16/24-Port Gigabit Managed PoE Switch

Quick Start Guide

V1.0.2

Foreword

General

This manual introduces the functions and operations of 16/24-port Gigabit managed PoE switch (hereinafter referred to as "the Device").

Safety Instructions

The following categorized signal words with defined meaning might appear in the manual.

Signal Words	Meaning
⚠ DANGER	Indicates a high potential hazard which, if not avoided, will result in death or serious injury.
⚠ WARNING	Indicates a medium or low potential hazard which, if not avoided, could result in slight or moderate injury.
⚠ CAUTION	Indicates a potential risk which, if not avoided, could result in property damage, data loss, lower performance, or unpredictable result.
TIPS	Provides methods to help you solve a problem or save you time.
NOTE	Provides additional information as the emphasis and supplement to the text.

Revision History

Version	Revision Content	Release Time
V1.0.2	Updated features.	August 2023
V1.0.1	Updated "1.1 Product Introduction" and "1.2 Product Features".	November 2020
V1.0.0	First release.	September 2020

About the Manual

- The manual is for reference only. If there is inconsistency between the manual and the actual product, the actual product shall prevail.
- We are not liable for any loss caused by the operations that do not comply with the manual.
- The manual would be updated according to the latest laws and regulations of related jurisdictions. For detailed information, refer to the paper manual, CD-ROM, QR code or our official website. If there is inconsistency between paper manual and the electronic version, the electronic version shall prevail.
- All the designs and software are subject to change without prior written notice. The product updates might cause some differences between the actual product and the manual. Please contact the customer service for the latest program and supplementary documentation.
- There still might be deviation in technical data, functions and operations description, or errors in print. If there is any doubt or dispute, we reserve the right of final explanation.
- Upgrade the reader software or try other mainstream reader software if the manual (in PDF format) cannot be opened.

- All trademarks, registered trademarks and the company names in the manual are the properties of their respective owners.
- Please visit our website, contact the supplier or customer service if there is any problem occurring when using the device.
- If there is any uncertainty or controversy, we reserve the right of final explanation.

Important Safeguards and Warnings

The manual helps you to use our product properly. To avoid danger and property damage, read the manual carefully before using the product, and we highly recommend you to keep it well for future reference.

Operating Requirements

- Do not expose the device directly to the sunlight, and keep it away from heat.
- Do not install the device in the damp environment, and avoid dust and soot.
- Make sure the device is in horizontal installation, and install the device on solid and flat surface to avoid falling down.
- Avoid liquid spattering on the device. Do not place object full of liquid on the device to avoid liquid flowing into the device.
- Install the device in the well-ventilated environment. Do not block the air vent of the device.
- Use the device at rated input and output voltage.
- Do not dissemble the device without professional instruction.
- Transport, use, and store the device in allowed ranges of humidity and temperature.
- Disconnect the power supply first to avoid personal injury when removing the cable.
- Voltage stabilizer and lightning arrester are optional according to site power supply and surrounding environment.

Power Supply Requirements

- Use the battery properly to avoid fire, explosion, and other dangers.
- Replace the battery with battery of the same type.
- Use locally recommended power cord in the limit of rated specifications.
- Use the standard power adapter. We will assume no responsibility for any problems caused by nonstandard power adapter.
- The power supply shall meet the SELV requirement. Use the power supply that conforms to Limited Power Source, according to IEC60950-1. Refer to the device label.
- Adopt GND protection for I-type device.
- The coupler is the disconnecting apparatus. Keep it at the angle for easy to operate.
- Be sure to ground the device (connect with copper wire whose cross section is not less than 2.5 mm^2 and resistance to ground is less than or equal to 4Ω).

Battery Caution

- Do not ingest battery to avoid chemical burn hazard.
- This product contains a coin cell battery. If the coin cell battery is swallowed, it can cause severe internal burns in just 2 hours and can lead to death.
- Keep new and used batteries away from children.
- If the battery compartment does not close securely, stop using the product and keep it away from children.
- If you think batteries might have been swallowed or placed inside any part of the body, seek immediate medical attention.
- Risk of explosion if the battery is replaced by an incorrect type.

- Do not throw or immerse into water, heat to more than 100°C（212°F）, repair or disassemble, leave in an extremely low air pressure environment or extremely high-temperature environment, crush, puncture, cut or incinerate.
- Dispose of the battery as required by local ordinances or regulations.

Table of Contents

1 Overview

1.1 Product Introduction

The 16/24-Port Gigabit Managed PoE Switch is designed and developed for field transmission application of high definition video. The product is equipped with high performance switching engine and large buffer, which features low transmission delay and high reliability.

With solid and sealed all-metal case design, the product has low power consumption. With a fan inside which improves high surface heat dissipation efficiency, the product can work in the environment from -10 °C to 55 °C. And power input end overcurrent, overvoltage, and EMC protection can effectively resist the interference from static electricity, lightning, and pulse.

The product owns powerful network management function. Network management system supports iLinksView, CLI, web, and network management software based on SNMP.

1.2 Product Features

- Layer 2 network management PoE switch.
- Support IEEE802.3af, IEEE802.3at standard.
- Port 1 and port 2 support IEEE802.3bt, and are compatible with Hi-PoE.
- Network redundancy: STP/RSTP/MSTP.
- Support IPv4/IPv6, and DHCP.
- Network management based on SNMP.
- Configuration: web console, Telnet, CLI command.
- QoS (IEEE802.1p/1Q), CoS/ToS to increase determinism.
- Enhanced network security with IEEE802.1X, SNMP v1/v2c/v3, HTTPS, and SSH.
- Large data buffer up to 4 MB, real-time transmission.
- MAC auto study and aging, MAC address list capacity is 8K.
- PD alive (PoE watchdog) mode.
- 250 m long-distance transmission mode.

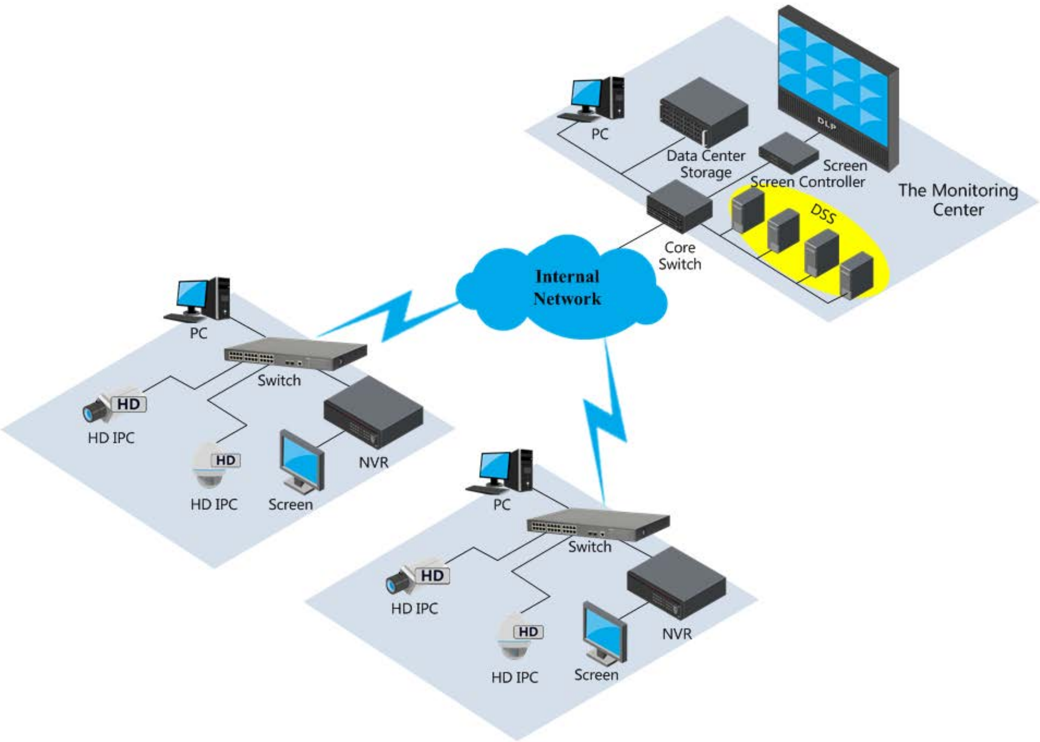
  📖

  In Extend Mode, the transmission distance of the PoE port is up to 250 m but the transmission rate drops to 10 Mbps. The actual transmission distance might vary due to power consumption of connected devices or the cable type and status.
- EMC high protection design.

1.3 Typical Application

We take the 24-Port Gigabit Managed PoE Switch as the example to introduce the typical networking scene.

Figure 1-1 Networking



2 Device Structure

2.1 Front Panel

16-Port Gigabit Managed PoE Switch

Figure 2-1 Front panel

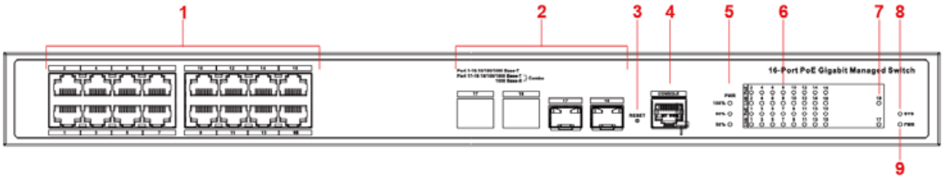


Table 2-1 Front panel description

No.	Name	Description
1	RJ45 port	Ethernet port, supports 10/100/1000 Mbps self-adaptive.
2	COMBO port	2 Ethernet ports, support 10/100/1000 Mbps self-adaptive; 2 optical ports, support 1000 Mbps self-adaptive.
3	Reset button	Long press the button for 5 s to reset the Device and recover default configuration.
4	Console serial port	Device debugging port.
5	PoE power usage indicator	Current power consumption display.
6	Downlink indicator	Current port link status and PoE status.
7	Uplink port indicator	Link/Act indicator.
8	System indicator	System status: ● When device is booting up, the light is flashing quickly. ● When device is working properly, the light is flashing slowly.
9	Power indicator	Current power status of the Device.

24-Port Gigabit Managed PoE Switch

Figure 2-2 Front panel

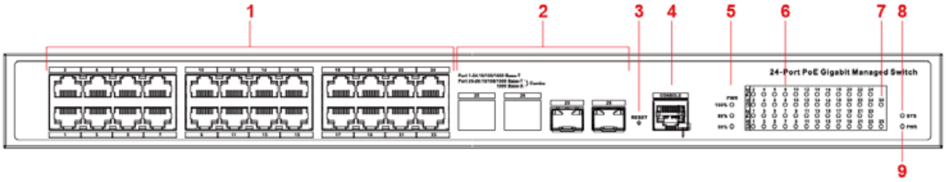


Table 2-2 Front panel description

No.	Name	Description
1	RJ45 port	Ethernet port, supports 10/100/1000 Mbps self-adaptive.
2	COMBO port	2 Ethernet ports, support 10/100/1000 Mbps self-adaptive; 2 optical ports, support 1000 Mbps self-adaptive.

No.	Name	Description
3	Reset button	Long press the button for 5 s to reset the Device and recover default configuration.
4	Console serial port	Device debugging port.
5	PoE power usage indicator	Current power consumption display.
6	Downlink indicator	Current port link status and PoE status.
7	Uplink port indicator	Link/Act indicator.
8	System indicator	System status: ● When device is booting up, the light is flashing quickly. ● When device is working properly, the light is flashing slowly.
9	Power indicator	Current power status of the Device.

2.2 Rear Panel

Figure 2-3 Rear panel

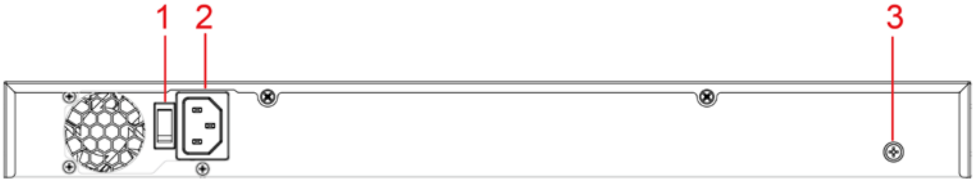


Table 2-3 Rear panel description

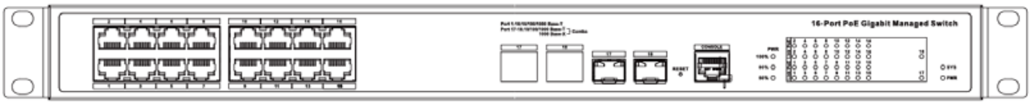
No.	Name	Description
1	Power switch	Power on or off the Device.
2	Power socket	Support 100-240 VAC.
3	Ground terminal	GND.

3 Installation

3.1 Installing the Device

The device supports standard rack mount.
Install the rack mount kit on both sides of the switch.

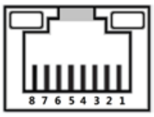
Figure 3-1 Rack mount



3.2 Wiring

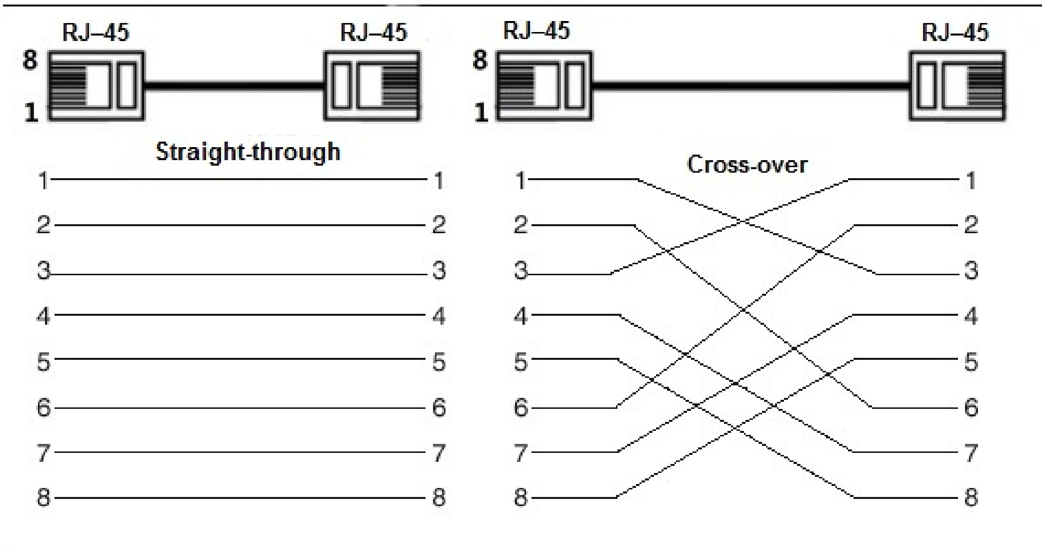
3.2.1 Ethernet Port

Figure 3-2 Ethernet port pin number



10/100/1000 Mbps Base-T Ethernet port adopts standard RJ45 port. Equipped with self-adaptation function, it can be automatically configured to full duplex/half-duplex operation mode, and supports MDI/MDI-X self-recognition function of the cable, which means that the switch can use cross-over cable or straight-through cable to connect terminal device to network device.

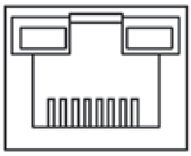
Figure 3-3 Pin description



The cable connection of RJ45 connector conforms to the standard 568B (1-orange white, 2-orange, 3-green white, 4-blue, 5-blue white, 6-green, 7-brown white, 8-brown).

3.2.2 Console Port

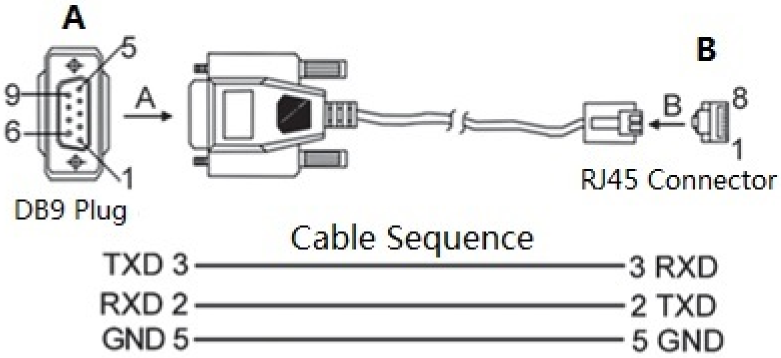
Figure 3-4 Console port



See Figure 3-4 for console port. The switch console port and computer controlling 9-pin serial port are connected with RJ-45-DB9 cable. You can call the console software of the device by operating the superterminal software of the Windows system for device configuration, maintenance, and management.

See Figure 3-5 for cable sequence of RJ-45-DB9.

Figure 3-5 Cable sequence of RJ45 DB9



One end of RJ45 DB9 cable is RJ45 connector, which needs to be inserted into the console port of the device. And the other end is DB9 plug, which needs to be inserted into the computer controlling 9-pin serial port.

Table 3-1 Pin description

DB9 pin	RJ45 pin	Signal	Description
2	3	RXD	Receiving data
3	2	TXD	Sending data
5	5	GND	GND

3.2.3 SFP Port

📖

The signal is transmitted through laser by optical fiber cable. The laser conforms to the requirement of level 1 laser products. To avoid injury of eyes, do not look at the 1000 Base-X optical port directly when the device is powered on.

Figure 3-6 SFP module structure

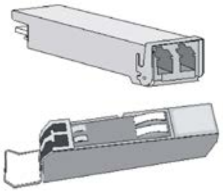
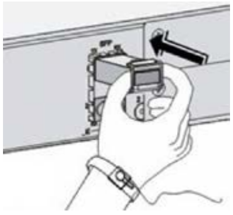


Figure 3-7 SFP module installation



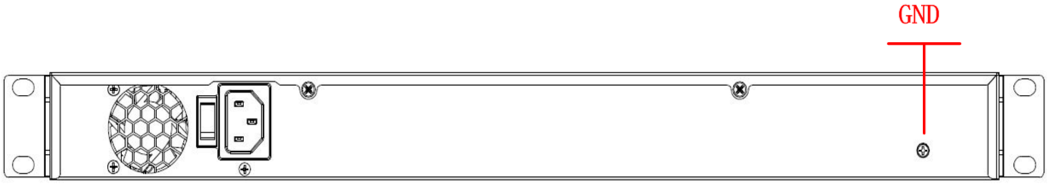
Installing SFP Port

Before installing SFP module, wear antistatic gloves, and then wear antistatic wrist strap. Make sure that the antistatic gloves and the antistatic wrist strap are in good contact.

1. Lift the handle of SFP module upward vertically, and stuck it to the top hook.
2. Hold the SFP module by both sides, and push it gently into the SFP slot till the SFP module is firmly connected to the slot (both the top and bottom spring strip of the SFP module are firmly stuck with the SFP slot).

3.2.4 GND

Figure 3-8 GND terminal



Normal GND of the device is the important guarantee for device lightning protection and anti-interference. You should connect the GND cable before powering on the device, and power off the device before disconnecting the GND cable.

There is a GND screw on the device cover board for the GND cable, which is called enclosure GND. Connect one end of the GND cable with the cold-pressed terminal, and fix it on the enclosure GND with the GND screw. The other end of the GND cable should be reliably connected to the ground.

📖

The sectional area of the GND cable shall be more than 2.5 mm^2, and the GND resistance shall be less than 4Ω.

4 Quick Operations

We will introduce VLAN configuration briefly in this section. See the corresponding command line manual for detailed configuration.

4.1 First Login by Console Port

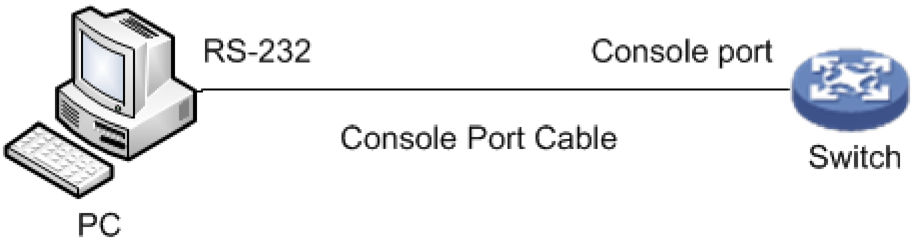
It is the most basic way to log in to the local interface via Console port, and it is also the method to configure other ways to log in to the device.

Step 1 Power off the PC.

Step 2 Use default console port cable to connect PC and the device.
First insert the DB-(hole) plug of console port cable into the 9-pin serial port of PC, and then insert the RJ45 plug into the console port of the device.

- Confirm the sign on the port during connection, in case it may plug into the wrong port.
- Plug out RJ45 and then DB-9 when dismantling console port cable.

Figure 4-1 Login via console port



Step 3 Power on the PC.

Step 4 Run terminal simulation program on the PC, and then select the serial port which is to connect the device, set the terminal communication parameters.
The following parameter values have to be in accordance with the values on the device, the default are shown as follows.

- Baud rate: 115200
- Data bit: 8
- Stop bit: 1
- Parity: none
- Flow control: none

- If the PC uses Windows Server 2003 operating system, please add super terminal program in the Windows component and then log in and manage the device according to the way introduced in this manual.
- If the PC uses Windows Server 2008, Windows Vista, Windows 7 or other operating systems, please prepare third-party terminal control software, refer to the software operation guide or online help for operation method.

Step 5 After device is powered on, it displays device self-check information on the terminal control software, and it will prompt users to press Enter key after self-check, then it will display username and password input prompt.

Step 6 Enter username and password, and then press Enter.

The default username is admin, and the default password is admin.

The following command line prompt (SWITCH#) is displayed after pressing Enter, which means login has been successful.

Enter corresponding command, and you can configure the device or check device operating status, and you can enter ? anytime if you need help.

```
+M25PXX : Init device with JEDEC ID 0xC22018.
Luton10 board detected (VSC7428 Rev. D).

RedBoot(tm) bootstrap and debug environment [ROMRAM]
Non-certified release, version 1_31-4752 - built 17:29:35, Jul 29 2017

Copyright (C) 2000, 2001, 2002, 2003, 2004, 2005, 2006, 2007, 2008, 2009
Free Software Foundation, Inc.
RedBoot is free software, covered by the eCos license, derived from the
GNU General Public License. You are welcome to change it and/or distribute
copies of it under certain conditions. Under the license terms, RedBoot's
source code and full license terms must have been made available to you.
Redboot comes with ABSOLUTELY NO WARRANTY.

Platform: VCore-III (MIPS32 24KEc) LUTON26
RAM: 0x80000000-0x88000000 [0x80028f20-0x87fdfffc available]
FLASH: 0x40000000-0x40ffffff, 256 x 0x10000 blocks
== Executing boot script in 3.000 seconds - enter ^C to abort
RedBoot> diag -p
RedBoot> fis load -x linux
MD5 signature validated
Stage1: 0x80100000, length 4641272 bytes
Initrd: 0x80600000, length 188416 bytes
Kernel command line: init=/usr/bin/stage2-loader loglevel=4
RedBoot> exec
Now booting linux kernel:
Base address 0x80080000 Entry 0x80100000
Cmdline : init=/usr/bin/stage2-loader loglevel=4
  Active fis: linux
[        0.374113] vcfw_uio vcfw_uio: UIO driver loading
[        0.378957] vcfw_uio vcfw_uio: Invalid memory resource
[        0.384141] iounmap: bad address      (null)
00:00:00 Stage 1 booted
00:00:00 Using device: /dev/mtd7
00:00:01 Mounted /dev/mtd7
00:00:01 Loading stage2 from NAND file 'n6G5Xw'
```

```
00:00:05 Overall: 4195 ms, ubifs = 748 ms, rootfs 3422 ms of which xz = 0 ms of which untar
= 0 ms
Starting application...wuxuwuxu
Using existing mount point for /switch/
system time:2017-10-14 17:59:53
W icfg 18:00:22 71/icfg_commit_tftp_load_and_trigger#2695: Warning: TFTP get
bringup-config: Operation timed out.

Press ENTER to get started

Username: admin
Password:
SWITCH#
```

Enter corresponding command to configure the device or check device operating status, and you can enter ? anytime if you need help.

4.2 Device Factory Default Configuration

You can log in to web page of the device via the following IP address.
Username and password can be applied to log in to web page via Console port.

Table 4-1 Device factory default

Parameter	**Note**
IP address	192.168.1.110
Username	admin
Password	

- iLinksView is enabled by default, and the default username is admin, the default password is lt_91_il_02_nmp.
- When using the iLinksView to manage the device, note that the username and password must be the same as that you have set in the iLinksView, otherwise the iLinksView cannot discover the device.

4.3 VLAN Configuration

VLAN (Virtual Local Area Network) is frequently used during actual application; it is divided into multiple network basics internally. VLAN is to organize several devices into one network logically, regardless of the physical location of the devices. Each VLAN is a logical network, which is equipped with all functions and attributes of traditional physical network. Each VLAN is a broadcast domain; broadcast packet can only be forwarded within one VLAN, not across the VLAN.

VLAN Based on Port

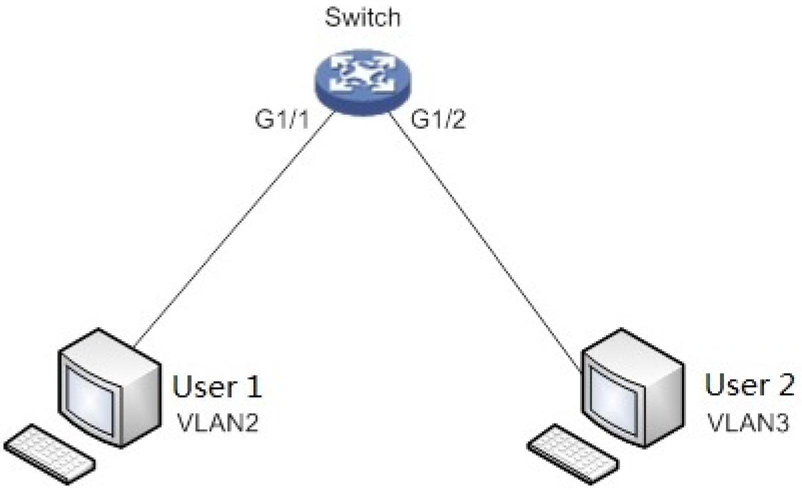
VLAN based on port means that one switch can realize the division of logical working groups via controlling interoperability of between two and among several ports. Dividing port VLAN reasonably can greatly improve network security and bandwidth use ratio, besides it reduces the probability of broadcast storm. The model supports 4094 VLAN; it needs to select a VLAN ID when creating VLAN, ranging from 2 to 4094. The switch creates VLAN1 by default and VLAN1 cannot be deleted.

Application Example

Networking Requirement

There are two users, user 1 and user 2. These two users need to be in different VLAN due to different network function and environment. User 1 belongs to VLAN2, connecting to switch port G1/1 (Gigabit Ethernet 1/1); user 2 belongs to VLAN 3, connecting to switch port G1/2 (Gigabit Ethernet 1/2).

Figure 4-2 VLAN networking



Configuration Steps

The switch configuration is shown as follows.

1. Log in to the device. Refer to "4.1 First Login by Console Port".
2. Run the following command to create VLAN.

```
SWITCH #configure terminal
SWITCH (config)#vlan 2
SWITCH (config-vlan)# exit
SWITCH (config)#vlan 3
SWITCH (config-vlan)# exit
```

3. Run the following command to distribute ports into the VLAN.

```
SWITCH (config)# interface GigabitEthernet 1/1
SWITCH (config-if)# switchport access vlan 2
SWITCH (config-if)# exit
SWITCH (config)# interface GigabitEthernet 1/2
SWITCH (config-if)# switchport access vlan 3
SWITCH (config-if)# exit
```

Appendix 1 Cybersecurity Recommendations

Mandatory actions to be taken for basic device network security:

1. **Use Strong Passwords**

   Please refer to the following suggestions to set passwords:

   - The length should not be less than 8 characters;
   - Include at least two types of characters; character types include upper and lower case letters, numbers and symbols;
   - Do not contain the account name or the account name in reverse order;
   - Do not use continuous characters, such as 123, abc, etc.;
   - Do not use overlapped characters, such as 111, aaa, etc.;

2. **Update Firmware and Client Software in Time**

   - According to the standard procedure in Tech-industry, we recommend to keep your device (such as NVR, DVR, IP camera, etc.) firmware up-to-date to ensure the system is equipped with the latest security patches and fixes. When the device is connected to the public network, it is recommended to enable the “auto-check for updates” function to obtain timely information of firmware updates released by the manufacturer.
   - We suggest that you download and use the latest version of client software.

"Nice to have" recommendations to improve your device network security:

1. **Physical Protection**

   We suggest that you perform physical protection to device, especially storage devices. For example, place the device in a special computer room and cabinet, and implement well-done access control permission and key management to prevent unauthorized personnel from carrying out physical contacts such as damaging hardware, unauthorized connection of removable device (such as USB flash disk, serial port), etc.

2. **Change Passwords Regularly**

   We suggest that you change passwords regularly to reduce the risk of being guessed or cracked.

3. **Set and Update Passwords Reset Information Timely**

   The device supports password reset function. Please set up related information for password reset in time, including the end user’s mailbox and password protection questions. If the information changes, please modify it in time. When setting password protection questions, it is suggested not to use those that can be easily guessed.

4. **Enable Account Lock**

   The account lock feature is enabled by default, and we recommend you to keep it on to guarantee the account security. If an attacker attempts to log in with the wrong password several times, the corresponding account and the source IP address will be locked.

5. **Change Default HTTP and Other Service Ports**

   We suggest you to change default HTTP and other service ports into any set of numbers between 1024~65535, reducing the risk of outsiders being able to guess which ports you are using.

6. **Enable HTTPS**

   We suggest you to enable HTTPS, so that you visit Web service through a secure communication channel.

7. **MAC Address Binding**

   We recommend you to bind the IP and MAC address of the gateway to the device, thus reducing the risk of ARP spoofing.

8. **Assign Accounts and Privileges Reasonably**

   According to business and management requirements, reasonably add users and assign a minimum set of permissions to them.

9. **Disable Unnecessary Services and Choose Secure Modes**

   If not needed, it is recommended to turn off some services such as SNMP, SMTP, UPnP, etc., to reduce risks.

   If necessary, it is highly recommended that you use safe modes, including but not limited to the following services:

   - SNMP: Choose SNMP v3, and set up strong encryption passwords and authentication passwords.
   - SMTP: Choose TLS to access mailbox server.
   - FTP: Choose SFTP, and set up strong passwords.
   - AP hotspot: Choose WPA2-PSK encryption mode, and set up strong passwords.

10. **Audio and Video Encrypted Transmission**

    If your audio and video data contents are very important or sensitive, we recommend that you use encrypted transmission function, to reduce the risk of audio and video data being stolen during transmission.

    Reminder: encrypted transmission will cause some loss in transmission efficiency.

11. **Secure Auditing**

    - Check online users: we suggest that you check online users regularly to see if the device is logged in without authorization.
    - Check device log: By viewing the logs, you can know the IP addresses that were used to log in to your devices and their key operations.

12. **Network Log**

    Due to the limited storage capacity of the device, the stored log is limited. If you need to save the log for a long time, it is recommended that you enable the network log function to ensure that the critical logs are synchronized to the network log server for tracing.

13. **Construct a Safe Network Environment**

    In order to better ensure the safety of device and reduce potential cyber risks, we recommend:

    - Disable the port mapping function of the router to avoid direct access to the intranet devices from external network.
    - The network should be partitioned and isolated according to the actual network needs. If there are no communication requirements between two sub networks, it is suggested to use VLAN, network GAP and other technologies to partition the network, so as to achieve the network isolation effect.
    - Establish the 802.1x access authentication system to reduce the risk of unauthorized access to private networks.
    - Enable IP/MAC address filtering function to limit the range of hosts allowed to access the device.