

GWN781x/783x Switch Firmware Release Notes

IMPORTANT UPGRADING NOTE

- 1. Once GWN781x is upgraded to firmware 1.0.7.x, downgrading to 1.0.3.x or lower firmware version is not allowed.
- 2. GWN781x/783x 1.0.7.71 requires GWN Manager version to be at least 1.1.28.27 or newer.



Table of Content

IMPORTANT UPGRADING NOTE	1
FIRMWARE FILE DOWNLOAD	3
FIRMWARE VERSION 1.0.9.15	4
PRODUCT NAME	
DATE	
FIRMWARE FILE INFORMATION	
CHANGES/ENHANCEMENT	
NEW FEATURE OVERVIEW	5
FIRMWARE VERSION 1.0.7.71	20
PRODUCT NAME	20
DATE	20
FIRMWARE FILE INFORMATION	20
ENHANCEMENTS	20
NEW FEATURE OVERVIEW	21
FIRMWARE VERSION 1.0.1.20	45
PRODUCT NAME	45
DATE	45
FIRMWARE FILE INFORMATION	45
CHANGES/ENHANCEMENT	45
FIRMWARE VERSION 1.0.1.8	46
PRODUCT NAME	46
DATE	46
FIRMWARE FILE INFORMATION	46
CHANGES/ENHANCEMENT	46



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

GWN7811, GWN7811P, GWN7812P, GWN7813, GWN7813P, GWN7830, GWN7831

DATE

8/29/2024

FIRMWARE FILE INFORMATION

- GWN781x Firmware file name: gwn781xfw.bin
 MD5 checksum: 5841770d64aacffaae17ce1ec6e3f5bb
- GWN7830 Firmware file name: gwn7830fw.bin
 MD5 checksum: 5841770d64aacffaae17ce1ec6e3f5bb
- GWN7831 Firmware file name: gwn7831fw.bin
 MD5 checksum: 5841770d64aacffaae17ce1ec6e3f5bb

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.
- Optimized RIP/RIPng.
- Optimized CBS valid range in Queue Shaping.
- Optimized the rate limit groups from 32 to 128 in ACL.
- 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 internal bugs.

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 区面
Port Auto Recovery			
Link Aggregation			
MAC Address Table			
VLAN			
Port Group > Add	Dest Canua		
Port Group 7 Add	Port Group		
		*ID	2 Valid range is 1-32
		Description	0~128 characters
		Click on port to select/un	nselect
		Port	
		2 4	6 8 10 12 14 16 18 20 22 24
		Constant Constants	
		1 3	5 7 9 11 13 15 17 19 21 23 25 26 27 28 gp.
		LAG	
			2 4 6 8 10 12 14
			1 3 5 7 9 11 13
			1 3 3 7 9 11 15
			Cancel OK

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.

Overview VLAN				
Switching VLAN	Port Settings Port Members Voic	CE 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			Cancel	
MAC Address Table	_	l		
VLAN	ц	LDP/LLDP MED		
Spanning Tree		Auto Config		
~ qı 🍥		LLDP Global Settings: LLDP: enabled		
😂 Multicast 🗸 🗸		Port Settings: RXTX : 1/0/1-1/0/10		
💮 Routing 🗸 🗸		TX : None RX : None Disabled: None		
l≃ QoS ∽		LLDP MED Network Policy		
⊘ Security ~		Auto Vioce Network Policy:	enabled	
🖉 Maintenance 🗸 🗸		LLDP MED Port Settings LLDP MED: Enabled : 1/0/1-1/0/1	8	
(§1 System ~		Disabled : None Network Policy TLV: Enabled : 1/0/1-1/0/1 Disabled : None		

• 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
	∗ Path Cost ^①	0			Valid range is 0-65535
	Edge Port	Auto	Enabled	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 OUI	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 ū
	C0:74:AD:00:00:00	FF:FF:FF:00:00:00	Grandstream	e õ
	EC:74:D7:00:00:00	FF:FF:FF:00:00:00	Grandstream	e ū
Link Aggregation	00:E0:BB:00:00:00	FF:FF:FF:00:00:00	3COM	e ū
MAC Address Table	00:03:68:00:00:00	FF:FF:FF:00:00:00	Cisco	e ü
	00:E0:75:00:00	FF:FF:FF:00:00:00	Veritel	e i
VLAN	00:D0:1E:00:00:00	FF:FF:FF:00:00:00	Pingtel	e i
Spanning Tree	c 00:01:E3:00:00:00	FF:FF:FF:00:00:00	Siemens	e i
IP V	00:60:89:00:00:00	FF:FF:FF:00:00:00	NEC/Philips	e i
	00:0F:E2:00:00:00	FF:FF:FF:00:00:00	H3C	e ū
	00:09:6E:00:00:00	FE:FE:FE:00:00:00	Avaya	e ū
	00:04:F2:00:00:00	FF:FF:FF:00:00:00	Polycom	e ū
	64:16:7F:00:00:00	FF:FF:FF:00:00:00	Polycom	e ū
	00:88:83:00:00:00	FF:FF:FF:00:00:00	Cisco	e ū

• Added IP configuration for MGMT VLAN

🕸 System 🗸 🗸

VLAN IP Interface

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.

IPv4 Interface	IPv6 Interface	IPv6 Router Advertisements	MGMT VLAN		
		MGMT VLAN		VLAN 1 ~	
		IPv4 Address	Settings		
		Address Type		Static IP	
		*Gateway Priori	ty	2	The valid range is 2-255. The smaller the value, the higher the priority.
		IPv6 Address	Settings		
		Enable			
				Cancel	
		Managemen	t Address		
		MGMT VLAN		VLAN 1	
		Status		UP	
		IPv4			
		Address Typ	e	Dynamic	
		IP Address		192.168.80.123	
		Mask Length	1	24	
		Gateway		192.168.80.1	
		IPv6			
		Enable Statu	IS	Disabled	
		Link-Local Ac	ddress	-	

• 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.



	*	IPv4 ACL > Add ACL			
Switching	÷		ACL Name		1-64 characters
	~		Rule Settings ③		
	×		•Rule ID	1	Valid range is 1-2147483647. The smaller
	¥				ID is matched first.
	÷		Action	Allow	
Security	~		Protocol Type	Drop Allow	
Storm Control	1		Source IP Address	Shut Down	
			Destination IP Address	Redirect to Interface	
			Tos Type	Any ~	
ACL			Time Policy	None	
IP Source Guar	rd		Advanced Settings		
	uard 🖪		Count		
			Count Unit	By packet By byte	
			Mirroring		
			Priority Mapping		
			Rate Limit	Disabled ~	
				The rate limit function needs to go to "Security-+ACL-+Rate Limit Settings" to	
Identify Author	oticatio			Cancel OK	

• 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		
ate Limit Settings				
Rate Limit Group ID		Rate Limit Type	Rate Threshold	Operation
21		**		ß
22				ľ
23				ß
24		**		ľ
25		**		ľ
26		**		ľ
27			**	
128		-	-	ß
			Total 128 < 1 11 12	2 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	×		E <i>P</i>
□ 4	VLAN			I ?
5	3			I ?
6				I d
7	IPv4 ACL v			I P
c 🗌 8				I d
9	MAC ACL			C P
10	None ~			I ?
	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 Routing ~	IP Source Guard				
± Qa5	Port Protection Quaternary Binding Table				
🤉 Security 🔷 🔨	Add Delete Refresh Import Export	Add Quanternary Binding ×			
Storm Control	Port IPv4 Address/Mask	Port	Type	Lease Time (s)	Operation
Part Security	1/0/1 192.168.122.254/255.255.2	1/0/1 ~	Static		Û
Port isolation		P Address Pivt Stemat		total 1 🖉	1 > 10/page ~
ACL.					
IP Source Guard		Mask Pul format			
IPv6 Source Guard					
Anti Attack	6.:	MAC Address The MAC address must be a unicasi address.			
DM.					
RADIUS		Mask FF : FF : FF : FF : FF			
TACACS+		VLAN			
(AMA):		Vahid ranger is 1-4094			
802.1X					
DHCP Snooping		Cancel Ox			
DHCPV6 Snooping					
2 Maintenance ~					



🐣 Routing 🗸 🗸	IPv6 Source Guard
	Port Protection Quaternary Binding Table
⊘ Security ^	Add Quanternary Binding $ imes$
Storm Control	•Port
Port Security	101 ~
	PAddress IP-6 format and must be a valid unicast address
ACL	Jrefa Length
IP Source Guard	Vietra Length Vialid range is 1-128
IPv6 Source Guard	MAC Address
Anti Attack	The MAC address must be a unicast address.
DAI	I I I I I I I I I I I I I I I I I I I
RADIUS	474 : 474 : 474 : 474 : 474 : 474
TACACS+	•YAN Valid range is 1-4994
AAA	Valid Langer is 1-dotre
802.1X	Cancel
le Maintenance ∨	

• 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.



룹 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.
				1.100	will associate VLANs 5, 6, 7, 8 and 11.
				Cancel OK	
	¢				
802.1X					
DHCP Snooping					
DHCPv6 Snooping					
열 Maintenance 🗸	DHCPv6 Snooping				
Maintenance ∨ A antiperiod of the second		Option Settings Port Sett	ings Statistics		
		Option Settings Port Sett	DHCPv6 Snooping (2	
Maintenance √ Maintenance Maintenance Maintenance Maintenance Maintenance Maintenance Maintenance Maintenance Maintenance Maintenance Maintenance Maintenance		Option Settings Port Sett	DHCPv6 Snooping (3	
Maintenance ✓ Maintenance ✓ Maintenance ✓ Maintenance ✓ Southag ✓ QoS ✓ Storm Control Port Security		Option Settings Port Sett	DHCPv6 Snooping (Entries Fixed for DHCPv6 Snooping ©	٥	Valiforges 15 8840
Maintenance Maintenance Maintenance Cods Cods Cods Port Security Port Isolation		Option Settings Port Sett	DHCPv6 Snooping (Entries Fixed for DHCPv6 Snooping ©	300	Vold range is 15:6840 Vold range is 15:6840 Wold rough is 3,56840 Wold rough is 3,56840
Maintenance Aninenance Anin		Option Settings Port Sett	DHCPv6 Snooping C Entries Fixed for DHCPv6 Snooping © PRed Duration (5)	300	
Maintenance > Routing > Routing > Backing > Port Security > Port Isolation ACL		Option Settings Port Sett	DHCPv6 Snooping C Entries Fixed for DHCPv6 Snooping © PRed Duration (5)	300	
Maintenance > Reating >		Option Settings Port Sett	DHCPv6 Snooping C Entries Fixed for DHCPv6 Snooping © PReed Duration (5)	500	
Maintenance > Routing > Recently > Sterm Control > Porticulation A ACL Postree Guard Posture Guard Anti Attack		Option Settings Port Sett	DHCPv6 Snooping C Entries Fixed for DHCPv6 Snooping © PReed Duration (5)	500	
Maintenance > Insuring >		Option Settings Port Sett	DHCPv6 Snooping C Entries Fixed for DHCPv6 Snooping © PReed Duration (5)	500	
Maintenance > Insuring > Storm Control > Port Isolation A ACL I InSurance Guard A Artil Attack		Option Settings Port Sett	DHCPv6 Snooping C Entries Fixed for DHCPv6 Snooping © PReed Duration (5)	500	
Maintenance > Resting >		Option Settings Port Sett	DHCPv6 Snooping C Entries Fixed for DHCPv6 Snooping © PReed Duration (5)	500	
Maintenance > Routing >		Option Settings Port Sett	DHCPv6 Snooping C Entries Fixed for DHCPv6 Snooping © PReed Duration (5)	500	
Maintenance Stantance Qués Qués Storm Courad Ports Sourtor Ports Roating Ports Roating <th></th> <th>Option Settings Port Sett</th> <th>DHCPv6 Snooping C Entries Fixed for DHCPv6 Snooping © PReed Duration (5)</th> <th>500</th> <th></th>		Option Settings Port Sett	DHCPv6 Snooping C Entries Fixed for DHCPv6 Snooping © PReed Duration (5)	500	
Number Number		Option Settings Port Sett	DHCPv6 Snooping C Entries Fixed for DHCPv6 Snooping © PReed Duration (5)	500	
Routing N Standard N Standard N Standard N Standard N Part Security N Part Attack N		Option Settings Port Sett	DHCPv6 Snooping C Entries Fixed for DHCPv6 Snooping © PReed Duration (5)	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 Wat	chdog Traceroute Mirroring Fibe	Module Copper Test One-cli	ck Debugging Mana	gement Platform Connection Dia
¢		×	Log Server Address Refresh	Clear All Export Settings			
k		~	Start date End date	Settings	×		
0		× 1	Details	Minimum Log Level ()		Level	Generated Time
2	Maintenance	~	SYSTEM-5-CPU_INFO: utilization	Notice	¥	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	K	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		Notice	Jul 30 2024 18:17:52
			DHCP_SNOOPING-5-UNTRUSTED_DI C0:74:AD:CC:DF:C0 and opcode OFF	ROP: Untrusted deny. Packet drop: VLAN 1, in: ER	erface Ethernet1/0/1, chaddr	Notice	Jul 30 2024 18:16:59
					Total 1533 🧹 🚺	2 3 154	> 10/page V Go to
	Energy Saving Man	BRAN					

• 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		
	Routing		▶IP Address		IPv4 format
			Packet Sending Interval (s)	30	Valid range is 30-3600
0			≵ Delay Time (s)	60	Valid range is 60-3600
ß	Maintenance		∗ Retry Times	2	Valid range is 1-10
	Upgrade		Shutdown Interval (s)	5	Valid range is 5-30
	Diagnostics			Cancel	
	Backup & Restore				
	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



igs	Ping	Ping Watchdog	Traceroute	Mirroring	Fiber Module	Copper Test	One-click Debugging	Management Platfo	orm Connection Diagnostics		
			Remot	te VLAN ()	1	2			Valid range is 1-4094, Example: "5-8, 11" will associate VLANs 5, 6, 7, 8 and 11.		
						Cancel	ок				
		de	Role		Ingress Mirroring	E	gress Mirroring	Output Port	Monitor Port	Remote VLAN	Operation
	oup Mo SP4		Role		Ingress Mirroring	E	gress Mirroring	Output Port	Monitor Port	Remote VLAN	Operation
-	Mo	IN									
Irroring Gr Group 1 2	Mo SP/	in In	-		-	-		1	-	-	23

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 Mode	1 RSPAN ~
	Role	Source Switch
		Source Switch Destination Switch
	Port	
	2 4 6 8 1 3 5 7	10 12 14 16 18 20 22 24 9 11 13 15 17 19 21 23 25 26 27 28 9 11 13 15 17 19 21 23 25 26 27 98
	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 ()		
	Rule ID	1	Valid range is 1-2147483647. The smaller ID is matched first.
	Action	Allow	v
	Protocol Type	Any	~
	Source IP Address	Any Custom	
	Destination IP Address	Any Custom	
			v
	Тоз Туре	Any	
	Time Policy	None	~
	Advanced Settings		
		_	_
	Mirroring		
	*Mirroring Group	Group 3	~
		Go to "Maintenance>Diagnostics>Mirroring" to configure take effect	
	Priority Mapping		
	Rate Limit	Disabled	~
		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			Ľ 🖉
2	-		l d
3	Edit	× -	I <i>P</i>
□ 4	VLAN		I ?
5	2		I 🖉
6			I 🖉
7	IPv4 ACL test	-	I 🖉
8	test	·	I 2
9	MAC ACL		I 2
□ 10	None	·	e 2
	Cancel OK	-	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.

Overvier			SNMP								
Switching			Global Settings	View Management	Group Mana	agement	Community Manager	ment Use	Management	Notification Management	Trap Event
9 IP					A	uthenticatio	on failed				
😂 Multicas					P	ort Up/Dow	n				
룹 Routing					C	old Start					
🗠 QoS					w	/arm Start					
Security					5	TP Bridge					
Amend Amend					C	PU					
Diagnos		Q			м	Ionitor					
	& Restore	Ŭ			Pr	ort ErrDisab	ble				
SNMP					М	IAC Address	s Notification				
RMON					P	ort Security					
LLDP/LL	DP-MED				L	ogs					
Energy	Saving Manag				V	LAN Creatio	n				
Alert					vi	LAN Deletio	n				
ĝ System					C	onfiguration	n Distribution				
								Cancel	ОК		

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	d	
© IP	~			Access Control				
😂 Multicast	~				Cancel OK			
പ്പ് Routing	~							
l∠ QoS	~	Rule	an ail anna an dalach da da	and other for much and of any inter and VI AN	l interfaces of the rules, with the lowest priority			
Security	~			ped rules for each set of services and vul-in	a internaces of the nules, with the lowest phongy			
🔑 Maintenance	~		Delete All					
😵 System	^	Rule ID	Service	Action	IP Address	Mask	VLAN Interface Operation	
Basic Settings	¢				1960			
Access Control					1			
User Management					No Data			
Time Policy								
1588v2 TC Beta								
Management A0	CL of H	lardware-based > Ac	bb					
			*Rule ID				Valid range is 1-2147483647. The smaller	
							ID is matched first.	
			Service			~		
			Action	۲	Allow O Drop			
			≱IP Address				IPv4 format	
			Mask①				IPv4 format	
			*VLAN Interf	ace		~		
					Cancel OK			



Overview Access Control			
Switching Web Service Manage	ment SSH Remote Access Management Platform	m Settings Management ACL of Hardware-based Management ACL of Softwa	re-based
© IP			
😂 Multicast 🗸 🗸			
🖺 Routing 🗸		1.00	
Lee Qos v		- The second sec	
⊘ Security ~			
🔑 Maintenance 🗸 🗸			
System	By applying ACL for verificatio	n, 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 ()		
	*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	
	1 3 5 7	9 11 13 15 17 19 21 23	25 26 27 28 ^{52P+} ^{52P+} ^{52P+} ^{52P+}
	LAG		
		2 4 6 8 10 12 14	
		1 3 5 7 9 11 13	
		Cancel OK	

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.



Ø	Overview	×	Access Control				
⊕		~	Web Service Management	SSH Remote Access	Management Platform Settings	Management ACL of Hardware-based	Management ACL of Software-based
0		~			Allow DHCP Option 43 to Override Management Server 💿		
		~			Management Server Settings		
•		~					
<u>~</u>		~			Management Platform	 GWN Manager GWN Router 	
ଡ		~			*Management Server Address		
	Maintenance	~			Management Server Port	7443	
-		Ť				Cancel OK	
¢	System	^				Cancel	
	Basic Settings	<					
	Access Control						
	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).

(2) Overview ~	1588v2 TC			
Switching ~		1588v2 TC		
© IP ~		Device Class	€2E TC ● P2P TC	
😂 Multicast 🗸 🗸				
🖻 Routing 🗸 🗸		Message Encapsulation Mode	MAC UDP UDP over IPv6	
L∠ 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	D	nabled	ß
Time Policy	1/0/2	D	sabled	Ľ
1588v2 TC Beta	1/0/3		nabled	ľ
	1/0/4		tabled	
	1/0/5		sabled	ľ
	1/0/7		sabed	C
	1/0/8		tabled	Ľ
	1/0/9	D	icolded	F2/1

• Added recovery function

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



FIRMWARE VERSION 1.0.7.71

PRODUCT NAME

GWN7811, GWN7811P, GWN7812P, GWN7813, GWN7813P, GWN7830, GWN7831

DATE

08/05/2024

FIRMWARE FILE INFORMATION

- GWN781x Firmware file name: gwn781xfw.bin
 MD5 checksum: aacbc68ce57d3e5331691bc1bc16c5d1
- GWN7830 Firmware file name: gwn7830fw.bin
 MD5 checksum: aacbc68ce57d3e5331691bc1bc16c5d1
- GWN7831 Firmware file name: gwn7831fw.bin
 MD5 checksum: aacbc68ce57d3e5331691bc1bc16c5d1

ENHANCEMENTS

- 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.
- 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 refresh IP address when using DHCP to get VLAN IP address.
- Added gateway priority when using DHCP to get VLAN IP address.
- Added default gateway configuration under MGMT VLAN.



- Added support for OSPFv3.
- Added IP/IPv6 unicast routing on/off (only CLI).
- 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 MAC bypass authentication.
- Added DHCPv6 Snooping.
- Added upgrade by FTP and Explicit FTPS.
- Added connection diagnostics with GWN.Cloud/Manager.
- Added DST mode for time settings.
- Added HTTPS/SSH port customization.
- Added GWN Manager takeover function.
- Added port group. (only CLI).
- Added 1588v2 P2P TC (only CLI).
- Added support to see switch clients and other information.
- Added support for 12 VTY (SSH or telnet) sessions
- 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.
- Fixed issue that network is not stable when ethernet cable is very long.
- Expanded DHCP leases range up to 11520 min.
- Some internal bugs fixed.

NEW FEATURE OVERVIEW

• 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.



ø	GWN7801							Sa	ve Q 💽 admin ~
		~	VLAN IP Interface			IPv	4 Interface		0
		~	IPv4 Interface IPv6 Interface IPv6 I	Router Advert	tisements	0	IP		
ا @		^	MGMT VLAN		VLAN 1		IP > VLAN IP Interface > IPv4 I	nterface	
			IPv4 Default Gateway						
	DHCP Server				Cancel	DK			
					Cancer				
			Interface Settings						
		,	Add Delete				All ~ A		VLAN/IP Address
			Loopback1	Status 🛈 UP	Туре		IPv4 Address	MTU	Operation
		~ <	Loopback1 * VLAN 1	UP	Static		192.168.80.201/24	1500	
		~						Total 2	< 1 > 10/page V
		~							
		~							
		~							
		~							
				(© 2023 Grandstream Net	works, Inc. Grandstr	eam 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.

GWN7801						Sa	we Q 🧕
Overview	^	System Info					
System Info		Basic Info		Resource Status			
		Device Name System Location	GWN7801	60%			33%
	ž	System Contact	Default	50%			CPU Usage
	~	MAC Address System OID	C0:74:AD:B9:3B:44 1.3.6.1.4.1.42379	30%			60% Memory Usage
	ž	Part Number Serial Number	9640004612A 20VXU28N90B93B44	10%			
	~ <	MGMT VLAN IPv4 Address IPv6 Global Unicast Address IPv6 Link Local Address	VLAN 1 192.168.80.201 :: fe80::c274:adff;feb9:3b44	0% 15:48:10 15:48:21 15:48: Device Temperature 33°C	31 15:48:41 15:48:5	61 15:49:01	
		IPv4 Default Gateway IPv6 Default Gateway	192.168.80.1 fe80::96a6:7eff:fe69:7bf1	System Events	•		
		System Time	2023-12-23 15:48:58 UTC+8:00	崔 Emergency	0 >	🤨 Critical	
		System Uptime System Version	0 hours, 10 minutes 1.0.5.2	🐥 Alert	2 >	Error	
		Hardware Version	V1.2A	Warning	22 >	Information	
		Boot Version	3.6.9.55156	Notification	206 >	Debug	

• 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%			34% 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	 Emergency Alert Warning 	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 Q 🕕 admin
Overview	 Port Info 		
Port Info			
Switching	 Click on the p 	ort above to view port information	
	U Basic In	fo	Neighbor Info
S Multicast	- Port Na	me: 1/0/1	Hostname:
	Port De	scription:	Device ID:
	Y Port Sta	tus: Down	IPv4 Address:
	Speed:	Auto	IPv6 Address:
	Duplex	Mode: Auto	Manufacturer:
	Flow Co	ntrol: Disabled (Off)	Current Rate:
	Jumbo I	irame: 9216	Current Pkts/Bytes:
	~		Up Time: ···
	Statistic	5	O PoE Power Supply 0
	< InOctet	. 0	
	InUcast		Interval 10 minutes ~
	InNUca		
	InDiscar		
	OutOct		1 = 1/2
	OutUca		0.8 mW
	OutNUc		
	OutDisc		0.6 mW
	InMulti		0.4 mW
	InBroad	castPkts: 0	0.2 mW
		ticastPkts: 0	
		adcastPkts: 0	0 m/N 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	QI	💽 admin 🗸
(?) Overview		Port Basic Setting	s > Edit Port					
Switching	^		Port	1/0/1				
Port Basic Setting	S		Port Type	Copper				
Port Statistics			Description		0-128 characters			
Loopback Detection			Port Enable	Enable Disabled				
Port Auto Recover								
Link Aggregation			Scheduled enabled	Only-Workday ^				
MAC Address Tab			100	None Only-Workday				
VLAN			10.000	G Add				
Spanning Tree		< c	Flow Control	Disabled Enabled Auto Flow Control setting will not take effect if Duplex Mode is set to "Half".				
© IP				Cancel				
Multicast								
중 Routing								
L∼ QoS								
Security	~							
S GWN7801	_					Save	QI	👤 admin ~
Overview		Port Settings >	Edit Port					

SWN7801			Save	Q U admin v
Overview ~	Port 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	Upilia	Only-Workday		
MAC Address Table	(formain teal	S Add		
VLAN		Cancel		
Spanning Tree	r.			
♥ IP ~				
😂 Multicast 🗸 🗸				

• Add more port statistics info

Support viewing port Private MIB information.



)Overview 🗸	Port Statistics						
Switching ^		Chatletics inter al (c)	10		_		
Port Basic Settings			Port:1/0/1		×		
Port Statistics	Statistics	Refresh Clear					
Loopback Detection	Clear All Port	Inte	erface Etherlike RMON	Private	utOctets	OutPackets	Oneration
Port Auto Recovery	1/0/1	RX_etherStatsUndersizeDr	opPktsRT 0		748971	35826	
Link Aggregation	1/0/2	RX_etherStatsPkts1519toM	axOctetsRT 0		/403/1		00
	1/0/3	TX_etherStatsPkts1519toM	axOctetsRT 0				
MAC Address Table	1/0/4		0				
VLAN	1/0/5						
Spanning Tree <	1/0/6						
IP V	1/0/7						
	1/0/8	-					
Multicast 🗸 🗸	1/0/9						
] Routing 🗸 🗸	1/0/10						
QoS V	LAG1						
	LAG2						
Security 🗸	LAG3						
Maintenance ~	LAG4						
System 🗸 🗸	LAG5				-		
- system	LAG6						

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.

	~	Loopback Detec	tion				
Switching	^		Loopback Detection				
Port Basic Setting	s						
				Cancel OK			
Loopback Detect	on	Port					
Port Auto Recove	y.	Edit Re	fresh				
Link Aggregation	3	Port	Loopback Detection	Detection Status	Port Status	Time Left (s)	Operation
		1/0/1	Disabled	Disabled	normal	0	Ľ
MAC Address Tal	ble	1/0/2	Disabled	Disabled	normal	0	ß
		1/0/3	Disabled	Disabled	normal	0	ß
	¢	1/0/4	Disabled	Disabled	normal	0	ß
	~	1/0/5	Disabled	Disabled	normal	0	ß
		1/0/6	Disabled	Disabled	normal	0	ß
		1/0/7	Disabled	Disabled	normal	0	Ľ
දි Routing	× .	1/0/8	Disabled	Disabled	normal	0	ß
	~	1/0/9	Disabled	Disabled	normal	0	ß
	~	1/0/10	Disabled	Disabled	normal	0	ß
	5	LAG1	Disabled	Disabled	normal	0	Ľ
	22.00	LAG2	Disabled	Disabled	normal	0	12
	~	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					
#	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	e Q 👤 admir
	~	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
	ction	1/0/2	Trunk				1	Ľ
		1/0/3	Trunk		Edit Port Member	×	1	Ľ
	very	1/0/4	QinQ	Port			1	C
	m	1/0/5	Trunk	1/0/4			1	Ľ
	abla	1/0/6	Trunk	Link Type			1	Ľ
MAC Address 1	uore	1/0/7	Trunk	QinQ			1	Ľ
		1/0/8	Trunk	↓ Untagged VLAN			1	Ľ
	<	1/0/9	Trunk	1			1	Ľ
	I	1/0/10	Trunk	PVID			1	Ľ
		LAG1	Trunk	QinQ port. Same as Unt	agged VLAN		1	Ľ
	~	LAG2	Trunk	1			1	C
	~	LAG3	Trunk				1	Ľ
	<i>.</i>	LAG4	Trunk	0	Cancel OK		1	Ľ
	Ť,	LAG5	Trunk			1	1	Ľ

• 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	itocol VLAN		
Port	Link Type	Tagged VLAN	Trunk Allowed VLANs	Untagged VLAN	PVID	Operation
1/0/1	Trunk		Edit Port Member	×	1	Ľ
1/0/2	Trunk				1	ľ
1/0/3	Trunk	Port			1	ľ
1/0/4	QinQ	1/0/5			1	ß
1/0/5	Trunk	Link Type			1	ß
1/0/6	Trunk	Trunk			1	Ľ
1/0/7	Trunk	Trunk Allowed VLANs		1	C	
1/0/8	Trunk	Enter "5-8, 11" to associa	ate 5 VLANs of "5, 6, 7, 8 and 11".	_	1	C
1/0/9	Trunk			_	1	C
1/0/10	Trunk	Untagged VLAN 1		_	1	C
LAG1	Trunk	1		_	1	C
LAG2	Trunk	PVID Trunk port. Same as Unt	agged VI &N		1	Ľ
LAG3	Trunk	1	1992-11 12 13		1	Ľ
LAG4	Trunk				1	Ľ
LAG5	Trunk	c	Cancel OK		1	Ľ
LAG6	Trunk				1	Ľ
LAG7	Trunk			1	1	ß

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		~		
		≱ 802.1p				
		Valid range is 0-7				
			Cancel OK			
	· P.					
Port Settings > E	dit					
	Port		1/0/3			
	∗ Link Type		Hybrid		~	
	∗ 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	_	
	Сапсе		

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	~
VLAN Translation		
Ingress		
VLAN Mapping1		
*Outer VLAN ()		
*VLAN after Outer Mapping ①		
L		Add 😑
	Cancel ОК	

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	Untagged OUI	~
*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 refresh IP address when using DHCP to get VLAN IP address

When the VLAN IPv4 interface uses DHCP to obtain an IP address, or the VLAN IPv6 uses "Auto Generate" to obtain a link-local address, or "Stateful DHCPv6", "Stateless DHCPv6", or "Stateless Auto Configuration" to obtain a global unicast address, re-acquisition of the IP address is supported.



VLAN IP Interface					
IPv4 Interface IPv6 Interface I	Pv6 Router Advertisements MGMT	[VLAN			
Add Delete				All	
IPv4 Interface	Status 💿	Туре	IPv4 Address	MTU	Operation
Loopback1	UP	Static		1500	C i C
* VLAN 1	UP	Dynamic	192.168.80.123/24	1500	e i C
	[Confirm to get IP address again? Once successfully obtained, the IP address may be changed Cancel OK			Tool 2 < 1 > 10/page ∨

• 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.

5	GWN7801				Save	Q 💽 admin 🛩
(?)			VLAN IP Interface			
⊕			IPv4 Interface IPv6 Interface	Pv6 Router Advertisements		
0			MGMT VLAN	VLAN 1		
			IPv4 Default Gat			
				Edit IPv4 Interface ×		
				VLAN		
			Interface Settings	VLAN 1		
			Add Delete	IPv4 Address Type		
			IPv4 Interface		MTU	Operation
			Loopback1	Gateway Priority Valid range is 2-255	1500	
		× 1	* VLAN 1	2	1500	e ti
4				MTU	fotal 2 🧹	1 > 10/page ~
lex.				Valid range is 1280-9216		
0				TUNY		
				Cancel		
			100 C			
193						



٢	GWN7801						Save Q 👤	admin ~
Q			IPv6 Interface >	Edit IPv6 Interface				
€	Switching			VLAN	VLAN 1			
Ģ) IP			IPv6 Enable				
	VLAN IP Interface				_			
	DHCP Server			Link-Local Address	Auto Generate Manually Configure			
	DHCP Relay			Global Unicast Address	slaac ~			
	ARP Table			*Gateway Priority	2	Valid range is 2-255		
	Neighbor Discovery			 ∎MTU	1500	Valid range is 1280-92	16	
		,		● MTU	1500 Cancel OK	Valid range is 1280-92	116	
Q))	Neighbor Discovery		¢	₽MTU		Valid range is 1280-92	16	
	Neighbor Discovery		c	•МТU		Valid range is 1280-92	16	
ľ	Neighbor Discovery DNS	~	c	"МТU		Valid range is 1280-92	16	
د لا	Neighbor Discovery DNS Multicast	×	c	∎MTU		Valid range is 1280-92	16	
© F	Neighbor Discovery DNS Multicast Routing QQS	~	¢	∎МТ∪		Valid range is 1280-92	16	

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.

S GWN7	7801				
🕜 Overview		VLAN IP Interfac	e		
Switching		IPv4 Interface	IPv6 Interface IPv6 Router A	dvertisements	
© IP	^		MGMT VLAN	VLAN 1	~
VLAN P Ir	nterface		IPv4 Default Gateway		
DHCP Ser	ver			Cancel OK	
DHCP Rel	ay				
S GWN7	7801				
GWN7		VLAN IP Interface	e		
		VLAN IP Interface	e IPv6 Interface IPv6 Router Ad	lvertisements	
 Overview 				Ivertisements VLAN 1	×
OverviewSwitching	• • •		IPv6 Interface IPv6 Router Ad		~
 Overview Switching IP 	, v , v nterface		IPv6 Interface IPv6 Router Ad		~

• Optimize DHCP option 43 configurations for DHCP server

Supports configuring specified services for DHCP Option 43.



S GWN7801			Save Q 💽 admin -
⑦ Overview ~	DHCP Server > Add Address Pool		
🕀 Switching 🗸	#IP POOL SUDNEL		
Ø IP ^	•Prefix Length		Valid range is 8-30
VLAN IP Interface	*Gateway		•
DHCP Server		Ado	a 🖸
	Duration (min)	120	Valid range is 1-2880
DHCP Relay	DNS Server		•
ARP Table		Ado	• •
Neighbor Discovery	WINS Server		•
DNS		Ado	•
😂 Multicast 🗸 🗸	Netbios Node Type	~	
දි Routing 🗸			
L∠ QoS ∨	DHCP Option1		
⊘ Security ∨	DHCP Option	43 🛞	The range is 2-254 (excluding 50-54, 56, 58, 59, 61 and 82)
ب Maintenance ۷	Туре	ASCII ~	
	Service	Custom	
Ø System ∽	Option Content		0-255 characters
	opton content		An Audio Scheller Ander B
			Add 😁
		Cancel Ок	

• Optimize routing table

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

Routing Table									
IPv4 Routing Table IPv6 F	Routing Table								
Refresh					All Types	~	Q Destinati	on IP A	ddress/Nex
Destination IP Address	Protocol Type	Priority	Cost	Next Hop	Outgoing Ir	nterfa	ce	Flags	0
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	
						Total 2	< 1	>	10/page ∨

Add OSPFv3

OSPFv3 is an OSPF routing protocol running on IPv6. It divides the autonomous system AS into one or more logical areas and publishes routes in the form of LSA.

Globally set parameters such as router ID, SPF calculation, and LSA. After establishing a full connection with the neighbor, if the router ID is modified, the OSPFv3 process must be restarted for it to take effect again.



OSPFv3		
Router ID 0		IPv4 format
Route Administrative Distance 💿		
SPF Calculation		
*Waiting Interval (ms)	0	Valid range is 0-500000
Minimum Interval (ms)	50	Valid range is 0-600000
*Maximum Interval (ms)	5000	Valid range is 0-600000
LSA Parameters		
*Receive Time (ms)	1000	Valid range is 0-600000
External Route Import		
Route Type	Direct Static RIPng	
	Cancel OK Reboot OSPFv3	

Set interface parameters, including the region to join, network type, etc.

Interface Settings > Edit Interface

Interface	VLAN 1		
OSPFv3			
Network Type	Broadcast	~	
Interface Suppre	ssion		
▶MTU	1500		Valid range is 1280-9216
Ignore MTU Valid	lation		
LSA Retransmiss	ion Interval (s) 5		Valid range is 1-65535
LSA Transmission	n Delay (s) 1		Valid range is 1-800
∗ Hello Interval (s)	10		Valid range is 1-65535
*Neighbor Expirat	ion Interval (s) 40		Valid range is 1-65535
*Cost	10		Valid range is 1-65535
*Priority	1		Valid range is 0-255
	Cancel	ок	

Set the zone parameters to which the interface joins.



OSPFv3									
Global	Area Settings	Interface Settings	Neighbor Info	Database Info					
Area ID				Area Type			No Summary	Ope	ration
0.0.0.1				Stub			Disabled	ľ	
0.0.0.12				Stub			Disabled	ľ	
									10/page ∨
					Edit Area Settings	×			
						- 1			
				Area ID		- 1			
				0.0.0.12		- 1			
				Area Type		- 1			
				O None 😐 :	Stub	- 1			
				No Summary		- 1			
						- 1			
					Cancel OK	- 1			

After the neighbor relationship is established, check the neighbor information and Database information.

OSPFv3										
Global	Area Settings	Interface Settings	Neighbor Info	Database Info						
			Туре		database					
			Self-Originate							
					Query					
			Database Info							
			Area	Scoped Link Sta	te Database	(Area 0.0.0.0)				
			Type LSId	AdvRoute	n Age	SeqNum		Payload		
			Area	Scoped Link Stat	te Database	(Area 0.0.0.1)				
			Type LSId	AdvRoute	n Age	SeqNum		Payload		
			Area	Scoped Link Stat	te Database	(Area 0.0.0.1	!)			
			Type LSId	AdvRoute	n Age	SeqNum		Payload		
			I/F S	coped Link State	e Database (I/F vlan2 in A	irea 0.0.0.12)			
			Type LSId	AdvRoute	r Age	SeqNum		Payload		
			AS So	oped Link State	Database					
			Type LSId	AdvRoute	n Age	SeqNum		Payload		

• 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 Ocustom	
	Tos Type	Any ~	
	Time Policy	None ~]
	Advanced Settings		
	Count		
	*Count ID		Valid range is 1-32
	Count Unit	By packet By byte	
	Mirroring		
	★Mirroring Group	~ ·	
		Go to "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 rule setting speed limit function: select speed limit group.



≱ ACL Name		1~64 characters
Rule Settings		
*Rule ID	1	Valid range is 1-2147483647. The smalle ID is matched first.
Action	Allow	~
Protocol Type	Any	~
Source IP Address	Any Custom	
Destination IP Address	Any Custom	
Tos Type	Any	~
Time Policy	Disabled	
Advanced Settings	2	
Count	3	
Mirroring	5	
Priority Mapping	6 7	
Rate Limit	1	^
	The rate limit function needs to go to "Security→ACL− configure the rate limit group to take effect	Rate Limit Settings" to

VLAN bind ACL:

ACL				
IPv4 ACL IPv6 ACL I	MAC ACL Port Binding to ACL VL	AN Binding to ACL Rate Limit	Settings	
Edit Unbind				
VLAN	IPv4 ACL Name	MAC	ACL Name	Operation
1				
2				
3		Edit	×	I d
4	VLAN			I d
5	4			Ľ 2
6	IPV4_ACL			e 2
7	First		~	C 2
8	MAC ACL		_	e 2
9	MACALL		~	C 🖉
10				C 🖉
	Cano	cel ОК	Total 19 <	1 2 > 10/page ∨ Go to
			_	

Speed limit group settings:



S 6	GWN7801					Save	Q 🧕 admin ~
		~	ACL				
🕀 Sw	witching	~	IPv4 ACL IPv6 ACL MAC ACL Port Bind	ling to ACL	VLAN Binding to ACL Rate Limit Settings		
		~	Burst Threshold Group 1				
		~	Burst Byte (bps)	7108	480	Enter a value between 128-8388480 that a multiple of 128	tis
		~	Burst Packet (pps)	10		Valid range is 1-65535	
		~	Burst Threshold Group 2				
⊘ Se	ecurity	~	Burst Byte (bps)	7108	480	Enter a value between 128-8388480 that a multiple of 128	tis
			Burst Packet (pps)	10		Valid range is 1-65535	
				Cane	cel OK		
AC	a		Rate Limit Settings				
			Rate Limit Group ID Rate	Limit Type	Burst Threshold Group	Rate Threshold	Operation
			1			**	Ľ
			2			**	Ľ
	nti Attack		3				Ľ
	ALLACK		4			-	Ľ
DA			5				Ľ
RA	ADIUS		6				
	ACACS+		7				
IA	ACACS+		8				Ľ

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	2 🚺 adn
	×	IPv6 Source Guard				
Switching		Port Protection Quaterna	ary Binding Table			
	~					
😂 Multicast	¥	Port	IPv6 Source Guard	Verification Type	Number of Quaternary Bindings	Operation
좀 Routing	~	1/0/1	Disabled	IPv6		e
		1/0/2	Disabled	IPv6	1	ß
		1/0/3	Disabled	IPv6	**:	Ø
Security	^	1/0/4	Disabled	IPv6	2	ß
		1/0/5	Disabled	IPv6	=	ß
		1/0/6	Disabled	IPV6	2	Ø
Port Isolation	<	1/0/7	Disabled	IPv6	2	e
		1/0/8	Disabled	IPv6	~	ß
	8 A.	1/0/9	Disabled	IPv6	÷	ß
IP Source Guard	d	1/0/10	Disabled	IPv6		e
IPv6 Source Gu	ard	LAG1	Disabled	IPv6	2	e
Anti Attack		LAG2	Disabled	IPv6		ß
		LAG3	Disabled	1Pv6	÷	ß
RADIUS		LAG4	Disabled	IPv6		ß
		LAG5	Disabled	IPv6		ø
		LAG6	Disabled	IPv6	12	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-based				
Security ^		802.1X Authentication				
		MAC Authentication				
		Guest VLAN				
			Cancel OK			
	Port					
Anti Attack	Port	User Authentication Mode	Authentication Method / Method	Guest VLAN	Authorized VLAN	Operation
DAI	c 1/0/1	MAC-Based		Disabled	Static	Ľ
	1/0/2	MAC-Based		Disabled	Static	Ľ
	1/0/3	MAC-Based		Disabled	Static	Ľ
	1/0/4	MAC-Based		Disabled	Static	Ľ
	1/0/5	MAC-Based		Disabled	Static	Ľ
АЛА	1/0/6	MAC-Based		Disabled	Static	e
	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	Ľ
	1/0/10	MAC-Based	**	Disabled	Static	Ľ
	1/0/11	MAC-Based		Disabled	Static	Ľ
🕃 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		ř	Port Mode > Edit					
		ř		Port	1/0/1			
0		^		User Authentication Mode 🛈	MAC-Based	~		
				Guest VLAN				
				Authorized VLAN ()	Static	v		
				Authentication Method1 😑				
				Authentication Method 💿	MAC Authentication	v		
				Method 🛈	Radius	v	•	
					Local	v	•	
						Add	0	
				Authentication Method2 😑				
	ААА			Authentication Method O	802.1X	v		
	Identity Authentica	tio		Method ()	Radius	\sim		
Ī							/	dd 🔂
					Cancel			
ß		~						

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 nonnel A	Identity Authentication Management				
Let Qas 🗠	Port Mode Port Authentication Sessions Local U	ser of MAC-based			
⊘ Security ^	Add Dates Delay Al	Add Local User of MAC-based	×		
Storm Control	MAC Address Port Control		1 (53)	Inactive Time (5)	Operation
PortSecurity		The MAC address of local user must be an unicast one.	_		
Port-Isolation		«MAC Address			
ACL		Port Control			
IP Source Guard		Force authentication Force unauthentication			
IPv6 Source Guard		VLANO			
Anti Attack		Valid range is 3-4054			
DAI		Reauthentication Time (s) Valid range is 300-23/37480/67			
RADIUS		3600			
TACACS+		Inactive Time (x) Valid range in 80-65335			
AAA		60			
Identity Authenticatio		Cancel			
DHCP Snooping		Spectra Contraction of the second sec	_		
DHCIV6 Snoopling					
🖉 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	ב		
	*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 Q 💽 admin ~
£	Routing	~	DHCPv6 Snooping			
Ľ		~	DHCPv6 Snooping	Option Settings Port Settings	Statistics	
0	Security	^		DHCPv6 Snooping		
				VLAN	_	Valid range is 1-4094. Example: "5-8, 11"
						will associate VLANs 5, 6, 7, 8 and 11.
					Cancel OK	
					Canter	
		Q				
	TACACS+					
	DHCP Snooping					
	DHCPv6 Snooping					
ß	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.





• Optimize EEE

Added actual port status display.

Overview	~	Energy Efficient Ethernet			
	~	Edit Refresh			
	~	Port	Configuration Status	Status	Operation
Multicast	~	1/0/1	Disabled	Disabled	ß
Routing	÷.	1/0/2	Disabled	Disabled	ß
		1/0/3	Disabled	Disabled	ß
		1/0/4	Disabled	Disabled	ß
	~	1/0/5	Disabled	Disabled	ß
Maintenance	^	1/0/6	Disabled	Disabled	ß
Upgrade		1/0/7	Disabled	Disabled	ß
Diagnostics	<	1/0/8	Disabled	Disabled	ß
Backup & Restor	e .				
SNMP					
RMON					
LLDP/LLDP-MED	Ì.				
	lanag				

• Add DST mode for time settings

Added daylight saving time offset setting and automated time configuration.

GWN7801		<u>1</u>				Save	Q		idmin ~
		Basic Settings							
			Basic Info						
			Device Name	GWN7801	1-64 characters				
			System Location	Default	0-64 characters				
					0.54 characters				
			System Contact	Detaut					
			Time Settings						
			Date & Time	Manual (Internet Automatic (NTP Server)					
rstem	^		System Time	2023-12-25 17:18:00 5	3				
asic Settings		¢		pool.ntp.org					
			Time Zone	(UTC+08:00) Beljing,Shanghal.Chongqing,Hong Kong,Uru	e.				
		Г	DayLight Saving (DST) Mode	Recurring	20				
			*Offset (Min)	60	Valid range is 1-144	0			
			•Starting Time		Select time	0			
			•Ending Time	· · · · ·	Select time	0			
		L			Caracterine .				
			Scheduled Reboot						
				Cancel					
	verview vitching uiticast uiticast soft soft soft soft soft soft soft so	vervlew vitching vitc	vervlew v Basic Settings vitching v utiticast v outing v oss v oscurity v sterm v sterm v	veck/ew Basic Settings witching Basic Info utilicast - os System Location skitning - os - skitning - skitning - os - skitning - <th>veckview v Basic Settings vitching vitching Basic Info vitching vibevice Name GWV7801 utilicaat system Location Default suting vitching System Contact Default os vitchings vitchings vitchings stem vitchings vitchings vitchings stem vitchings vitchings vitchings ster System Time 2023/12/25 17:18:00 vitchings ster Management Daylight Saving (DST) Mode Recurring vitching vef Management Gol vitching vitching vitching starting Time vitching vitching vitching vitching vef Management Starting Time vitching vitching vitching vef Management</th> <th>vectorized Basic Settings vitching Basic Info utiticatt • Derivice Name OVN7801 1=64 devisitors. utiticatt • System Location Default 0=64 devisitors. os • System Contact Default 0=64 devisitors. os • Time Settings Date & Time Nanual • Automatic (NTP Server) ster System Time 2023-12:255 17:18:00 O vecry thrup ANTP Server pool.ntp.org. cccess Control ANTP Server pool.ntp.org. ver Management Offset (Min) 60 ver Management Starting Time ver vering ver vering ver Management Starting Time ver vering vering vering time vering vering vering vering time vering</th> <th>veckview > Basic Settings vitching > Basic Info ublicatt > > ublicatt > > usting > > usting > > ublicatt > > ublicatt > > usting > > ust System Location Default > ublicatt > > > ust System Contact Default > > ust Date & Time Manual @ Automatic (NTP Server) > > stet System Time 2023-12-25171:18:00 > > wer Management me Policy DayUght Saving (DST) Mode eccurring > ust Automatic (NTP Server) Setect time Setect time Setect time > DayUght Saving (DST) Mode eccurring > Setect time ust Automatic (NTP Server) Setect time Setect time stending Time</th> <th>vetrylew Basic Settings vetrylew Basic Settings vetrylem Basic Info utilicaat suting os suting os suting os suting os stem ter Management. me Policy Basic Settings vetrylem stem vetrylem ve</th> <th>vetArlow Basic Settings vetArlow Basic Settings vetArlow Basic Info utilicati Device Name obs System Location os System Contact os Time Settings recers Control Manual set Settings NTP Server policing. DayLight Saving (DST) Mode vetarring Of Set (Min) vetarring Of Setting Time vetarring Seterting Time vetarring Seterting Time vetarring Seterting Time vetarring Time Setert time O Setert time O Setert time O </th>	veckview v Basic Settings vitching vitching Basic Info vitching vibevice Name GWV7801 utilicaat system Location Default suting vitching System Contact Default os vitchings vitchings vitchings stem vitchings vitchings vitchings stem vitchings vitchings vitchings ster System Time 2023/12/25 17:18:00 vitchings ster Management Daylight Saving (DST) Mode Recurring vitching vef Management Gol vitching vitching vitching starting Time vitching vitching vitching vitching vef Management Starting Time vitching vitching vitching vef Management	vectorized Basic Settings vitching Basic Info utiticatt • Derivice Name OVN7801 1=64 devisitors. utiticatt • System Location Default 0=64 devisitors. os • System Contact Default 0=64 devisitors. os • Time Settings Date & Time Nanual • Automatic (NTP Server) ster System Time 2023-12:255 17:18:00 O vecry thrup ANTP Server pool.ntp.org. cccess Control ANTP Server pool.ntp.org. ver Management Offset (Min) 60 ver Management Starting Time ver vering ver vering ver Management Starting Time ver vering vering vering time vering vering vering vering time vering	veckview > Basic Settings vitching > Basic Info ublicatt > > ublicatt > > usting > > usting > > ublicatt > > ublicatt > > usting > > ust System Location Default > ublicatt > > > ust System Contact Default > > ust Date & Time Manual @ Automatic (NTP Server) > > stet System Time 2023-12-25171:18:00 > > wer Management me Policy DayUght Saving (DST) Mode eccurring > ust Automatic (NTP Server) Setect time Setect time Setect time > DayUght Saving (DST) Mode eccurring > Setect time ust Automatic (NTP Server) Setect time Setect time stending Time	vetrylew Basic Settings vetrylew Basic Settings vetrylem Basic Info utilicaat suting os suting os suting os suting os stem ter Management. me Policy Basic Settings vetrylem stem vetrylem ve	vetArlow Basic Settings vetArlow Basic Settings vetArlow Basic Info utilicati Device Name obs System Location os System Contact os Time Settings recers Control Manual set Settings NTP Server policing. DayLight Saving (DST) Mode vetarring Of Set (Min) vetarring Of Setting Time vetarring Seterting Time vetarring Seterting Time vetarring Seterting Time vetarring Time Setert time O Setert time O Setert time O

Add HTTPS/SSH port customization



S GWN7801				Save
(2) Overview		Access Control		
Switching		Web Service Management SSH Remote Access	Manager Settings	
		+HTTPS	443	Valid range is 443 and 1024-65535
		Inactive Session Timeout (min)	1440	Valid range is 1-1440
		Telnet		
		SSH		
		◆SSH Port	22	Valid range is 22 and 1024-65535
		•331 FOR		
🔞 System	^		Cancel	
	le l			
Access Control				
User Manageme	nt			

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

• Optimize Manager settings

S GWN7801				Save 🛛 Q 🕴 💽 admin ~
Overview		Access Control		
Switching		Web Service Management SSH Remote Access	Manager Settings	
© IP		Allow DHCP Option 43 to Override ①		
😂 Multicast		Manager Settings		
न Routing		Manager Server Address		
L∽ QoS				
Security		Manager Server Port	8443	Valid range is 1-65535
🔑 Maintenance			Cancel	
🕄 System	^			
Basic Settings				
Access Control				
User Managemer				
Time Policy				

• 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 1.0.1.20

PRODUCT NAME

GWN7811, GWN7811P, GWN7812P, GWN7813, GWN7813P

DATE

11/07/2023

FIRMWARE FILE INFORMATION

GWN781x Firmware file name: gwn781xfw.bin
 MD5 checksum: 70d00f61ebe58d9ad79e707f81b0256e

CHANGES/ENHANCEMENT

- Added support for GWN Cloud 1.1.25.23.
- Optimized CPU usage.
- Added support of SSH and TELNET in # mode.
- Added support of Dynamic Voice VLAN.
- Added support of voice VLAN OUI untagged mode.
- Added support of EXEC CLI config commands by GWN Cloud.
- Added SNTP GWN Cloud interface.
- Added GWN Cloud time sync interface.
- Added support EXEC CLI config command by GWN Cloud.
- Fixed the issue that GWN781x OSPF sometimes configuration loss after modifying the area, also added error prompt when the key character range is exceeded.
- Fixed the issue that after deleted a static NDP, it cannot re-create it.
- Fixed the issue that after unplugging ethernet cable on static IP interface, the IP address would change to 0.0.0.0.
- Fixed the issue that in very rare conditions that the device might automatically restart.
- Fixed the issue that when IPSG is enabled, sender with IP 0.0.0.0 still has ARP probe packets dropped.
- Fixed the issue that Time Policy allow create new policy with exist names.
- Fixed the issue that the switch obtains an ipv6 address stateless, but after the interface is down, the ipv6 address is still present.
- Fixed the issue that Neighbor Discovery query results for the web and CLI are incorrect.
- Fixed the issue that if OSPF key mode is set to md5, the key cannot be saved in plain text, and an error message is displayed.
- Fixed some issues when work with GWN Cloud.
- Internal bug fixes.



FIRMWARE VERSION 1.0.1.8

PRODUCT NAME

GWN7811, GWN7811P, GWN7812P, GWN7813, GWN7813P

DATE

08/04/2023

FIRMWARE FILE INFORMATION

• GWN781x Firmware file name: gwn781xfw.bin MD5 checksum: c4393865767f3b042086515b75029db6

CHANGES/ENHANCEMENT

• This is the first release of GWN781x.