinQ port. Same as Unta	agged VLAN		1	C
	~	LAG2	Trunk	1			1	C
	~	LAG3	Trunk				1	C
	~	LAG4	Trunk	C	Cancel OK		1	Ľ
	Ť,	LAG5	Trunk			1	1	C

#### • Optimize trunk port settings

Trunk Allowed VLANs allows configuration of VLANs that do not yet exist on the switch, and takes effect only for configured VLANs.



VLAN						
VLAN	Port Settings Por	t Members Voice VLAN	OUI MAC VLAN Pro	tocol VLAN		
Port	Link Type	Tagged VLAN	Trunk Allowed VLANs	Untagged VLAN	PVID	Operation
1/0/1	Trunk		dit Port Member	×	1	C
1/0/2	Trunk				1	C
1/0/3	Trunk	Port			1	C
1/0/4	QinQ	1/0/5			1	ľ
1/0/5	Trunk	Link Type Trunk		1	ß	
1/0/6	Trunk				1	ß
1/0/7	Trunk	Trunk Allowed VLAN			1	C
1/0/8	Trunk	Enter "5-8, 11" to associa	te 5 VLANs of "5, 6, 7, 8 and 11".		1	C
1/0/9	Trunk		-	1	C	
1/0/10	Trunk	*Untagged VLAN	Jntagged VLAN		1	C
LAG1	Trunk	1			1	Ľ
LAG2	Trunk	<b>PVID</b> Trunk port. Same as Unta	arred VI AN		1	Ľ
LAG3	Trunk	1			1	Ľ
LAG4	Trunk				1	Ľ
LAG5	Trunk	C	ancel OK		1	Ľ
LAG6	Trunk				1	Ľ
LAG7	Trunk			1	1	Ľ

VLAN						
VLAN	Port Settings	Port Members Voice VLA	N OUI MAC VLAN	Protocol VLAN		
Port	Link Type	Tagged VLAN	Trunk Allowed VLANs	Untagged VLAN	PVID	Operation
1/0/1	Trunk			1	1	Ľ
1/0/2	Trunk	2-16	2-298	1	1	Ľ
1/0/3	Trunk			1	1	Ľ
1/0/4	QinQ			1	1	Ľ
1/0/5	Trunk			1	1	Ľ

## Add MAC-based VLAN

VLANs are divided according to the source MAC address of the data frame. Through the configured MAC address and VLAN mapping table, when the switch receives an untagged frame, it adds the specified VLAN tag to the data frame according to the mapping table. Note: This is only effective for Hybrid ports.



VLAN						
VLAN Port S	ettings Port Men	bers Voice VLAN	N OUI MAC VLAN	Protocol VLAN		
Add Dele						
MAC Address			Add MAC VLAN	×	802.1p	Operation
	() Th	e MAC address must be	a unicast address.			
		*MAC Address	: : :			
		★Mask Length Valid range is 9-48				
		48				
		•VLAN Please select		~		
		<b>≱</b> 802.1p				
		Valid range is 0-7				
			Cancel OK			
	· P.					
Port Settings > E	dit					
	Port		1/0/3			
	<b>∗</b> Link Type		Hybrid		~	
	<b>∗</b> PVID		1			Valid range is 1-4094
	Accept Frame Ty	70.0	All Tag Only	Untag Only		
		pe -		O ontag only		
	TPID		0x8100		~	
	Ingress Filtering					
	VLAN Translatio	n				
	MAC VLAN					
	Protocol VLAN					
			Cancel OK			

### • Add protocol-based VLAN

VLANs are divided according to the protocol (family) type and encapsulation format to which the data frame belongs. Through the configured protocol field and VLAN mapping table in the Ethernet frame, when the switch receives an untagged frame, it adds the specified VLAN Tag according to the mapping table.

Note: This is only effective for Hybrid ports.



VLAN			
VLAN Port Settings	Port Members Voice VLAN OUI MAC VLAN	Protocol VLAN	
Add Delete			
Protocol Index	Frame Type	Protocol Type Value	Operation
	Add Protocol VLAN	×	
	Protocol Index		
	0.		
	Frame Type		
	Ethernet II	×	
	Protocol Type Value Valid range: 0x600-0xFFE		
	Cancel OK		
		_	

ort Settings > I	Edit		
	Port	1/0/2	
	+Link Type	Hybrid	
	*PVID	1	Valid range is 1-4094
	Accept Frame Type	All	
	TPID	0x8100 ~	
	Ingress Filtering		
	VLAN Translation		
	MAC VLAN		
	Protocol VLAN		
	◆Protocol Template	Protocol Template VLAN 0 802	Add
		Сапсе	

#### Add VLAN translation

By modifying the VLAN Tag carried in the message, different VLANs can be mapped to each other. Note: a. This feature is only effective for Trunk and Hybrid ports.

b. Configuration restrictions:

(1) The GWN7800 series switches only support the 1 to 1 function of the outer VLAN (including 1:1 and N:1).

(2) The outer VLAN allows the configuration of a single VLAN or a VLAN range. Only one outer VLAN can be configured after mapping, and it must be a VLAN to which the port has been added.

(3) The total number of VLAN mapping groups supported by the switch is 256, and the maximum



number of VLAN mapping groups supported on a single port is 128.

(4) The total number of VLAN ranges supported by the switch is 16, and the maximum number of VLAN ranges supported on a single port is 16.

Port Settings > Edit		
Port	1/0/2	
*Link Type	Trunk	×
*PVID	1	Valid range is 1-4094
Accept Frame Type	All Tag Only Untag Only	
TPID	0x8100	v
VLAN Translation		
Ingress		
VLAN Mapping1		
*Outer VLAN ③		
<b>∗</b> VLAN after Outer Mapping ⊙		
		Add 😝
	Cancel	

### Add untagged OUI mode for voice VLAN

Compared with the Tagged OUI mode, the Untagged OUI mode is added. The only difference is that the Untagged label is added, and the rest is the same as the Tagged OUI mode.

Voice VLAN		~
*Voice VLAN ID	Disabled Auto Voice VLAN	
CoS/802.1p Priority	Tagged OUI	Valid range is 0-7
CoS Remarking	Untagged OUI	
*Aging Time (Min)	1440	Valid range is 30-65536

• Add gateway priority when using DHCP to get VLAN IP address

The IPv4 interface supports specifying a priority when obtaining a gateway from DHCP; the IPv6 interface supports specifying a priority when obtaining an IPv6 global unicast address gateway from SLAAC, Stateless DHCPv6, and Stateful DHCPv6.

Note: The gateway priority is: statically configured gateway > gateway with a set priority (the smaller the priority value, the greater the priority) > gateway obtained from DHCP on the VLAN interface (VLAN



ID from small to large, first come first served). If the statically configured gateway network segment is the same as any interface network segment, the statically configured gateway takes effect. Otherwise, the effective gateway is selected according to the gateway priority configuration. If the priorities are the same, the gateway with the smaller VLAN ID takes effect first.

S GWN7801				Save	Q   💽 admin +
(2) Overview - VL	AN IP Interface				
⊕ switching vIP	v4 Interface IPv6 Interface IPv6 Router Advertis	sements			
♥ IP ^	MGMT VLAN	VLAN 1			
VLAN IP Interface	IPv4 Default Gateway	1			
DHCP Server		Edit IPv4 Interface ×			
DHCP Relay	VLAN				
ARP. Table	erface Settings				
Neighbor Discovery	Add Delete IPv4 Address		All Types ~		
DNS	IPv4 Interface	DHCP	M	TU	Operation
	Gateway Prio		15		
S Multicast 🗸 🎽	* VLAN 1 2		15	00	
占 Routing ~	*MTU	No. 6515	Total	2 <	1 > 10/page V
L≃ Qo5 ~	Valid range is 12 1500	200-9216			
⊘ Security ~					
👌 Maintenance 🗸 🗸		Cancel OK			
🛞 System 🗸 🗸					
S GWN7801				Save	Q   🚺 admin ~
Overview ~ IPv	/6 Interface > Edit IPv6 Interface				
🌐 Switching 🗸 🗸					
91 (9)	VLAN	VLAN 1			
VLAN IP Interface	IPv6 Enable				
DHCP Server	Link-Local Address	Auto Generate     Manually Configure			
	Global Unicast Address	SLAAC	·		
DHCP Relay	*Gateway Priority	2	Valid range is 2-255		
ARP Table			_		
Neighbor Discovery	♦MTU	1500	Valid range is 1280-921	6	
DNS		Cancel			
😂 Multicast 🗸 <					
പ്പ് Routing V					
QoS ∽					
Security ~					
🖉 Maintenance 🗸 🗸					

## Add default gateway configuration under MGMT VLAN

Configure a default static gateway in the MGMT VLAN and keep the configuration synchronized with the default route next hop address added to the static route.



5	GWN7801				
@	Overview	~	VLAN IP Interfac	e	
	Switching	~	IPv4 Interface	IPv6 Interface IPv6 Router Ad	dvertisements
0	IP	^		MGMT VLAN	VLAN 1 V
	VLAN P Interface			IPv4 Default Gateway	
	DHCP Server				Cancel
	DHCP Relay				
5	GWN7801				
<b>@</b>	Overview	~	VLAN IP Interface	2	
⊕	Switching	~	IPv4 Interface	IPv6 Interface IPv6 Router Adv	vertisements
0	IP	^		MGMT VLAN	VLAN 1 ~
	VLAN IP Interface			IPv6 Default Gateway	
	DHCP Server				Cancel OK
	DHCP Relay				

• Optimize DHCP option 43 configurations for DHCP server

S GWN7801				Save Q   🧕
	~	DHCP Server > Add Address Pool		
Switching	~	♣IP POOI Subnet.		
) IP	^	•Prefix Length		Valid range is 8-30
VLAN IP Interface		Gateway		•
			Ado	•
DHCP Server		Duration (min)	120	Valid range is 1-2880
DHCP Relay		DNS Server		•
		DH3 SCHO	Ado	•
Neighbor Discove	ry	WINS Server		•
DNS		HIRG JEITE	Ado	•
Multicast		Netbios Node Type	~	
S Routing	~	near on note type		
		DHCP Option1		
	ř	DHCP Option	43 🛞	The range is 2-254 (excluding 50-54, 56,
	~			58, 59, 61 and 82)
	~	Туре	ASCII	
	~	Service	Custom ~	
		Option Content		0-255 characters

Supports configuring specified services for DHCP Option 43.



### • Optimize routing table

#### Optimize the destination IP address display and increase the Path Cost value

Routing Table							
IPv4 Routing Table IPv6 R	Routing Table						
Refresh					All Types	<ul> <li>✓ Q Desti</li> </ul>	nation IP Address/Ne
Destination IP Address	Protocol Type	Priority	Cost	Next Hop	Outgoing In	terface	Flags 🕕
0.0.0/0	DHCP	1	0	192.168.80.1	VLAN 1		SFA
192.168.80.0/24	Direct	0	0	0.0.0.0	VLAN 1		SFA
					1	Total 2 <	1 > 10/pag

#### • Add ACL advanced settings, including mirroring, statistic and priority remapping for rule

Statistics: Once the ACL rule is hit, the counting starts. Supports statistics by packet or by byte. Mirror: After selecting the mirror group, you need to go to Maintenance  $\rightarrow$  Diagnosis  $\rightarrow$  Mirror Configuration Observation Port to take effect.

Priority Mapping: After it is turned on, once the ACL rule is hit, the priority of the message will be remapped inside the switch.

ACL > Add ACL			
	Source IP Address	Any Custom	
	Destination IP Address	Any     Custom	
	Тоѕ Туре	Any ~	
	Time Policy	None ~	
	Advanced Settings		
	Count		
	<b>∗</b> Count ID		Valid range is 1-32
	Count Unit	By packet      By byte	
	Mirroring		
	*Mirroring Group	eq:Goto*Maintenance>Diagnostics>Mirroring* to configure the monitor port to take effect	]
	Priority Mapping		
	*Priority		Valid range is 0-7
	Rate Limit	Disabled ~	
		The rate limit function needs to go to "Security→ACL→Rate Limit Settings" to configure the rate limit group to take effect	

#### • Add rate limit by ACL binding to VLAN

Speed limit for VLAN. By binding VLAN to ACL, speed limit is achieved by selecting speed limit group for rules. Once the rule is hit, it will take effect according to the settings of the specified speed limit



group.

▲ACL Name		1~64 characters
Rule Settings		
<b>≱</b> Rule ID	1	Valid range is 1-2147483647. The smaller ID is matched first.
Action	Allow	~
Protocol Type	Any	~
Source IP Address	Any     Custom	
Destination IP Address	Any     Custom	
Тоз Туре	Any	~
Time Policy	Disabled	
Advanced Settings	2	
Count	3	
Mirroring	5	
Priority Mapping	6 7	
Rate Limit	1	^
		ings" to

ACL rule setting speed limit function: select speed limit group.

## VLAN bind ACL:

IPv4 ACL IPv6 ACL	MAC ACL	Port Binding to A	CL VLAN Binding to ACL	Rate Limit Settings		
VLAN	IPv4 A	CL Name		MAC ACL Name		Operation
1						
2	100					
3			Edit	×		
4		VLAN				
5		4				
6		IPV4_ACL				
7		First		~		
8		MAC ACL				
9		MACACL		~		
10						
			Cancel OK		Total 19 < 1 2 >	10 / page ∨ Go to

Speed limit group settings:



S GWN	7801				Save	Q   👤 admin 🗸
		ACL				
Switching		IPv4 ACL IPv6 ACL MAC ACL Port I	Binding to ACL	VLAN Binding to ACL Rate Limit Settings		
		Burst Threshold Group 1	I			
		*Burst Byte (bps)	7108	8480	Enter a value between 128-8388480 th a multiple of 128	at is
		Burst Packet (pps)	10		Valid range is 1-65535	
		Burst Threshold Group 2	2			
⊘ Security		Burst Byte (bps)	7108	8480	Enter a value between 128-8388480 th a multiple of 128	at is
		Burst Packet (pps)	10		Valid range is 1-65535	
	irity		Can	ncel ОК		
	tion					
ACL		Rate Limit Settings				
		Rate Limit Group ID Ra	ate Limit Type	Burst Threshold Group	Rate Threshold	Operation
		1			**	Ľ
IPv6 Sour		2			**	Ľ
Anti Atta		3			**	Ľ
		4				Ľ
		5				Ľ
RADIUS		6				Ľ
TACACS+		7				Ľ
inchest		8				ß

Add import/export IPSG binding table for IP Source Guard

Port Protection Qua	ternary Binding Table					
Add Delete	Refresh Import	Export				
Port	IPv4 Address	MAC Address	VLAN	Туре	Lease Time (s)	Operation
1/0/1	192.168.122.254	00:0B:82:AD:74:5F	2	Static		Ū

• Add IPv6 Source Guard

IPv6 source attack protection is a source IPv6 address filtering technology based on the Layer 2 interface. It can prevent malicious hosts from forging the IPv6 addresses of legitimate hosts to impersonate legitimate hosts and ensure that unauthorized hosts cannot access or attack the network by setting their own IPv6 addresses.

IPv6SG uses the binding table (source IPv6 address, source MAC address, VLAN, and inbound interface binding) to match and check the IPv6 packets received on the Layer 2 interface. Only packets that match the binding table are allowed to pass, and other packets will be discarded.



S GWN7801					Save	Q   💽 admi
	×	IPv6 Source Guard				
Switching		Port Protection Quaterna	ary Binding Table			
	~					
😂 Multicast	Υ.	Port	IPv6 Source Guard	Verification Type	Number of Quaternary Bindings	Operation
홈 Routing	~	1/0/1	Disabled	IPv6		e
		1/0/2	Disabled	IPv6	<b>1</b>	ß
		1/0/3	Disabled	IPv6	11C	Ø
Security	^	1/0/4	Disabled	IPv6	2	ß
		1/0/5	Disabled	IPv6	=	ß
		1/0/6	Disabled	IPv6		Ø
Port Isolation	<	1/0/7	Disabled	IPv6	2	e
		1/0/8	Disabled	IPv6	**	Z
		1/0/9	Disabled	IPv6	-	ß
IP Source Guard	d	1/0/10	Disabled	IPv6		e
	ard	LAG1	Disabled	IPv6	2	e
Anti Attack		LAG2	Disabled	IPv6		ß
		LAG3	Disabled	IPv6	÷	ß
RADIUS		LAG4	Disabled	IPv6		ß
		LAGS	Disabled	IPv6	-	Ø
		LAG6	Disabled	IPv6		ß

### Add MAC bypass authentication

In addition to the previously supported 802.1X authentication, identity authentication management now supports MAC authentication.

🖞 Routing 🗸 🗸	Identity Authentication	Management				
	Port Mode Port	Authentication Sessions Local User of MAC-base	ed			
Security ^		802.1X Authentication				
		MAC Authentication				
		Guest VLAN				
			Cancel			
	Port					
	Edit					
Anti Attack	Port	User Authentication Mode	Authentication Method / Method	Guest VLAN	Authorized VLAN	Operation
DAI	1/0/1	MAC-Based		Disabled	Static	ß
	1/0/2	MAC-Based		Disabled	Static	ß
	1/0/3	MAC-Based		Disabled	Static	e
	1/0/4	MAC-Based		Disabled	Static	Ľ
	1/0/5	MAC-Based		Disabled	Static	Ľ
АЛА	1/0/6	MAC-Based		Disabled	Static	Ľ
	1/0/7	MAC-Based	**	Disabled	Static	Ľ
DHCP Snooping	1/0/8	MAC-Based	**	Disabled	Static	Ľ
	1/0/9	MAC-Based	**	Disabled	Static	Z
	1/0/10	MAC-Based		Disabled	Static	ß
	1/0/11	MAC-Based		Disabled	Static	ß
₿ System - ~	1/0/12	MAC-Based		Disabled	Static	ß

MAC authentication has been added to the port authentication method, and the authentication methods support RADIUS and Local.

By default, the order of port authentication methods is 802.1X, MAC, and the order of authentication methods is RADIUS, Local.



ð			Port Mode > <b>Edit</b>					
	QoS Security			Port	1/0/1			
0	Storm Control			User Authentication Mode 💿	MAC-Based	~		
				Guest VLAN				
				Authorized VLAN ()	Static	×		
				Authentication Method1 😑				
				Authentication Method 💿	MAC Authentication	v		
				Method 🛈	Radius	v	•	
					Local	$\sim$	•	
					1	Add	•	
				Authentication Method2 😑				
	AAA			Authentication Method 💿	802.1X	$\sim$		
	Identity Authentica	tio		Method ()	Radius	v		
								Add
					Cancel			
2								

To add a MAC-based local user, you need to add the MAC address, port control mode, VLAN authorized for use after authentication, re-authentication time, and inactive time.

EP nonneit A	Identity Authentication Management				
Let QoS ~	Port Mode Port Authentication Sessions Local U	ser of MAC-based			
⊘ Security ^	Add Datery Ad	Add Local User of MAC-based	×		
Storm Control	MAC Address Port Control	The MAC address of local user must be an unicast one-	1 (5)	inactive Time (s)	Operation
Port Security			_		
Port Isolation		MAC Address			
ACL		Port Control			
IP Source Guard		Force authentication     Force unauthentication			
IPv6 Source Guard		VLAN (D			
Anti Attack		Valid energy is 1-4054			
DAI -		Reauthentication Time (s) Valut sarge is 300-21.67487647			
RADIUS		3600			
TACACS+		Inactive Time (s)			
A4A		Valid range is 80-65535 60			
Identity Authenticatio					
DHCP Snooping		Cancel	_		
DHCIV6 Snooping					
& Maintenance ~					
🕲 System 🗸					

## • Optimize remote ID and Circuit ID for DHCP Snooping

The Remote ID and Circuit ID of Option 82 can be configured in standard format and private format. Standard format: The default format is set according to TLV (type-length-value). Private format: Only Value is used for setting.



DHCP Snoopir	ng				
DHCP Snoopin;	g Option 82	Port Settings Statistics			
	Format	Normal     Private			
	*Remote ID	c0:74:ad:b9:3b:44		1~63 characters	
		Add Circuit	×		
Circuit ID	Delete	Port 1/0/1  *VLAN  Format  Circuit ID 1-63 characters  Cancel OK	·		Operation

### Add DHCPv6 Snooping

It is used to ensure that the client obtains an IPv6 address or IPv6 prefix from a valid server and can record the correspondence between the DHCPv6 client IPv6 address or IPv6 prefix and the MAC address.

5	GWN7801				_		_			Save	Save Q
£	Routing	~	DHCPv6 Snooping	3							
		~	DHCPv6 Snooping	Option Settings	Port Settings	Statistics					
0	Security	^		DHCPv6 Snooping	(						
				VLAN					Valid range is 1-4094, E	Valid ranze is 1-4094, Example: "5-8, 11	Valid range is 1-4094. Example: "5-8, 11"
				VLAN						will associate VLANs 5, 6, 7, 8 and 11.	
						Cancel	ς				
	DHCP Snooping										
	DHCPv6 Snooping										
ور	Maintenance	~									



#### • Add upgrade by FTP and Explicit FTPS

Network upgrade supports FTP and explicit FTPS. Firmware detection and upgrade are performed by filling in the FTP or explicit FTPS firmware server address.

It also supports DHCP Option to carry FTP or explicit FTPS server address. The device reads and parses it and uses this address for upgrade.

Note: ftp:// protocol header refers to FTP upgrade method, and ftps:// protocol header refers to FTPS upgrade method.

Upgrade				
	(i) Current version: 1.0.5.2			
	Upgrade via Manual Upload			
	Upload Firmware File to Update	Select file to upload	Supported file formats: bin	
	Upgrade via Network			
	Allow DHCP Option 43/160/66 to Override Server ()	Off		
	Firmware Upgrade Protocol 🛈	HTTP	]	
	Firmware Server Path 🛈	TFTP HTTP		
	FTP/Explicit FTPS/HTTP/HTTPS Username	HTTPS FTP		
	FTP/Explicit FTPS/HTTP/HTTPS Password	Explicit FTPS		
	Check/Download New Firmware at Bootup			
	Scheduled Upgrade	Once enabled, the switch will automatically detect and upgrade within the scheduled time		
		Cancel OK Check for Updates		

#### Add connection diagnostics with GWN.Cloud/Manager

When the switch and GWN.Cloud/GWN Manager connection is unstable, the user can log in to the local Web GUI diagnostic page to check the cloud connection status and view related logs.



5	GWN7801									Save 🛛 Q 👘 🔍 admin 🗸
Ø		×	Diagnostics							
0		~	Logs	Ping	Traceroute	Mirroring	Fiber Module	Copper Test	One-click Debugging	Cloud / Manager Connection Diagnostics
0		~								
\$		~								
2		Ý								
Ľ		~						1		
Ø		~								
æ	Maintenance	^								
							The switch	is currently not r	nanaged by Cloud / Mana	ger
		•								
	Backup & Restore									
		ag								
ø		~								

# • Optimize EEE

ලි System

Added actual port status display.

S GWN7801					Save. Q   💽 admin ->
Overview	~	Energy Efficient Ethernet			
Switching	~	Edit			
	~	Port	Configuration Status	Status	Operation
😂 Multicast	~	1/0/1	Disabled	Disabled	ß
금 Routing	÷	1/0/2	Disabled	Disabled	12
		1/0/3	Disabled	Disabled	ß
		1/0/4	Disabled	Disabled	ß
	~	1/0/5	Disabled	Disabled	ß
A Maintenance	^	1/0/6	Disabled	Disabled	ß
Upgrade		1/0/7	Disabled	Disabled	ß
Diagnostics	<	1/0/8	Disabled	Disabled	ß
Backup & Resto	re				
SNMP					
RMON					
LLDP/LLDP-MED	R.				
Energy Saving N	Manag				



#### • Add DST mode for time settings

S GWN7801 🔘 admin ~ C Overview Basic Settings B Switching Basic Info Device Name GWN7801 System Location Default Default System Contact 🗠 Qos Time Settings Additional Maintenance Date & Time Manual (Interview) Automatic (NTP Server) 8 System System Time 2023-12-25 17:18:00 8 NTP Server pool.ntp.org Time Zone (UTC+08:00) Beijing.Shanghai.Chongqing.Hong Kong.Uru... DayLight Saving (DST) Mode Recurring Offset (Min) 60 +Starting Time Ending Time Scheduled Reboot Cancel OK

Added daylight saving time offset setting and automated time configuration.

#### Add HTTPS/SSH port customization

Users use customized HTTPS and SSH ports to access and configure device.

5	GWN7801					Save	Q   🚺 admin ~
Ø	Overview		Access Control				
•			Web Service Manag	sement SSH Remote Access N	Manager Settings		
0				*HTTPS	443	Valid range is 443 and 1024-65535	
\$			•	Inactive Session Timeout (min)	1440	Valid range is 1-1440	
đ				Telnet			
L~				SSH			
0			ſ	•SSH Port	22	Valid range is 22 and 1024-65535	
ß			L			and raige over and rare asso	
ĝ	System	^			Cancel OK		
			c				
	Access Control						
	User Management	:					



• Optimize Manager settings

S GWN7801				
	~	Access Control		
Gwitching	~	Web Service Management SSH Remote Access	Manager Settings	
О ІР	~	Allow DHCP Option 43 to Override ①		
	~	Manager Settings		
	~		-	
	~	Manager Server Address		
	~	Manager Server Port	8443	Valid range is 1-65535
	~		Cancel	
🔞 System	^			
	<			
Access Control				
User Managem	ent			

• Add GWN Manager takeover function

When GWN Manager wants to take over a managed switch, it can force the takeover by entering the switch password.



# FIRMWARE VERSION 1.0.3.8

## PRODUCT NAME

GWN7816(P)

# DATE

12/4/2023

## **FIRMWARE FILE INFORMATION**

GWN7816(P) Firmware file name: gwn7816fw.bin
 MD5 checksum: b568755fddd4286ba98d423e920e9bcf

# **CHANGES/ENHANCEMENT**

• This is the initial firmware for GWN7816(P)



# FIRMWARE VERSION 1.0.3.3

## PRODUCT NAME

GWN7832

# DATE

10/17/2023

## **FIRMWARE FILE INFORMATION**

GWN7832 Firmware file name: gwn7832fw.bin
 MD5 checksum: f4fef887515210fd74574aebd7f55bdd

# **CHANGES/ENHANCEMENT**

• This is the initial firmware for GWN7832



# FIRMWARE VERSION 1.0.1.14

## PRODUCT NAME

GWN7806(P)

# DATE

8/12/2023

## **FIRMWARE FILE INFORMATION**

GWN7806(P) Firmware file name: gwn7806fw.bin
 MD5 checksum: 68748aa8734a8979dff9b8692f1d37e3

# **CHANGES/ENHANCEMENT**

• This is the initial firmware for GWN7806