EDIMAX

NETWORKING PEOPLE TOGETHER

24 / 16 Gigabit Web Smart Switch

User's Manual

Release 1.03

Table of Contents

Revision History

Release	Date	Revision
0.99	12/30/2004	A1
1.03	01/20/2005	A1
1.03	01/26/2005	A1

Caution

Circuit devices are sensitive to static electricity, which can damage their delicate electronics. Dry weather conditions or walking across a carpeted floor may cause you to acquire a static electrical charge.

To protect your device, always:

Touch the metal chassis of your computer to ground the static electrical charge before you pick up the circuit device.

Pick up the device by holding it on the left and right edges only.

Electronic Emission Notices

Federal Communications Commission (FCC) Statement

This equipment has been tested and found to comply with the limits for a class A computing device pursuant to Subpart J of part 15 of FCC Rules, which are designed to provide reasonable protection against such interference when operated in a commercial environment.

European Community (CE) Electromagnetic Compatibility Directive

This equipment has been tested and found to comply with the protection requirements of European Emission Standard EN55022/EN60555-2 and the Generic European Immunity Standard EN50082-1.

EMC:	EN55022(1988)/CISPR-22(1985)	class A
	EN60555-2(1995)	class A
	EN60555-3	
	IEC1000-4-2(1995)	4K V CD, 8KV, AD
	IEC1000-4-3(1995)	3V/m
	IEC1000-4-4(1995)	1KV – (power line), 0.5KV – (signal line)

About this user's manual

In this user's manual, it will not only tell you how to install and connect your network system but configure and monitor the 16 Gigabit Web Smart Switch through the built-in console and web by RS-232 serial interface and Ethernet ports step-by-step. Many explanation in detail of hardware and software functions are shown as well as the examples of the operation for web-based interface and text-based menu-driven console interface.

Overview of this user's manual

Chapter 1 "Introduction" describes the features of 16 Gigabit Web Smart Switch
Chapter 2 "Installation"
Chapter 3 "Operating Concept and Management"
Chapter 4 "Operation of Web-based Management"
Chapter 5 "Maintenance"

Publication date: January, 2005
Revision A1

1. Introduction

1-1. Overview of Gigabit Web Smart Switch

24/ 16-port Gigabit Web Smart Switch is a standard switch that meets all IEEE 802.3/u/x/z Gigabit, Fast Ethernet specifications. The switch included 22 or 14-Port 10/100/1000Mbps TP and 2-Port Gigabit TP/SFP Fiber Web Smart management Ethernet Switch. The switch can be managed through Ethernet port using Web-based management unit, associated with web-based management, the network administrator can logon the switch to monitor, configure and control each port's activity. In addition, the switch implements the QoS (Quality of Service), VLAN, and Trunking. It is suitable for office application.

In this switch, last two ports includes two types of media --- TP and SFP Fiber (LC, BiDi-SC…); this port supports 10/100/1000Mbps TP or 1000Mbps SFP Fiber with auto-detected function. 1000Mbps SFP Fiber transceiver is used for high-speed connection expansion.

1000Mbps LC, Multi-Mode, SFP Fiber transceiver

1000Mbps LC, 10km, SFP Fiber transceiver

1000Mbps LC, 30km, SFP Fiber transceiver

1000Mbps LC, 50km, SFP Fiber transceiver

1000Mbps BiDi-SC, 20km, 1550nm SFP Fiber WDM transceiver
1000Mbps BiDi-SC, 20km, 1310nm SFP Fiber WDM transceiver

10/100/1000Mbps TP is a standard Ethernet port that meets all IEEE 802.3/u/x/z Gigabit, Fast Ethernet specifications. 1000Mbps SFP Fiber transceiver is a Gigabit Ethernet port that fully complies with all IEEE 802.3z and 1000Base-SX/LX standards.

1000Mbps Single Fiber WDM (BiDi) transceiver is designed with an optic Wavelength Division Multiplexing (WDM) technology that transports bi-directional full duplex signal over a single fiber simultaneously.

- **Key Features in the Device**

QoS:

The switch offers powerful QoS function. This function supports TOS field of IP header (equal DSCP low 3 bits) on Layer 3 of network framework and 6 kinds of special network transmission events on Layer 4.

VLAN:

Supports Port-based VLAN, IEEE802.1Q Tag VLAN. And supports 16 active VLANs and VLAN ID 1~4094.

Port Trunking:

Allows one or more links to be aggregated together to form a Link Aggregation Group by the static setting.

1-2. Checklist

Before you start installing the switch, verify that the package contains the following:

A set of 16 Gigabit Web Smart Switch

Modules (optional)

Mounting Accessory (for 19" Rack Shelf)

This User's Manual in CD-ROM

AC Power Cord

Please notify your sales representative immediately if any of the aforementioned items is missing or damaged.

1-3. Features

The 16 Gigabit Web Smart Switch, a standalone off-the-shelf switch, provides the comprehensive features listed below for users to perform system network administration and efficiently and securely serve your network.

- **Hardware**

  - 22 or 14 10/100/1000Mbps Auto-negotiation Gigabit Ethernet TP ports
  - 2 10/100/1000Mbps TP or 1000Mbps SFP Fiber dual media auto sense
  - 400KB on-chip frame buffer
  - Jumbo frame support
  - Programmable classifier for QoS (Layer 4/Multimedia)
  - 8K MAC address and 4K VLAN support (IEEE802.1Q)
  - Per-port shaping, policing, and Broadcast Storm Control
  - IEEE802.1Q-in-Q nested VLAN support
  - Full-duplex flow control (IEEE802.3x) and half-duplex backpressure
  - Extensive front-panel diagnostic LEDs; System: Power, TP Port, LINK/ACT, 10/100/1000Mbps, SFP Port 23, 24 or 15,16: SFP(LINK/ACT)

- **Management**

  - Supports concisely the status of port and easily port configuration
  - Supports per port traffic monitoring counters
  - Supports a snapshot of the system Information when you login
  - Supports port mirror function
  - Supports the static trunk function

- Supports 802.1Q VLAN
- Supports user management and limits one user to login
- Maximal packet length can be up to 9216 bytes for jumbo frame application
- Supports Broadcasting Suppression to avoid network suspended or crashed
- Supports to send the trap event while monitored events happened
- Supports default configuration which can be restored to overwrite the current configuration which is working on via Web UI and Reset button of the switch
- Supports on-line plug/unplug SFP modules
- Supports Quality of Service (QoS) for real time applications based on the information taken from Layer 2 to Layer 4, such as VoIP
- Built-in web-based management instead of using CLI interface, providing a more convenient GUI for the user

Publication date: January, 2005
Revision A1

1-4. View of 16 Gigabit Web Smart Switch

Fig. 1-1 Full View of 16 Gigabit Web Smart Switch

1-4-1. User Interfaces on the Front Panel (Button, LEDs and Plugs)

There are 16 TP Gigabit Ethernet ports and 2 SFP fiber ports for optional removable modules on the front panel of the switch. LED display area, locating on the left side of the panel, contains a Power LED, which indicates the power status and 16 ports working status of the switch.

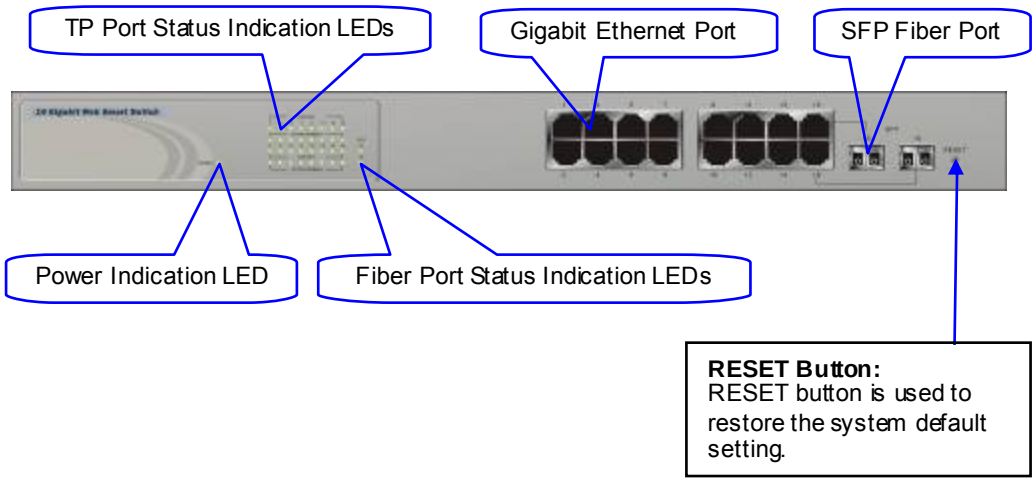


Fig. 1-2 Front View of 16 Gigabit Web Smart Switch

- **LED Indicators**

LED	Color	Function
System LED		
POWER	Green	Lit when +5V DC power is on and good
10/100/1000Ethernet TP Port LED		
LINK/ACT	Green	Lit when connection with remote device is good Blinks when any traffic is present Off when cable connection is not good
10/100/1000Mbps	Green/ Ember	Lit green when 1000Mbps speed is active Lit ember when 100Mbps speed is active Off when 10Mbps speed is active
1000SX/LX Gigabit Fiber Port LED		
SFP(LINK/ACT)	Green	Lit when connection with the remote device is good Blinks when any traffic is present Off when module connection is not good

Table1-1

1-4-2. User Interfaces on the Rear Panel

Fig. 1-3 Rear View of 16 Gigabit Web Smart Switch

1-5. View of the Optional Modules

In the switch, Port 15~16 includes two types of media --- TP and SFP Fiber (LC, BiDi-SC…); this port supports 10/100/1000Mbps TP or 1000Mbps SFP Fiber with auto-detected function. 1000Mbps SFP Fiber transceiver is used for high-speed connection expansion; nine optional SFP types provided for the switch are listed below:

1000Mbps LC, MM, SFP Fiber transceiver (SFP.0LC.202)

1000Mbps LC, SM 10km, SFP Fiber transceiver (SFP.0LC.212.10)

1000Mbps LC, SM 30km, SFP Fiber transceiver (SFP.0LC.212.30)

1000Mbps LC, SM 50km, SFP Fiber transceiver (SFP.0LC.212.50)

1000Mbps LC, SM 70km, SFP Fiber transceiver (SFP.0LC.212.70)

1000Mbps LC, SM 110km, SFP Fiber transceiver (SFP.0LC.212.B0)

1000Mbps BiDi SC, type 1, SM 20km, SFP Fiber WDM transceiver (SFP.0BS.621.201)

1000Mbps BiDi SC, type 2, SM 20km, SFP Fiber WDM transceiver (SFP.0BS.621.202)

1000Mbps LC, SM 10km, SFP Fiber transceiver with DDM (SFP.DLC.212.10)

Fig. 1-4 Front View of 1000Base-SX/LX LC, SFP Fiber Transceiver

Fig. 1-5 Front View of 1000Base-LX BiDi SC SFP Fiber Transceiver

2. Installation

2-1. Starting Gigabit Web Smart Switch Up

This section will give users a quick start for:

- Hardware and Cable Installation
- Management Station Installation
- Software booting and configuration

2-1-1. Hardware and Cable Installation

At the beginning, please do first:

Wear a grounding device to avoid the damage from electrostatic discharge

Be sure that power switch is OFF before you insert the power cord to power source

- **Installing Optional SFP Fiber Transceivers to the Gigabit Web Smart Switch**

Note: If you have no modules, please skip this section.

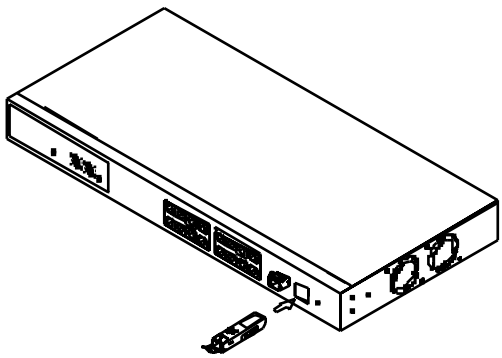


Fig. 2-1 Installation of Optional SFP Fiber Transceiver

- **Connecting the SFP Module to the Chassis:**

The optional SFP modules are hot swappable, so you can plug or unplug it before or after powering on.

1. Verify that the SFP module is the right model and conforms to the chassis
2. Slide the module along the slot. Also be sure that the module is properly seated against the slot socket/connector
3. Install the media cable for network connection
4. Repeat the above steps, as needed, for each module to be installed into slot(s)
5. Have the power ON after the above procedures are done

- **TP Port and Cable Installation**

In the switch, TP port supports MDI/MDI-X auto-crossover, so both types of cable, straight-through (Cable pin-outs for RJ-45 jack 1, 2, 3, 6 to 1, 2, 3, 6 in 10/100M TP; 1, 2, 3, 4, 5, 6, 7, 8 to 1, 2, 3, 4, 5, 6, 7, 8 in Gigabit TP) and crossed-over (Cable pin-outs for RJ-45 jack 1, 2, 3, 6 to 3, 6, 1, 2) can be used. It means you do not have to tell from them, just plug it.

Use Cat. 5 grade RJ-45 TP cable to connect to a TP port of the switch and the other end is connected to a network-aware device such as a workstation or a server.

Repeat the above steps, as needed, for each RJ-45 port to be connected to a Gigabit 10/100/1000 TP device.

Now, you can start having the switch in operation.

- **Power On**

The switch supports 100-240 VAC, 50-60 Hz power supply. The power supply will automatically convert the local AC power source to DC power. It does not matter whether any connection plugged into the switch or not when power on, even modules as well. After the power is on, all LED indicators will light up immediately and then all off except the power LED still keeps on. This represents a reset of the system.

- **Firmware Loading**

After resetting, the bootloader will load the firmware into the memory. It will take about 30 seconds, after that, the switch will flash all the LED once and automatically performs self-test and is in ready state.

2-1-2. Cabling Requirements

To help ensure a successful installation and keep the network performance good, please take a care on the cabling requirement. Cables with worse specification will render the LAN to work poorly.

2-1-2-1. Cabling Requirements for TP Ports

For Fast Ethernet TP network connection

The grade of the cable must be Cat. 5 or Cat. 5e with a maximum length of 100 meters.

Gigabit Ethernet TP network connection

The grade of the cable must be Cat. 5 or Cat. 5e with a maximum length of 100 meters. Cat. 5e is recommended.

2-1-2-2. Cabling Requirements for 1000SX/LX SFP Module

It is more complex and comprehensive contrast to TP cabling in the fiber media. Basically, there are two categories of fiber, multi mode (MM) and single mode (SM). The later is categorized into several classes by the distance it supports. They are SX, LX, LHX, XD, and ZX. From the viewpoint of connector type, there mainly are LC and BIDI SC.

Gigabit Fiber with multi-mode LC SFP module

Gigabit Fiber with single-mode LC SFP module

Gigabit Fiber with BiDi SC 1310nm SFP module

Gigabit Fiber with BiDi SC 1550nm SFP module

The following table lists the types of fiber that we support and those else not listed here are available upon request.

<table>
<tr><td rowspan="4">IEEE 802.3z Gigabit Ethernet 1000SX 850nm</td><td colspan="4">Multi-mode Fiber Cable and Modal Bandwidth</td></tr>
<tr><td colspan="2">Multi-mode 62.5/125μm</td><td colspan="2">Multi-mode 50/125μm</td></tr>
<tr><td>Modal Bandwidth</td><td>Distance</td><td>Modal Bandwidth</td><td>Distance</td></tr>
<tr><td>160MHz-Km</td><td>220m</td><td>400MHz-Km</td><td>500m</td></tr>
<tr><td>200MHz-Km</td><td>275m</td><td>500MHz-Km</td><td>550m</td></tr>
<tr><td rowspan="3">1000Base-LX/LHX/XD/ZX</td><td colspan="4">Single-mode Fiber 9/125μm</td></tr>
<tr><td colspan="4">Single-mode transceiver 1310nm 10Km</td></tr>
<tr><td colspan="4">Single-mode transceiver 1550nm 30, 50Km</td></tr>
<tr><td rowspan="4">1000Base-LX Single Fiber (BIDI SC)</td><td colspan="2" rowspan="2">Single-Mode *20Km</td><td>TX(Transmit)</td><td>1310nm</td></tr>
<tr><td>RX(Receive)</td><td>1550nm</td></tr>
<tr><td colspan="2" rowspan="2">Single-Mode *20Km</td><td>TX(Transmit)</td><td>1550nm</td></tr>
<tr><td>RX(Receive)</td><td>1310nm</td></tr>
</table>

Table2-1

2-1-2-3. Switch Cascading in Topology

- **Takes the Delay Time into Account**

Theoretically, the switch partitions the collision domain for each port in switch cascading that you may up-link the switches unlimitedly. In practice, the network extension (cascading levels & overall diameter) must follow the constraint of the IEEE 802.3/802.3u/802.3z and other 802.1 series protocol specifications, in which the limitations are the timing requirement from physical signals defined by 802.3 series specification of Media Access Control (MAC) and PHY, and timer from some OSI layer 2 protocols such as 802.1d, 802.1q, LACP and so on.

The fiber, TP cables and devices' bit-time delay (round trip) are as follows:

1000Base-X TP, Fiber		100Base-TX TP		100Base-FX Fiber	
Round trip Delay: 4096		Round trip Delay: 512			
Cat. 5 TP Wire:	11.12/m	Cat. 5 TP Wire:	1.12/m	Fiber Cable:	1.0/m
Fiber Cable :	10.10/m	TP to fiber Conv erter: 56			
Bit Time unit : 1ns (1sec./1000 Mega bit)		Bit Time unit: 0.01μs (1sec./100 Mega bit)			

Table 2-2

Sum up all elements' bit-time delay and the overall bit-time delay of wires/devices must be within Round Trip Delay (bit times) in a half-duplex network segment (collision domain). For full-duplex operation, this will not be applied. You may use the TP-Fiber module to extend the TP node distance over fiber optic and provide the long haul connection.

- **Typical Network Topology in Deployment**

A hierarchical network with minimum levels of switch may reduce the timing delay between server and client station. Basically, with this approach, it will minimize the number of switches in any one path; will lower the possibility of network loop and will improve network efficiency. If more than two switches are connected in the same network, select one switch as Level 1 switch and connect all other switches to it at Level 2. Server/Host is recommended to connect to the Level 1 switch. This is general if no VLAN or other special requirements are applied.

Case1: All switch ports are in the same local area network. Every port can access each other (See Fig. 2-2).

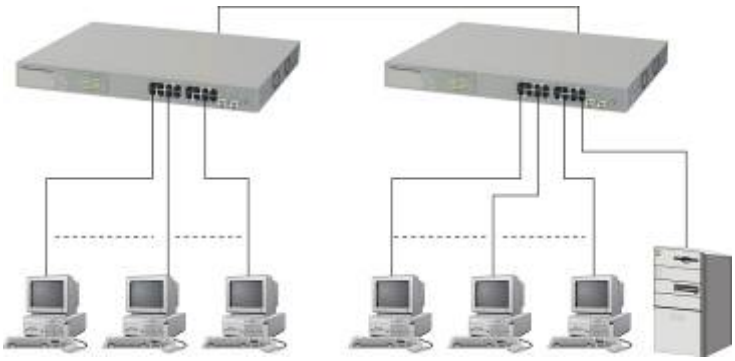


Fig. 2-2 No VLAN Configuration Diagram

If VLAN is enabled and configured, each node in the network that can communicate each other directly is bounded in the same VLAN area.

Here VLAN area is defined by what VLAN you are using. The switch supports both port-based VLAN and tag-based VLAN. They are different in practical deployment, especially in physical location. The following diagram shows how it works and what the difference they are.

Case2a: Port-based VLAN (See Fig.2-3).

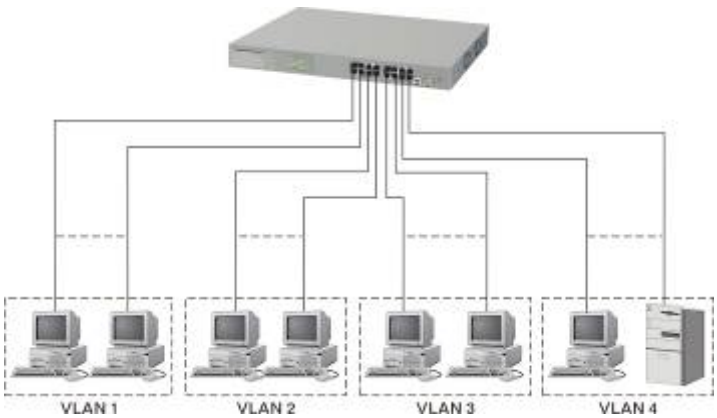


Fig. 2-3 Port-based VLAN Diagram

1. The same VLAN members could not be in different switches.
2. Every VLAN members could not access VLAN members each other.
3. The switch manager has to assign different names for each VLAN groups at one switch.

Case 2b: Port-based VLAN (See Fig.2-4).

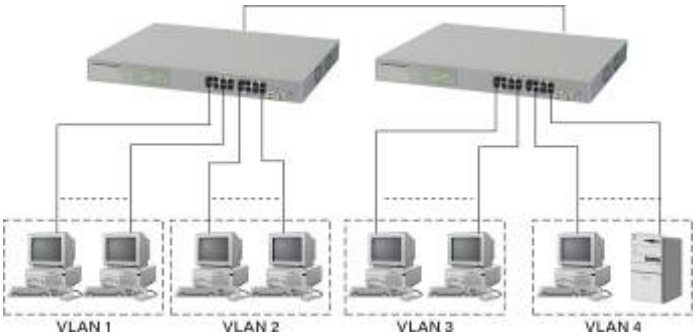


Fig. 2-4 Port-based VLAN Diagram

1. VLAN1 members could not access VLAN2, VLAN3 and VLAN4 members.
2. VLAN2 members could not access VLAN1 and VLAN3 members, but they could access VLAN4 members.
3. VLAN3 members could not access VLAN1, VLAN2 and VLAN4.
4. VLAN4 members could not access VLAN1 and VLAN3 members, but they could access VLAN2 members.

Case3a: The same VLAN members can be at different switches with the same VID (See Fig. 2-5).

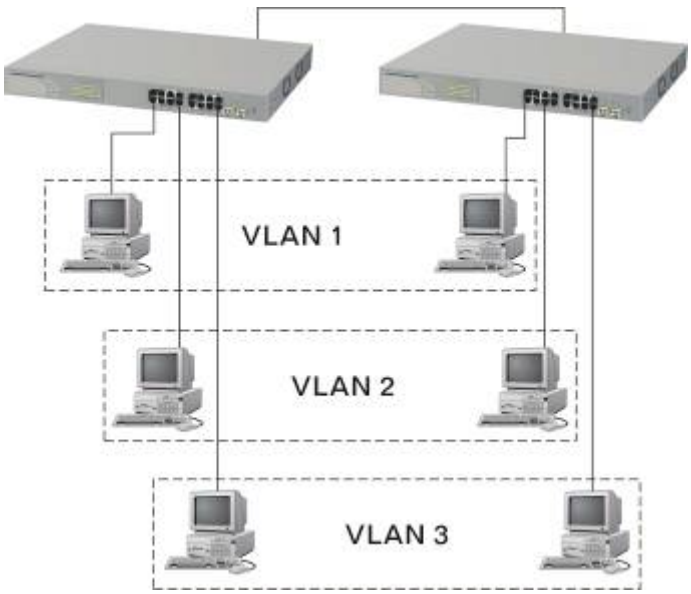


Fig. 2-5 Attribute-based VLAN Diagram

2-1-3. Configuring the Management Agent of Gigabit Web Smart Switch

In the way of web, user is allowed to startup the switch management function. Users can use any one of them to monitor and configure the switch. You can touch them through the following procedures.

Section 2-1-3-1: Configuring Management Agent of 16 Gigabit Web Smart Switch through Ethernet Port

2-1-3-1. Configuring Management Agent of Gigabit Web Smart Switch through Ethernet Port

There are two ways to configure and monitor the switch through the switch's Ethernet port. They are Web browser and SNMP manager. The user interface for the last one is NMS dependent and does not cover here. We just introduce the first type of management interface. Web-based UI for the switch is an interface in a highly friendly way.

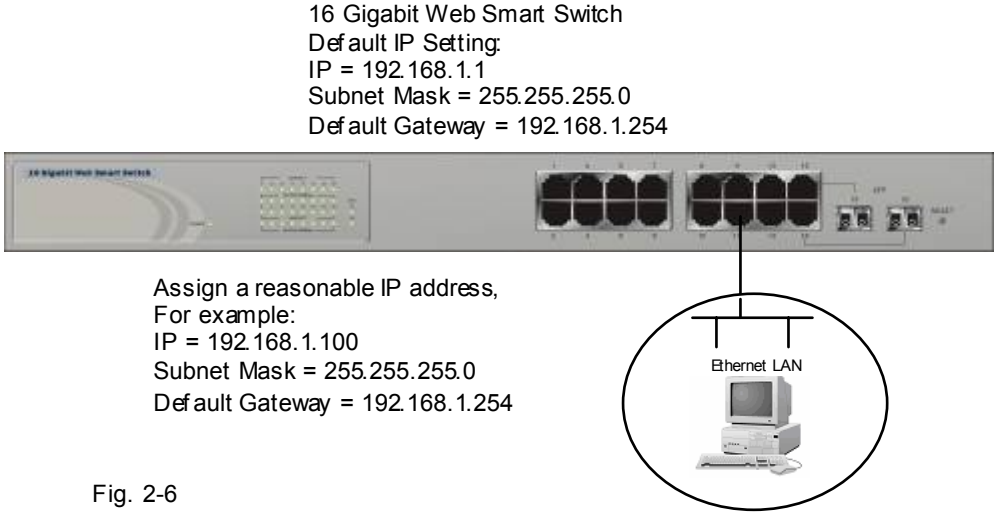


Fig. 2-6

- **Managing Gigabit Web Smart Switch through Ethernet Port**

Before you communicate with the switch, you have to finish first the configuration of the IP address or to know the IP address of the switch. Then, follow the procedures listed below.

Set up a physical path between the configured the switch and a PC by a qualified UTP Cat. 5 cable with RJ-45 connector.

Note: If PC directly connects to the switch, you have to setup the same subnet mask between them. But, subnet mask may be different for the PC in the remote site. Please refer to Fig. 2-6 about the Gigabit Web Smart Switch default IP address information.

Run web browser and follow the menu. Please refer to Chapter 4.

Fig. 2-7 the Login Screen for Web

2-1-4. IP Address Assignment

For IP address configuration, there are three parameters needed to be filled in. They are IP address, Subnet Mask, Default Gateway and DNS.

IP address:

The address of the network device in the network is used for internetworking communication. Its address structure looks is shown in the Fig. 2-8. It is “classful” because it is split into predefined address classes or categories.

Each class has its own network range between the network identifier and host identifier in the 32 bits address. Each IP address comprises two parts: network identifier (address) and host identifier (address). The former indicates the network where the addressed host resides, and the latter indicates the individual host in the network which the address of host refers to. And the host identifier must be unique in the same LAN. Here the term of IP address we used is version 4, known as IPv4.

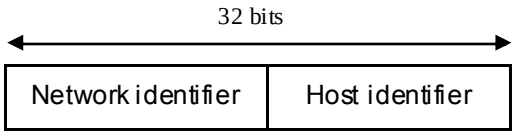
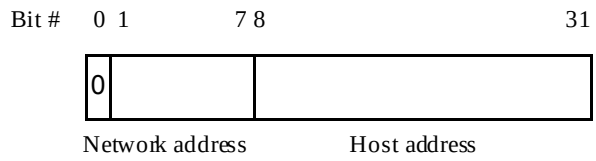


Fig. 2-8 IP address structure

With the classful addressing, it divides IP address into three classes, class A, class B and class C. The rest of IP addresses are for multicast and broadcast. The bit length of the network prefix is the same as that of the subnet mask and is denoted as IP address/X, for example, 192.168.1.0/24. Each class has its address range described below.

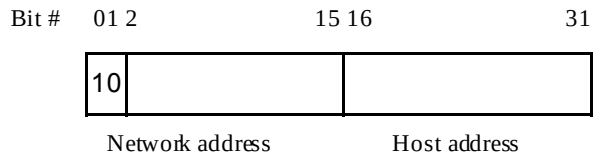
Class A:

Address is less than 126.255.255.255. There are a total of 126 networks can be defined because the address 0.0.0.0 is reserved for default route and 127.0.0.0/8 is reserved for loopback function.



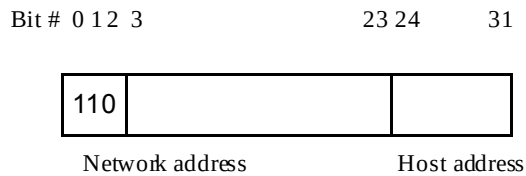
Class B:

IP address range between 128.0.0.0 and 191.255.255.255. Each class B network has a 16-bit network prefix followed 16-bit host address. There are 16,384 (2^14)/16 networks able to be defined with a maximum of 65534 (2^16 –2) hosts per network.



Class C:

IP address range between 192.0.0.0 and 223.255.255.255. Each class C network has a 24-bit network prefix followed 8-bit host address. There are 2,097,152 (2^21)/24 networks able to be defined with a maximum of 254 (2^8 –2) hosts per network.



Class D and E:

Class D is a class with first 4 MSB (Most significance bit) set to 1-1-1-0 and is used for IP Multicast. See also RFC 1112. Class E is a class with first 4 MSB set to 1-1-1-1 and is used for IP broadcast.

According to IANA (Internet Assigned Numbers Authority), there are three specific IP address blocks reserved and able to be used for extending internal network. We call it Private IP address and list below:

Class A	10.0.0.0 --- 10.255.255.255
Class B	172.16.0.0 --- 172.31.255.255
Class C	192.168.0.0 --- 192.168.255.255

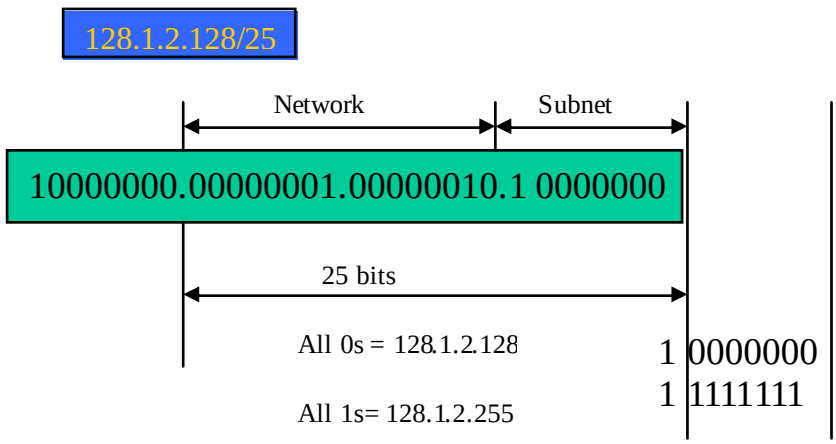
Please refer to RFC 1597 and RFC 1466 for more information.

Subnet mask:

It means the sub-division of a class-based network or a CIDR block. The subnet is used to determine how to split an IP address to the network prefix and the host address in bitwise basis. It is designed to utilize IP address more efficiently and ease to manage IP network.

For a class B network, 128.1.2.3, it may have a subnet mask 255.255.0.0 in default, in which the first two bytes is with all 1s. This means more than 60 thousands of nodes in flat IP address will be at the same network. It's too large to manage practically. Now if we divide it into smaller network by extending network prefix from 16 bits to, say 24 bits, that's using its third byte to subnet this class B network. Now it has a subnet mask 255.255.255.0, in which each bit of the first three bytes is 1. It's now clear that the first two bytes is used to identify the class B network, the third byte is used to identify the subnet within this class B network and, of course, the last byte is the host number.

Not all IP address is available in the sub-netted network. Two special addresses are reserved. They are the addresses with all zero's and all one's host number. For example, an IP address 128.1.2.128, what IP address reserved will be looked like? All 0s mean the network itself, and all 1s mean IP broadcast.



In this diagram, you can see the subnet mask with 25-bit long, 255.255.255.128, contains 126 members in the sub-netted network. Another is that the length of network prefix equals the number of the bit with 1s in that subnet mask. With this, you can easily count the number of IP addresses matched. The following table shows the result.

Prefix Length	No. of IP matched	No. of Addressable IP
/32	1	-
/31	2	-
/30	4	2
/29	8	6
/28	16	14
/27	32	30
/26	64	62
/25	128	126
/24	256	254
/23	512	510
/22	1024	1022
/21	2048	2046
/20	4096	4094
/19	8192	8190
/18	16384	16382
/17	32768	32766
/16	65536	65534

Table 2-3

According to the scheme above, a subnet mask 255.255.255.0 will partition a network with the class C. It means there will have a maximum of 254 effective nodes existed in this sub-netted network and is considered a physical network in an autonomous network. So it owns a network IP address which may looks like 168.1.2.0.

With the subnet mask, a bigger network can be cut into small pieces of network. If we want to have more than two independent networks in a worknet, a partition to the network must be performed. In this case, subnet mask must be applied.

For different network applications, the subnet mask may look like 255.255.255.240. This means it is a small network accommodating a maximum of 15 nodes in the network.

Default gateway:

For the routed packet, if the destination is not in the routing table, all the traffic is put into the device with the designated IP address, known as default router. Basically, it is a routing policy.

For assigning an IP address to the switch, you just have to check what the IP address of the network will be connected with the switch. Use the same network address and append your host address to it.

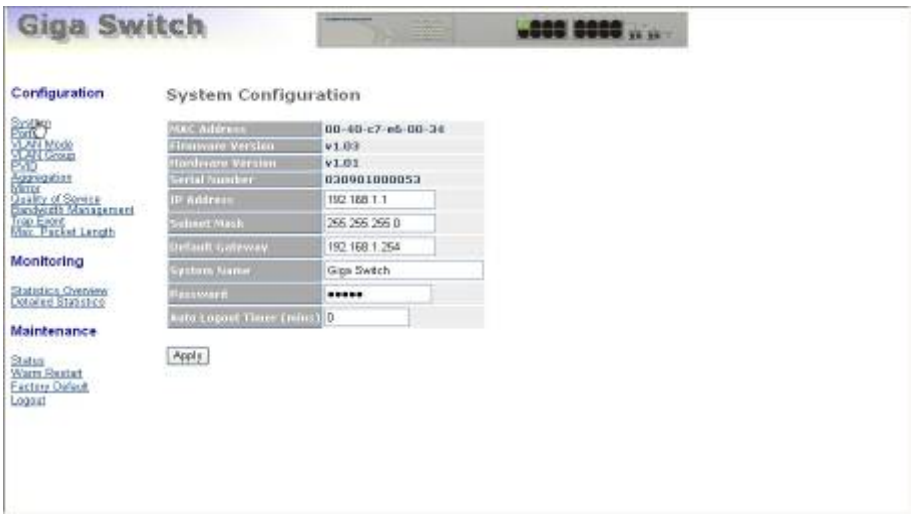


Fig. 2-9

First, IP Address: as shown in the Fig. 2-9, enter “192.168.1.1”, for instance. For sure, an IP address such as 192.168.1.x must be set on your PC.

Second, Subnet Mask: as shown in the Fig. 2-9, enter “255.255.255.0”. Any subnet mask such as 255.255.255.x is allowable in this case.

2-2. Typical Applications

The Gigabit Web Smart Switch implements Gigabit Ethernet TP ports with auto MDIX and two slots for the removable module supporting comprehensive fiber types of connection, including LC and BiDi-LC SFP modules. For more details on the specification of the switch, please refer to Appendix A.

The switch is suitable for the following applications.

Central Site/Remote site application is used in carrier or ISP (See Fig. 2-10)

Peer-to-peer application is used in two remote offices (See Fig. 2-11)

Office network(See Fig. 2-12)

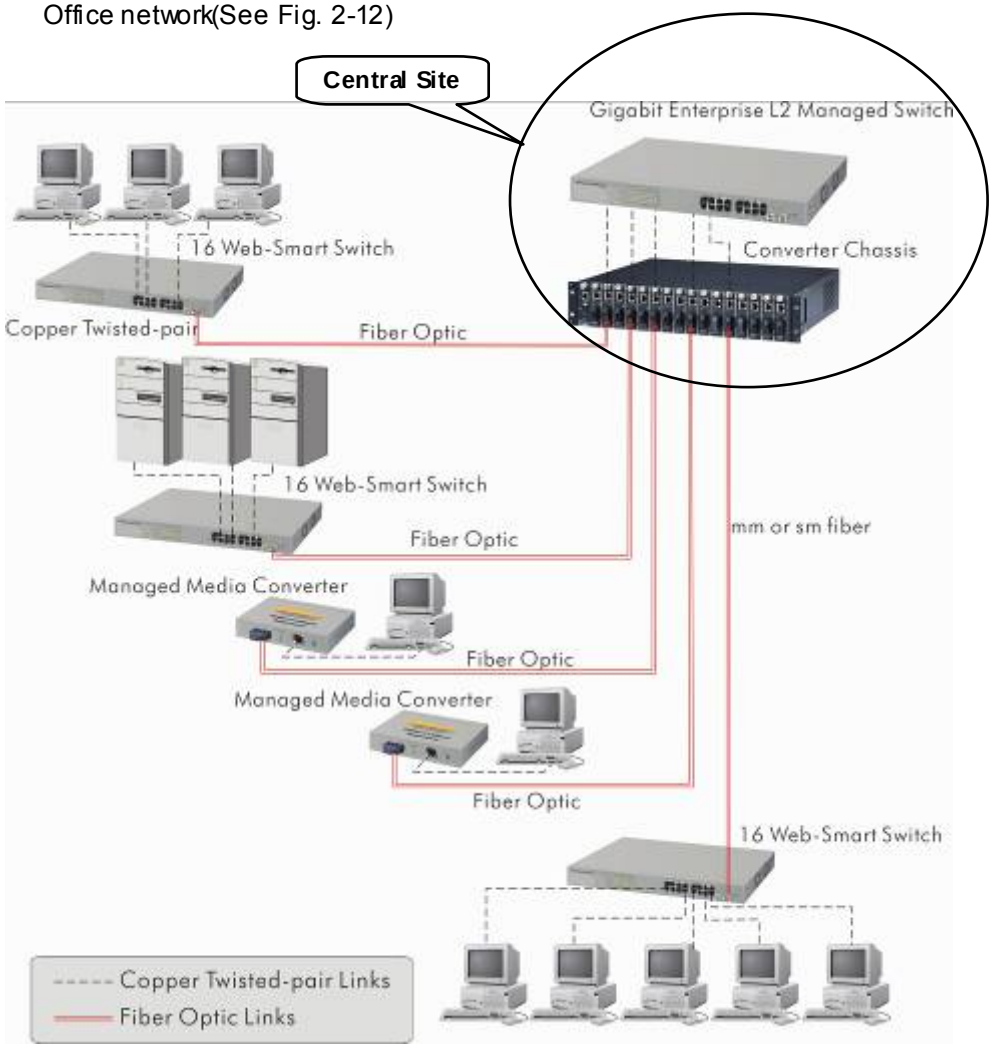


Fig. 2-10 Network Connection between Remote Site and Central Site

Fig. 2-10 is a system wide basic reference connection diagram. This diagram demonstrates how the switch connects with other network devices and hosts.

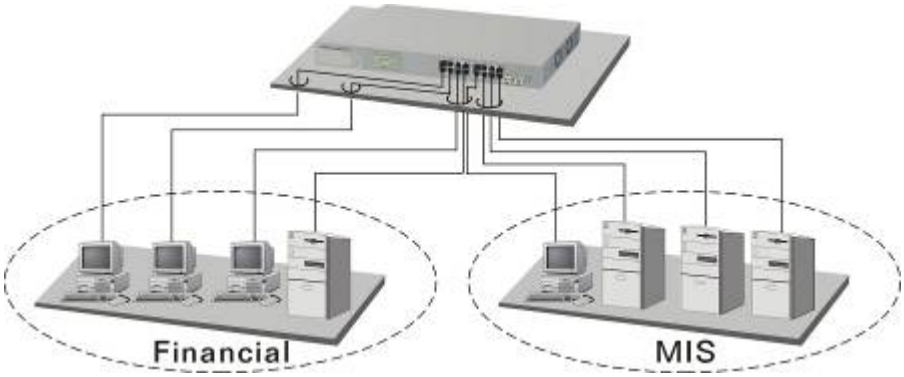


Fig. 2-11 Peer-to-peer Network Connection

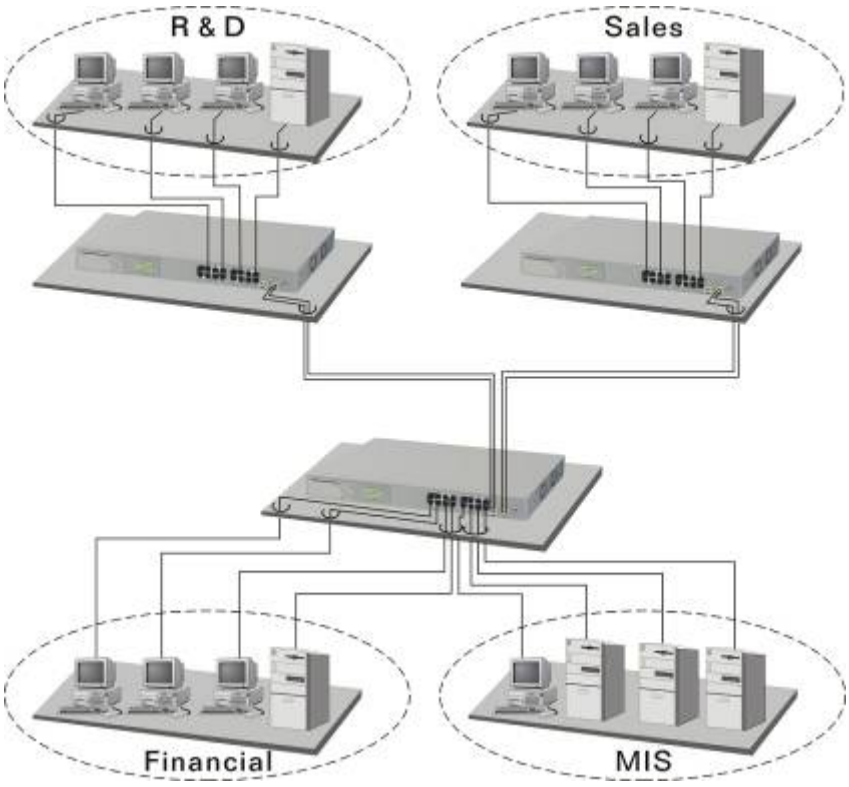


Fig. 2-12 Office Network Connection

3. Basic Concept and Management

This chapter will tell you the basic concept of features to manage this switch and how they work.

3-1. What's the Ethernet

Ethernet originated and was implemented at Xerox in Palo Alto, CA in 1973 and was successfully commercialized by Digital Equipment Corporation (DEC), Intel and Xerox (DIX) in 1980. In 1992, Grand Junction Networks unveiled a new high speed Ethernet with the same characteristic of the original Ethernet but operated at 100Mbps, called Fast Ethernet now. This means Fast Ethernet inherits the same frame format, CSMA/CD, software interface. In 1998, Gigabit Ethernet was rolled out and provided 1000Mbps. Now 10G/s Ethernet is under approving. Although these Ethernet have different speed, they still use the same basic functions. So they are compatible in software and can connect each other almost without limitation. The transmission media may be the only problem.

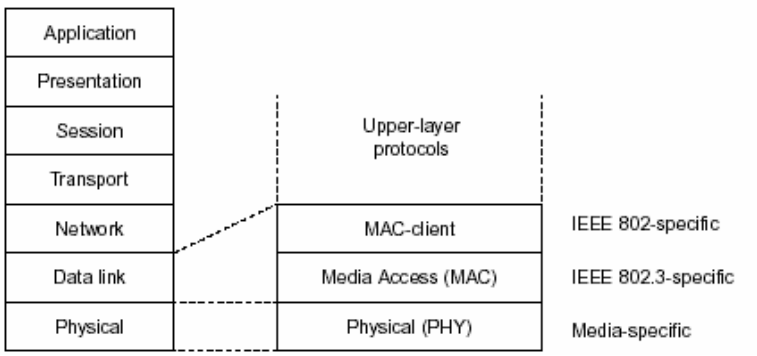
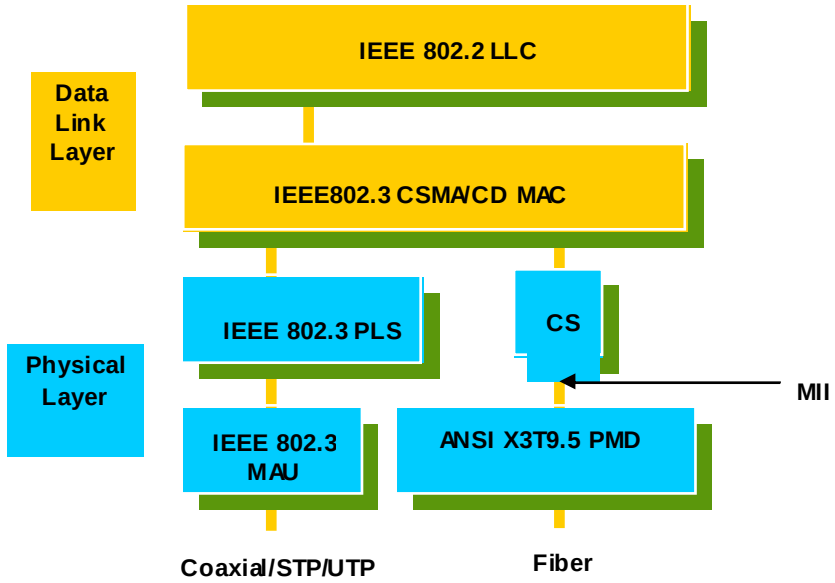


Fig. 3-1 IEEE 802.3 reference model vs. OSI reference mode

In Fig. 3-1, we can see that Ethernet locates at the Data Link layer and Physical layer and comprises three portions, including logical link control (LLC), media access control (MAC), and physical layer. The first two comprises Data link layer, which performs splitting data into frame for transmitting, receiving acknowledge frame, error checking and re-transmitting when not received correctly as well as provides an error-free channel upward to network layer.



This above diagram shows the Ethernet architecture, LLC sub-layer and MAC sub-layer, which are responded to the Data Link layer, and transceivers, which are responded to the Physical layer in OSI model. In this section, we are mainly describing the MAC sub-layer.

Logical Link Control (LLC)

Data link layer is composed of both the sub-layers of MAC and MAC-client. Here MAC client may be logical link control or bridge relay entity.

Logical link control supports the interface between the Ethernet MAC and upper layers in the protocol stack, usually Network layer, which is nothing to do with the nature of the LAN. So it can operate over other different LAN technology such as Token Ring, FDDI and so on. Likewise, for the interface to the MAC layer, LLC defines the services with the interface independent of the medium access technology and with some of the nature of the medium itself.

DSAP address	SSAP address	Control	Information
8 bits	8 bits	8 or 16 bits	M*8 bits

DSAP address	=	Destination service access point address field
SSAP address	=	Source service access point address field
Control	=	Control field [16 bits for formats that include sequence numbering, and 8 bits for formats that do not (see 5.2)]
Information	=	Information field
*	=	Multiplication
M	=	An integer value equal to or greater than 0. (Upper bound of M is a function of the medium access control methodology used.)

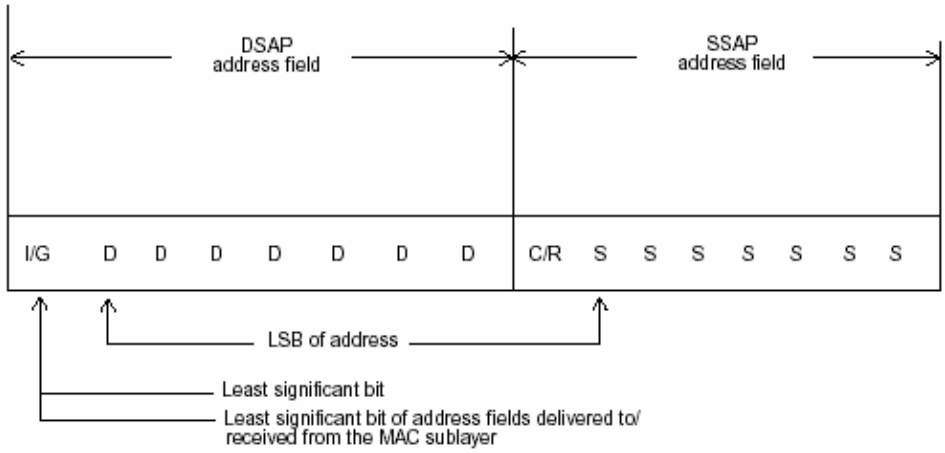
Table 3-1 LLC Format

The table 3-1 is the format of LLC PDU. It comprises four fields, DSAP, SSAP, Control and Information. The DSAP address field identifies the one or more service access points, in which the I/G bit indicates it is individual or group address. If all bit of DSAP is 1s, it's a global address. The SSAP address field identifies the specific services indicated by C/R bit (command or response). The DSAP and SSAP pair with some reserved values indicates some well-known services listed in the table below.

0xAAAA	SNAP
0xE0E0	Novell IPX
0xF0F0	NetBios
0xFEFE	IOS network layer PDU
0xFFFF	Novell IPX 802.3 RAW packet
0x4242	STP BPDU
0x0606	IP
0x9898	ARP

Table 3-2

LLC type 1 connectionless service, LLC type 2 connection-oriented service and LLC type 3 acknowledge connectionless service are three types of LLC frame for all classes of service. In Fig 3-2, it shows the format of Service Access Point (SAP). Please refer to IEEE802.2 for more details.



I/G = 0 Individual DSAP
I/G = 1 Group DSAP
C/R = 0 Command
C/R = 1 Response

XODDDDDD DSAP address
XOSSSSSS SSAP address

X1DDDDDD Reserved for ISO definition
X1SSSSSS Reserved for ISO definition

Fig. 3-2 SAP Format

3-2. Media Access Control (MAC)

MAC Addressing

Because LAN is composed of many nodes, for the data exchanged among these nodes, each node must have its own unique address to identify who should send the data or should receive the data. In OSI model, each layer provides its own mean to identify the unique address in some form, for example, IP address in network layer.

The MAC is belonged to Data Link Layer (Layer 2), the address is defined to be a 48-bit long and locally unique address. Since this type of address is applied only to the Ethernet LAN media access control (MAC), they are referred to as MAC addresses.

The first three bytes are Organizational Unique Identifier (OUI) code assigned by IEEE. The last three bytes are the serial number assigned by the vendor of the network device. All these six bytes are stored in a non-volatile memory in the device. Their format is as the following table and normally written in the form as aa-bb-cc-dd-ee-ff, a 12 hexadecimal digits separated by hyphens, in which the aa-bb-cc is the OUI code and the dd-ee-ff is the serial number assigned by manufacturer.

Bit 47 bit 0

1st byte	2nd byte	3rd byte	4th byte	5th byte	6th byte
OUI code			Serial number		

Table 3-3 Ethernet MAC address

The first bit of the first byte in the Destination address (DA) determines the address to be a Unicast (0) or Multicast frame (1), known as I/G bit indicating individual (0) or group (1). So the 48-bit address space is divided into two portions, Unicast and Multicast. The second bit is for global-unique (0) or locally-unique address. The former is assigned by the device manufacturer, and the later is usually assigned by the administrator. In practice, global-unique addresses are always applied.

A unicast address is identified with a single network interface. With this nature of MAC address, a frame transmitted can exactly be received by the target an interface the destination MAC points to.

A multicast address is identified with a group of network devices or network interfaces. In Ethernet, a many-to-many connectivity in the LANs is provided. It provides a mean to send a frame to many network devices at a time. When all bit of DA is 1s, it is a broadcast, which means all network device except the sender itself can receive the frame and response.

Ethernet Frame Format

There are two major forms of Ethernet frame, type encapsulation and length encapsulation, both of which are categorized as four frame formats 802.3/802.2 SNAP, 802.3/802.2, Ethernet II and Netware 802.3 RAW. We will introduce the basic Ethernet frame format defined by the IEEE 802.3 standard required for all MAC implementations. It contains seven fields explained below.

PRE	SFD	DA	SA	Type/Length	Data	Pad bit if any	FCS
7	7	6	6	2	46-1500		4

Fig. 3-3 Ethernet frame structure

- **Preamble (PRE)** —The PRE is 7-byte long with alternating pattern of ones and zeros used to tell the receiving node that a frame is coming, and to synchronize the physical receiver with the incoming bit stream. The preamble pattern is:

  10101010 10101010 10101010 10101010 10101010 10101010 10101010

  Start-of-frame delimiter (SFD) — The SFD is one-byte long with alternating pattern of ones and zeros, ending with two consecutive 1-bits. It immediately follows the preamble and uses the last two consecutive 1s bit to indicate that the next bit is the start of the data packet and the left-most bit in the left-most byte of the destination address. The SFD pattern is 10101011.

Destination address (DA) — The DA field is used to identify which network device(s) should receive the packet. It is a unique address. Please see the section of MAC addressing.

Source addresses (SA) — The SA field indicates the source node. The SA is always an individual address and the left-most bit in the SA field is always 0.

Length/Type — This field indicates either the number of the data bytes contained in the data field of the frame, or the Ethernet type of data. If the value of first two bytes is less than or equal to 1500 in decimal, the number of bytes in the data field is equal to the Length/Type value, i.e. this field acts as Length indicator at this moment. When this field acts as Length, the frame has optional fields for 802.3/802.2 SNAP encapsulation, 802.3/802.2 encapsulation and Netware 802.3 RAW encapsulation. Each of them has different fields following the Length field.

If the Length/Type value is greater than 1500, it means the Length/Type acts as Type. Different type value means the frames with different protocols running over Ethernet being sent or received.

For example,

0x0800	IP datagram
0x0806	ARP
0x0835	RARP
0x8137	IPX datagram
0x86DD	IPv6

Data — Less than or equal to 1500 bytes and greater or equal to 46 bytes. If data is less than 46 bytes, the MAC will automatically extend the padding bits and have the payload be equal to 46 bytes. The length of data field must equal the value of the Length field when the Length/Type acts as Length.

Frame check sequence (FCS) — This field contains a 32-bit cydic redundancy check (CRC) value, and is a check sum computed with DA, SA, through the end of the data field with the following polynomial.

$$G(x) = x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$$

It is created by the sending MAC and recalculated by the receiving MAC to check if the packet is damaged or not.

How does a MAC work?

The MAC sub-layer has two primary jobs to do:

1. *Receiving and transmitting data*. When receiving data, it parses frame to detect error; when transmitting data, it performs frame assembly.
2. *Performing Media access control*. It prepares the initiation jobs for a frame transmission and makes recovery from transmission failure.

Frame transmission

As Ethernet adopted Carrier Sense Multiple Access with Collision Detect (CSMA/CD), it detects if there is any carrier signal from another network device running over the physical medium when a frame is ready for transmission. This is referred to as sensing carrier, also “Listen”. If there is signal on the medium, the MAC defers the traffic to avoid a transmission collision and waits for a random period of time, called backoff time, then sends the traffic again.

After the frame is assembled, when transmitting the frame, the preamble (PRE) bytes are inserted and sent first, then the next, Start of frame Delimiter (SFD), DA, SA and through the data field and FCS field in turn. The followings summarize what a MAC does before transmitting a frame.

MAC will assemble the frame. First, the preamble and Start-of-Frame delimiter will be put in the fields of PRE and SFD, followed DA, SA, tag ID if tagged VLAN is applied, Ethertype or the value of the data length, and payload data field, and finally put the FCS data in order into the responded fields.

Listen if there is any traffic running over the medium. If yes, wait.

If the medium is quiet, and no longer senses any carrier, the MAC waits for a period of time, i.e. inter-frame gap time to have the MAC ready with enough time and then start transmitting the frame.

During the transmission, MAC keeps monitoring the status of the medium. If no collision happens until the end of the frame, it transmits successfully. If there is a collision happened, the MAC will send the patterned jamming bit to guarantee the collision event propagated to all involved network devices, then wait for a random period of time, i.e. backoff time. When backoff time expires, the MAC goes back to the beginning state and attempts to transmit again. After a collision happens, MAC increases the transmission attempts. If the count of the transmission attempt reaches 16 times, the frame in MAC’s queue will be discarded.

Ethernet MAC transmits frames in half-duplex and full-duplex ways. In half-duplex operation mode, the MAC can either transmit or receive frame at a moment, but cannot do both jobs at the same time.

As the transmission of a MAC frame with the half-duplex operation exists only in the same collision domain, the carrier signal needs to spend time to travel to reach the targeted device. For two most-distant devices in the same collision domain, when one sends the frame first, and the second sends the frame, in worst-case, just before the frame from the first device arrives. The collision happens and will be detected by the second device immediately. Because of the medium delay, this corrupted signal needs to spend some time to propagate back to the first device. The maximum time to detect a collision is approximately twice the signal propagation time between the two most-distant devices. This maximum time is traded-off by the collision recovery time and the diameter of the LAN.

In the original 802.3 specification, Ethernet operates in half duplex only. Under this condition, when in 10Mbps LAN, it's 2500 meters, in 100Mbps LAN, it's approximately 200 meters and in 1000Mbps, 200 meters. According to the theory, it should be 20 meters. But it's not practical, so the LAN diameter is kept by using to increase the minimum frame size with a variable-length non-data extension bit field which is removed at the receiving MAC. The following tables are the frame format suitable for 10M, 100M and 1000M Ethernet, and some parameter values that shall be applied to all of these three types of Ethernet.

Actually, the practice Gigabit Ethernet chips do not feature this so far. They all have their chips supported full-duplex mode only, as well as all network vendors' devices. So this criterion should not exist at the present time and in the future. The switch's Gigabit module supports only full-duplex mode.

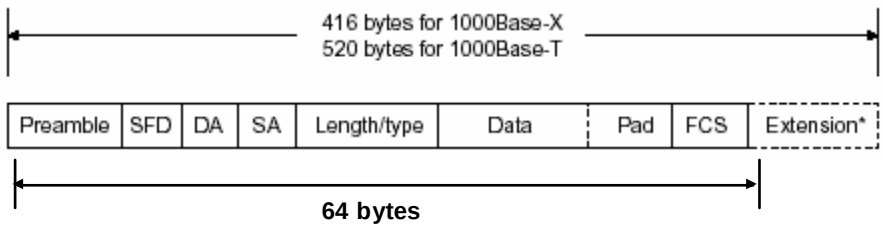
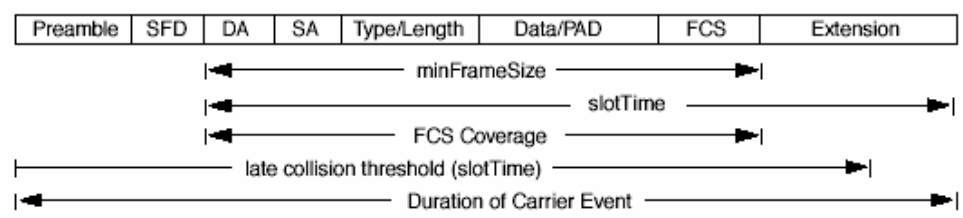


Fig. 3-4 Gigabit Ethernet Frame

Parameter value/LAN	10Base	100Base	1000Base
Max. collision domain DTE to DTE	100 meters	100 meters for UTP 412 meters for fiber	100 meters for UTP 316 meters for fiber
Max. collision domain with repeater	2500 meters	205 meters	200 meters
Slot time	512 bit times	512 bit times	512 bit times
Interframe Gap	9.6us	0.96us	0.096us
AttemptLimit	16	16	16
BackoffLimit	10	10	10
JamSize	32 bits	32 bits	32 bits
MaxFrameSize	1518	1518	1518
MinFrameSize	64	64	64
BurstLimit	Not applicable	Not applicable	65536 bits

Table 3-4 Ethernet parameters for half duplex mode



In full-duplex operation mode, both transmitting and receiving frames are processed simultaneously. This doubles the total bandwidth. Full duplex is much easier than half duplex because it does not involve media contention, collision, retransmission schedule, padding bits for short frame. The rest functions follow the specification of IEEE802.3. For example, it must meet the requirement of minimum inter-frame gap between successive frames and frame format the same as that in the half-duplex operation.

Because no collision will happen in full-duplex operation, for sure, there is no mechanism to tell all the involved devices. What will it be if receiving device is busy and a frame is coming at the same time? Can it use “backpressure” to tell the source device? A function flow control is introduced in the full-duplex operation.

3-3. Flow Control

Flow control is a mechanism to tell the source device stopping sending frame for a specified period of time designated by target device until the PAUSE time expires. This is accomplished by sending a PAUSE frame from target device to source device. When the target is not busy and the PAUSE time is expired, it will send another PAUSE frame with zero time-to-wait to source device. After the source device receives the PAUSE frame, it will again transmit frames immediately. PAUSE frame is identical in the form of the MAC frame with a pause-time value and with a special destination MAC address 01-80-C2-00-00-01. As per the specification, PAUSE operation can not be used to inhibit the transmission of MAC control frame.

Normally, in 10Mbps and 100Mbps Ethernet, only symmetric flow control is supported. However, some switches (e.g. 16 Gigabit Web Smart Switch) support not only symmetric but asymmetric flow controls for the special application. In Gigabit Ethernet, both symmetric flow control and asymmetric flow control are supported. Asymmetric flow control only allows transmitting PAUSE frame in one way from one side, the other side is not but receipt-and-discard the flow control information. Symmetric flow control allows both two ports to transmit PASUE frames each other simultaneously.

Inter-frame Gap time

After the end of a transmission, if a network node is ready to transmit data out and if there is no carrier signal on the medium at that time, the device will wait for a period of time known as an inter-frame gap time to have the medium clear and stabilized as well as to have the jobs ready, such as adjusting buffer counter, updating counter and so on, in the receiver site. Once the inter-frame gap time expires after the de-assertion of carrier sense, the MAC transmits data. In IEEE802.3 specification, this is 96-bit time or more.

Collision

Collision happens only in half-duplex operation. When two or more network nodes transmit frames at approximately the same time, a collision always occurs and interferes with each other. This results the carrier signal distorted and un-discriminated. MAC can afford detecting, through the physical layer, the distortion of the carrier signal. When a collision is detected during a frame transmission, the transmission will not stop immediately but, instead, continues transmitting until the rest bits specified by jamSize are completely transmitted. This guarantees the duration of collision is enough to have all involved devices able to detect the collision. This is referred to as Jamming. After jamming pattern is sent, MAC stops transmitting the rest data queued in the buffer and waits for a random period of time, known as backoff time with the following formula. When backoff time expires, the device goes back to the state of attempting to transmit frame. The backoff time is determined by the formula below. When the times of collision is increased, the backoff time is getting long until the collision times excess 16. If this happens, the frame will be discarded and backoff time will also be reset.

$$0 \le r < 2^k$$

where

k = min (n, 10)

Frame Reception

In essence, the frame reception is the same in both operations of half duplex and full duplex, except that full-duplex operation uses two buffers to transmit and receive the frame independently. The receiving node always “listens” if there is traffic running over the medium when it is not receiving a frame. When a frame destined for the target device comes, the receiver of the target device begins receiving the bit stream, and looks for the PRE (Preamble) pattern and Start-of-Frame Delimiter (SFD) that indicates the next bit is the starting point of the MAC frame until all bit of the frame is received.

For a received frame, the MAC will check:

If it is less than one slotTime in length, i.e. short packet, and if yes, it will be discarded by MAC because, by definition, the valid frame must be longer than the slotTime. If the length of the frame is less than one slotTime, it means there may be a collision happened somewhere or an interface malfunctioned in the LAN. When detecting the case, the MAC drops the packet and goes back to the ready state.

If the DA of the received frame exactly matches the physical address that the receiving MAC owns or the multicast address designated to recognize. If not, discards it and the MAC passes the frame to its client and goes back to the ready state.

If the frame is too long. If yes, throws it away and reports frameTooLong.

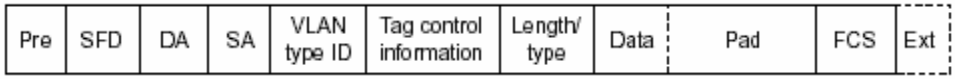
If the FCS of the received frame is valid. If not, for 10M and 100M Ethernet, discards the frame. For Gigabit Ethernet or higher speed Ethernet, MAC has to check one more field, i.e. extra bit field, if FCS is invalid. If there is any extra bits existed, which must meet the specification of IEEE802.3. When both FCS and extra bits are valid, the received frame will be accepted, otherwise discards the received frame and reports frameCheckError if no extra bits appended or alignmentError if extra bits appended.

If the length/type is valid. If not, discards the packet and reports lengthError.

If all five procedures above are ok, then the MAC treats the frame as good and de-assembles the frame.

What if a VLAN tagging is applied?

VLAN tagging is a 4-byte long data immediately following the MAC source address. When tagged VLAN is applied, the Ethernet frame structure will have a little change shown as follows.



Only two fields, VLAN ID and Tag control information are different in comparison with the basic Ethernet frame. The rest fields are the same.

The first two bytes is VLAN type ID with the value of 0x8100 indicating the received frame is tagged VLAN and the next two bytes are Tag Control Information (TCI) used to provide user priority and VLAN ID, which are explained respectively in the following table.

Bits 15-13	User Priority 7-0, 0 is lowest priority
Bit 12	CFI (Canonical Format Indicator) 1: RIF field is present in the tag header 0: No RIF field is present
Bits 11-0	VID (VLAN Identifier) 0x000: Null VID. No VID is present and only user priority is present. 0x001: Default VID 0xFFF: Reserved

Table 3-5

Note: RIF is used in Token Ring network to provide source routing and comprises two fields, Routing Control and Route Descriptor.

When MAC parses the received frame and finds a reserved special value 0x8100 at the location of the Length/Type field of the normal non-VLAN frame, it will interpret the received frame as a tagged VLAN frame. If this happens in a switch, the MAC will forward it, according to its priority and egress rule, to all the ports that is associated with that VID. If it happens in a network interface card, MAC will deprive of the tag header and process it in the same way as a basic normal frame. For a VLAN-enabled LAN, all involved devices must be equipped with VLAN optional function.

At operating speeds above 100 Mbps, the slotTime employed at slower speeds is inadequate to accommodate network topologies of the desired physical extent. Carrier Extension provides a means by which the slotTime can be increased to a sufficient value for the desired topologies, without increasing the minFrameSize parameter, as this would have deleterious effects. Nondata bits, referred to as extension bits, are appended to frames that are less than slotTime bits in length so that the resulting transmission is at least one slotTime in duration. Carrier Extension can be performed only if the underlying physical layer is capable of sending and receiving symbols that are readily distinguished from data symbols, as is the case in most physical layers that use a block encoding/decoding scheme.

The maximum length of the extension is equal to the quantity (slotTime - minFrameSize). The MAC continues to monitor the medium for collisions while it is transmitting extension bits, and it will treat any collision that occurs after the threshold (slotTime) as a late collision.

3-4. How does a switch work?

The switch is a layer 2 Ethernet Switch equipped with 16 Fast Ethernet ports and 2 optional modules which support Gigabit Ethernet or 100M Ethernet. Each port on it is an independent LAN segment and thus has 26 LAN segments and 26 collision domains, contrast to the traditional shared Ethernet HUB in which all ports share the same media and use the same collision domain and thus limit the bandwidth utilization. With switch's separated collision domain, it can extend the LAN diameter farther than the shared HUB does and highly improve the efficiency of the traffic transmission.

Due to the architecture, the switch can provide full-duplex operation to double the bandwidth per port and many other features, such as VLAN, bandwidth aggregation and so on, not able to be supported in a shared hub.

Terminology

Separate Access Domains:

As per the description in the section of "What's the Ethernet", Ethernet utilizes CSMA/CD to arbitrate who can transmit data to the station(s) attached in the LAN. When more than one station transmits data within the same slot time, the signals will collide, referred to as collision. The arbitrator will arbitrate who should gain the media. The arbitrator is a distributed mechanism in which all stations contend to gain the media. Please refer to "What's the Ethernet" for more details.

In Fig.3-5, assumed in half duplex, you will see some ports of the switch are linked to a shared HUB, which connects many hosts, and some ports just are individually linked to a single host. The hosts attached to a shared hub will be in the same collision domain, separated by the switch, and use CSMA/CD rule. For the host directly attached to the switch, because no other host(s) joins the traffic contention, hence it will not be affected by CSMA/CD. These LAN segments are separated in different access domains by the switch.

Micro-segmentation:

To have a port of the switch connected to a single host is referred to as micro-segmentation. It has the following interesting characteristics.

There is no need the access contention (e.g.Collision). They have their own access domain. But, collision still could happen between the host and the switch port.

When performing the full duplex, the collision vanishes.

The host owns a dedicated bandwidth of the port.

The switch port can run at different speed, such as 10Mbps, 100Mbps or 1000Mbps. A shared hub cannot afford this.

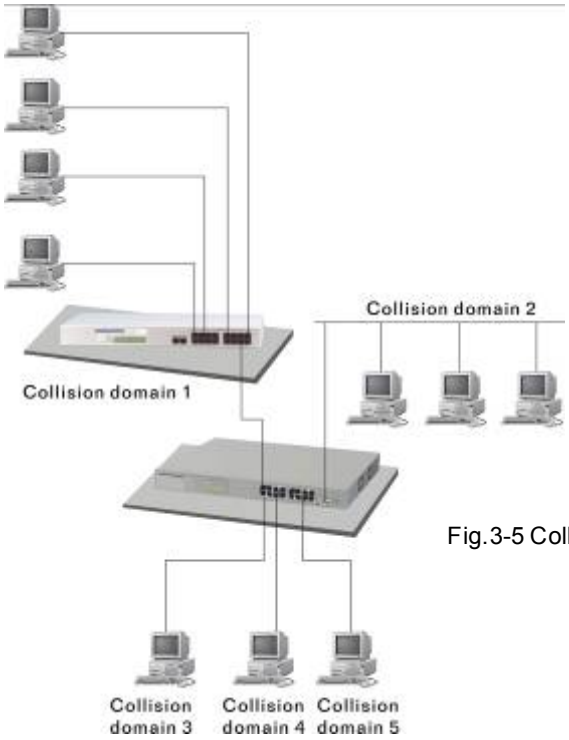


Fig.3-5 Collision Domain

Extended Distance Limitations:

The diameter of a half-duplex LAN segment is determined by its maximum propagation delay time. For example, in 10M LAN, the most distance of a LAN segment using yellow cable is 2500 meters and 185 meters when using coaxial cable. The switch with its per port per collision domain can extend the distance like a bridge does. And what's more, when operating in full-duplex mode, the distance can reach farther than half duplex because it is not limited by the maximum propagation delay time (512 bits time). If fiber media is applied, the distance can be up to tens of kilometers.

Traffic Aggregation:

Traffic aggregation is to aggregate the bandwidth of more than one port and treat it as a single port in the LAN. This single port possesses the features of a normal port but loading balance. This is a great feature for the port needing more bandwidth but cannot afford paying much cost for high bandwidth port.

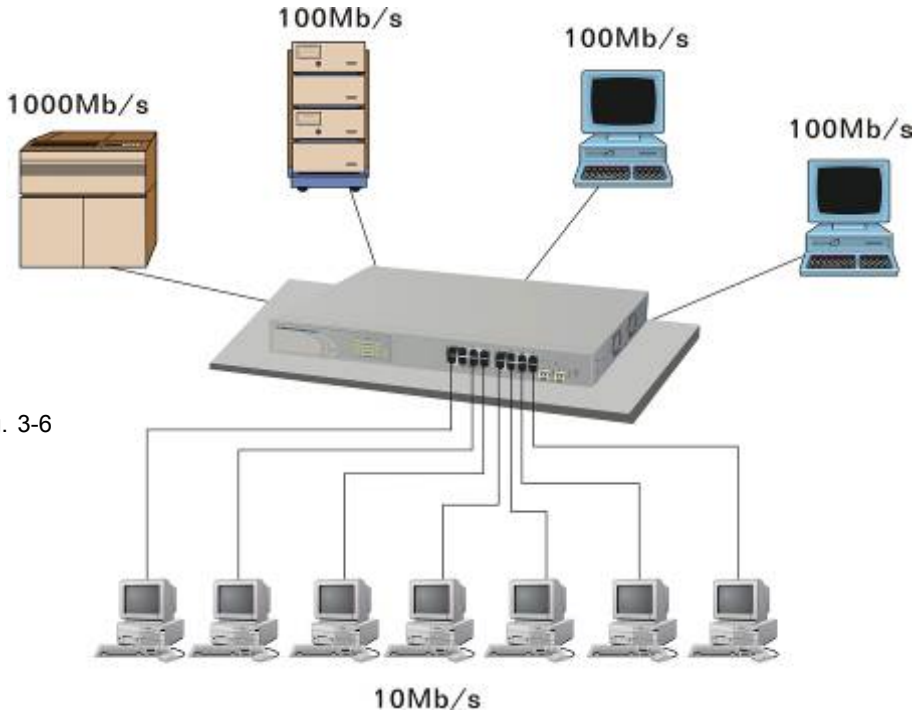


Fig. 3-6

How does a switch operate?

A Layer 2 switch uses some features of the Data Link layer in OSI model to forward the packet to the destination port(s). Here we introduce some important features of a switch and how they work.

MAC address table

When a packet is received on a port of switch, the switch first checks if the packet good or bad and extracts the source MAC address (SA) and destination MAC address (DA) to find 1) if SA is existed in the MAC address table, if no, puts it in the MAC address table, if yes, 2) looks up DA and its associated port to which the traffic is forwarded. If DA does not exist, have the packet broadcasted.

Due to the size of the MAC address limited, MAC address aging function is applied. When the MAC address has resided and keeps no update in the table for a long time, this means the traffic using that entry has yet come for a while. If this time period is more than the aging time, the entry will be marked invalid. The vacancy is now available for other new MAC.

Both learning and forwarding are the most important functions in a switch. Besides that, VLAN can be one of the rules to forward the packet. There are ingress rule and egress rule applied. The ingress rule is used to filter the incoming packet by VLAN ID and so on and to decide whether the packet is allowed to enter the switch or not. The egress rule is used to forward the packet to the proper port.

Mac address aging

There is a field in MAC address table used to put the entry's Age time which determines how long a MAC entry can reside in a switch. The age time is refreshed when a packet with that SA. Usually, the age time is programmable.

Transmission schedule

In most layer 2 switches, the QoS is supported. QoS in a switch must associate a transmission schedule to transmit the packet. This function is much to do with the priority level a packet has. With the given priority, the scheduler will do the proper action on it. The scheduler has many ways to implement, and different chips may support different schedule algorithms. Most common schedulers are:

FCFS: First Come First Service.

Strictly Priority: All High before Low.

Weighted Round Robin:

Set a weight figure to the packet with a priority level, say 5-7, and next, set another weight to the packet with a priority level, say 2-4 and so on. The WRR will transmit the packet with the weight. So the packet of each priority level can be allocated a fixed bandwidth.

Bandwidth rating

Bandwidth rating is the limitation set by administrator, and it can be applied to those with SLA. Bandwidth rating can be total bandwidth, types of service of a port with many steps. The switch supports by-port Ingress and Egress total bandwidth rate control capacity. The bandwidth rate resolution is 0.1 Mbps (100Kbps) and ranges from 0 to 100Mbps.

3-5. Virtual LAN

What is a VLAN?

It is a subset of a LAN. Before we discuss VLAN, we must understand what LAN is. In general, a LAN is composed of different physical network segments bridged by switches or bridges which attach to end stations in the same broadcast domain. The traffic can reach any station on the same LAN. Beyond this domain, the traffic cannot go without router's help. This also implies that a LAN is limited. If you need to communicate with the station outside the LAN, a router is needed which always lies on the edge of the LAN.

For a layer 2 VLAN, it assumes it is a logical subset of a physical LAN separated by specific rules such as tag, port, MAC address and so on. In other words, they can communicate with each other between separated small physical LANs within a LAN but can not be between any two separated logical LANs.

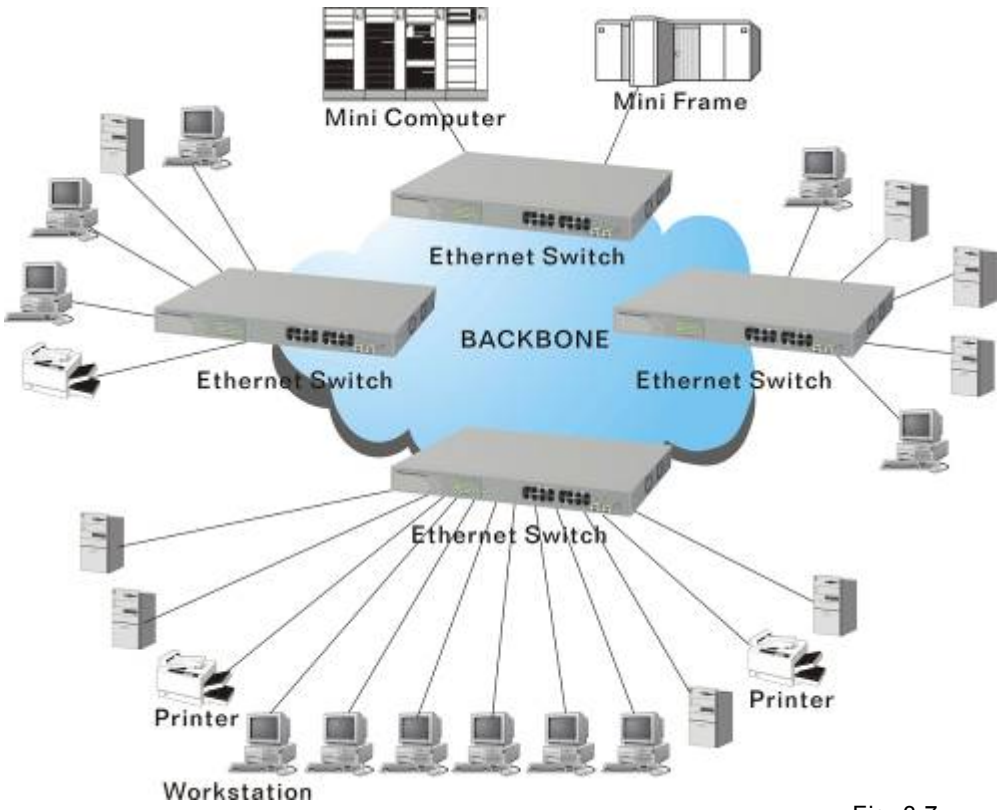


Fig. 3-7

In the figure above, all stations are within the same broadcast domain. For these stations, it is obviously that the traffic is getting congested while adding more stations on it. With the more and more users joining the LAN, broadcast traffic will rapidly decrease the performance of the network. Finally, the network may get down.

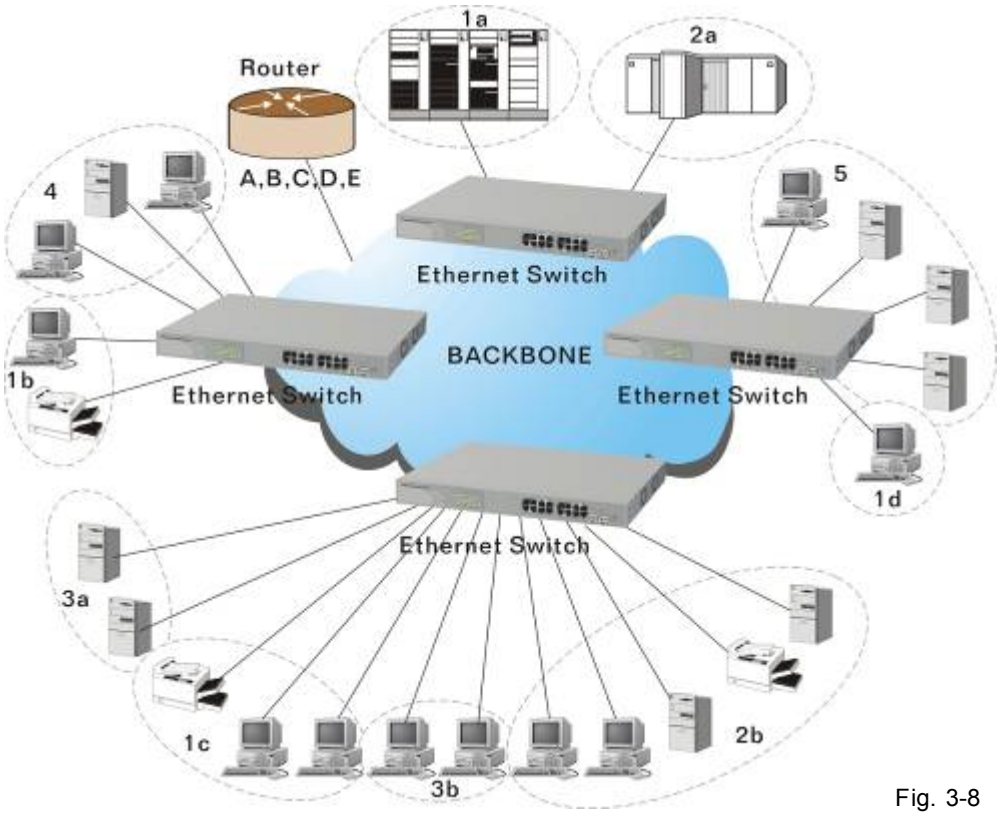


Fig. 3-8

Now we apply VLAN technology to configure the system shown as the figure above. We can partition the users into the different logical networks which have their own broadcast domain. The traffic will not disturb among these logical networks. The users 1x (x denotes a ~ d) are members of VLAN 1. Any traffic within VLAN 1 does not flow to VLAN 2 and others. This helps us configure the network easily according to the criteria needed, for example, financial, accounting, R&D and whatever you think it necessary. You can also easily move a user to a different location or join a new user somewhere in the building to VLAN. Without VLAN, it is very hard to do. Basically, VLAN can afford offering at least 3 benefits: move and change users, reduce broadcast traffic and increase performance, Security.

Besides, VLAN can highly reduce the traffic congestion and increase total performance because there are no more too many users in the same broadcast domain.

There are many types of VLAN applied. Most popular is port-based VLAN, tag-based VLAN and protocol-based VLAN.

- Port-based VLAN

  Some physical ports are configured as members of a VLAN. All stations attached on these ports can communicate with each other.

- Tag-based VLAN

  It identifies the membership by VLAN ID, no matter where the packet comes from. It is also referred to as 802.1Q VLAN.

- Protocol-based VLAN

  It identifies the VLAN membership by layer 3 protocol types, for example IPX, Appletalk, IP, etc.

Other VLAN technologies not mentioned above are MAC-based VLAN, IP-based VLAN and so on.

Terminology

Tagged Frame:

A frame, carrying a tag field following the source MAC address, is four bytes long and contains VLAN protocol ID and tag control information composed of user priority, Canonical Format Indicator (CFI) and optional VLAN identifier (VID). Normally, the maximal length of a tagged frame is 1522 bytes.

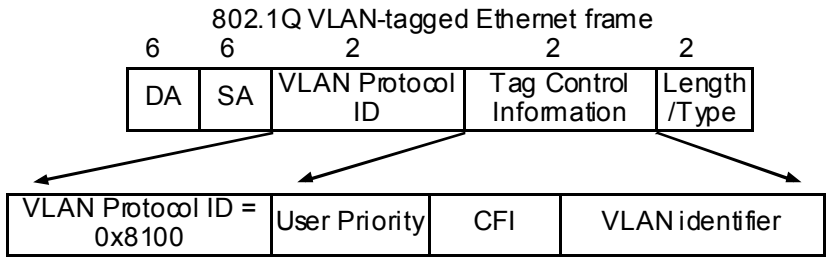


Fig.3-9 Tag Format

VLAN Protocol ID: 8100 is reserved for VLAN-tagged frame.

User Priority: 3 bits long. User priority is defined to 7 – 0. 0 is the lowest priority.

CFI: Canonical Format Indicator. 1 bit long. It is used to encapsulate a token ring packet to let it travel across the Ethernet. Usually, it is set to 0.

VLAN ID: 12 bits long. 0 means no VLAN ID is present. 1 means default VLAN, 4095 reserved.

VLAN-tagged frame:

An Ethernet frame, carrying VLAN tag field, contains VLAN identification without the value of 0 and 4095, and priority information.

Priority-tagged frame:

An Ethernet frame, carrying VLAN tag field, contains VLAN identification with the value of 0 and priority information.

Untagged frame:

An Ethernet frame carries no VLAN tag information.

VLAN Identifier:

Also referred to as VID. It is used to identify a member whether it belongs to the VLAN group with the VID. The assignable number is 1- 4094. If VID=0, the tagged frame is a priority packet. Both the value of 0 and 4095 also cannot be assigned in VLAN management.

Port VLAN Identifier:

VLAN identifier of a port. It also can be referred to as PVID. When an untagged frame or a priority-tagged frame is received, the frame will be inserted the PVID of that port in the VLAN tag field. The frame with VID assigned by a port is called PVID. Each port can only be assigned a PVID. The default value for PVID is 1, the same as VID.

Ingress filtering:

The process to check a received packet and compare its VID to the VLAN membership of the ingress port. The ingress filtering can be set by per port. When receiving a packet, VLAN bridge examines if the VID in the frame's header presents.

If the VID of the received packet presents, the VID of the packet is used. And VLAN bridge will check its MAC address table to see if the destination ports are members of the same VLAN. If both are members of the tagged VLAN, then the packet will be forwarded.

If the packet is an untagged or a null tag packet, the ingress port's PVID is applied to the packet. VLAN bridge will then look up the MAC address table and determine to which ports the packet should be forwarded. Next, it will check to see if the destination ports belong to the same VLAN with that PVID. If the destination ports are members of the VLAN used by ingress port, the packet will be forwarded.

Note: VID can not be 0 or 4095.

Ingress Rule:

Each packet received by a VLAN-aware bridge will be classified to a VLAN. The classification rule is described as follows.

1. If the VID of the packet is null VID (VID=0)or this packet is an untagged packet:
   If there are still some other ways(e.g. protocol, MAC address, application, IP-subnet, etc.) to classify the incoming packets beside port-based classification in implement and these approaches can offer non-zero VID, then, use the value of VID offered by other classifications for VLAN's classification.
   If there is only port-based classification in implement or other classification approaches cannot offer non-zero VID for the incoming packets, then assign the PVID to the incoming packets as VID for the classification of the VLAN group.
2. If the VID is not a null VID (VID≠0), then use the value to classify the VLAN group.

Egress Rule:

An egress list is used to make the tagging and forwarding decision on an outgoing port. It specifies the VLANs whose packets can be transmitted out and specifies if the packet should be tagged or not. It can be configured for port's VLAN membership, and tagged or untagged for a transmitted packet. When a packet is transmitted out, the VLAN bridge checks the port's egress list. If the VLAN of the packet is on the egress list of the port on which the packet transmits out, the packet will be transmitted with the priority accordingly. If enabled, an egress port will transmit out a tagged packet if the port is connected to a 802.1Q-compliant device. If an egress port is connected to a non-802.1Q device or an end station, VLAN bridge must transmit out an untagged packet, i.e. the tag has been stripped off in an egress port. Egress rule can be set by per port.

Independent VLAN Learning (IVL):

It specifies the mode how to learn MAC address. For a specified VLAN, it will use an independent filtering database (FID) to learn or look up the membership information of the VLAN and decide where to go.

Shared VLAN Learning (SVL):

It specifies the mode how to learn MAC address. In this mode, some VLAN or all VLANs use the same filtering database storing the membership information of the VLAN to learn or look up the membership information of the VLAN. In 16 Gigabit Web Smart Switch, you can choose a VID for sharing filtering database in Shared VID field if you wish to use the existed filtering database. For a specified VLAN, when a MAC address is learned by a switch, VLAN will use this formation to make forwarding decision.

Filtering Database:

Referred to as FID. It can provide the information where the packet will be sent to. Filtering database will supply the outgoing port according to the request from forwarding process with VID and DA. When a packet is received, if it has a non-zero VID, then FID will offer the associated outgoing ports information to the packet.

In SVL, VLANs use the same Filtering Database. In IVL, VLANs use different FIDs. Any VID can be assigned to the same FID by administrator.

How does a Tagged VLAN work?

If the ingress filtering is enabled and when a packet is received, VLAN bridge will first check if the VID of the packet presents.

1). If the packet has a non-zero VID, VLAN bridge will apply this VID as the VLAN ID of the packet in the network.

2). For a packet with null tag or no VLAN tag, if VLAN bridge provides rules to decide its VID, then apply this VID to the packet.

If VLAN bridge does not support any rule for VID, then apply the PVID of the port to the packet which came from that port. VLAN bridge checks to see if the ingress port and the received packet are on the same VLAN. If not, drops it. If yes, forwards it to the associated ports. Meanwhile, this VLAN must be applied to the egress port, or the packet will be dropped.

If ingress filtering is disabled, VLAN bridge will only check the MAC address table to see if the destination VLAN exists. If VLAN does not exist, then drop the packet, and if both DA and VLAN do not exist, forwards the packet. If just knows VLAN existed, then floods the packet to all the ports the VLAN covers.

If we plan to deploy four VLANs in an office and use a switch to partition them, we should check which ports belong to which VLAN first. Assuming a 24-port switch is applied.

Name	VID	Port Members
Marketing	2	1,2,3,4,5
Service	3	6,7,20,21,22
Sales	4	8,9,10,11,12,13,14,15,16
Administration	1	17,18,19,23,24

Table 3-6

Next, assigns IP address to each VLAN. Usually, we use 10.x.x.x as internal IP block. Because there are total four VLANs in the network, we must assign 4 IP blocks to each of them.

Name	VID	Network Address
Marketing	2	10.1.2.0/24
Service	3	10.1.3.0/24
Sales	4	10.1.4.0/24
Administration	1	10.1.1.0/24

Table 3-7

Here we apply the subnet mask 255.255.255, and each VLAN is capable of supporting 254 nodes.

3-6. Link Aggregation

Basically, Link Aggregation is to aggregate the bandwidth of more than one port to an assigned logical link. This highly increases total bandwidth to the targeted device. There is more than one Link Aggregation technology in many vendors' switch products already, which may cause the problem of interoperability. This is the reason why now we have 802.3ad Link Aggregation Control Protocol (LACP).

Why 802.3ad (LACP)?

Network is varying. For example, if a port malfunctioned or unplugged accidentally in a static trunk port, administrator has to reconfigure it, or the network will get trouble. Therefore, offering a tool with automatic recovery capability is necessary for an administrator. LACP is a protocol that allows a switch able to know whether its partner has the capability to co-setup a trunk between them.

Usually, if administrator wishes to increase the bandwidth of a specific link, he may:

Buy new network equipments with higher throughput, or

2. Aggregate the bandwidth of more than one port to a logical link.

If the item 1 is the case, you will pay much more cost beyond your budget, and the solution caused by the limitation of hardware performance may not be scalable.

If the item 2 is the case, now you do not have to pay much more extra cost and can keep flexible according to the demand of bandwidth because all equipments are there already. And what's more, you can avoid worrying about the interoperability issue. Applying LACP in your network, you will not only gain benefits below to improve the performance of your network but also have these investments usable to future new products.

Public standardized specification
No interoperability issue
No change to IEEE 802.3 frame format, no change in software and management.
Increased bandwidth and availability
Load sharing and redundancy
Automatic configuration
Rapid configuration and reconfiguration
Deterministic behavior
Low risk of duplication or mis-ordering
Support existing IEEE 802.3 MAC Clients
Backwards compatibility with aggregation-unaware devices

There are also some constraints when applying LACP.

LACP does not support inter-switch bandwidth aggregation.
The ports aggregated must operate in full-duplex mode.
The ports in the same Link Aggregation Group must have the same speed, for example, all with 100Mbps or all 1000Mbps. You cannot aggregate a 1000Mbps and two 100Mbps for a 1.2Gbps trunk port.

Terminology

Link Aggregation:

It is a method to have multiple physical links with the same media and speed bundled to be a logical link forming a Link Aggregation Group with a group ID. With the viewpoint of MAC client, each Link Aggregation Group is an independent link.

There are three cases of link used in the network, which are switch to switch, switch to station and station to station. Here station may be a host or a router.

Link Aggregation, called port trunking sometimes, has two types of link configuration, including static port trunk and dynamic port trunk.

- Static Port Trunk:

  When physical links are changed, administrator needs to manually configure the switches one by one.

- Dynamic Port Trunk:

  When physical links are changed, LACP takes over and automatically reconfigure. Administrator does not have to do anything and may see the trap message of LACP changed in NMS.

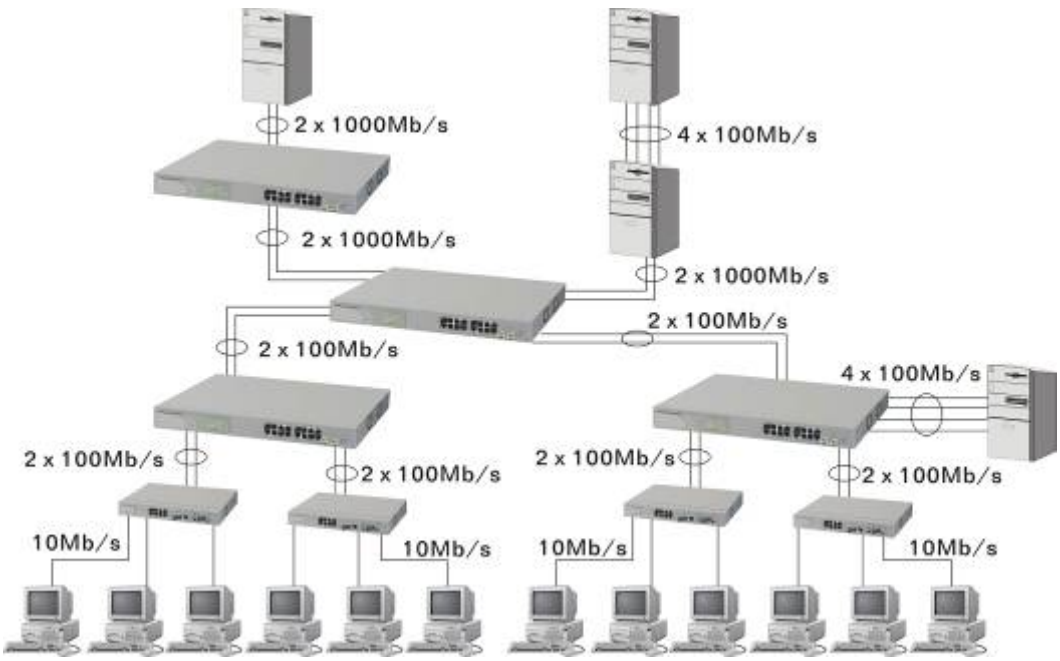


Fig. 3-10 Example of Link Aggregation Application

4. Operation of Web-based Management

This chapter instructs you how to configure and manage the 16 Gigabit Web Smart Switch through the web user interface it supports, to access and manage 14 10/100/1000Mbps TP Port and 2 Gigabit TP/SFP Fiber dual media port. The switch provides 14 fixed Gigabit Ethernet TP ports and 2 optional Gigabit dual media ports supporting either fiber or TP media. With this facility, you can easily access and monitor through any one port of the switch all the status of the switch, including MIBs status, each port activity, multicast traffic, and so on.

The default values of 16 Gigabit Web Smart Switch are listed in the table below:

IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.254
Password	admin

Table 4-1

After the 16 Gigabit Web Smart Switch has been finished configuration, you can browse it by using the IP address you set up. For instance, type http://192.168.1.1 in the address row in a browser, it will show the following screen (see Fig.4-1) and ask you inputting password in order to login and access authentication. The default password is “admin”. For the first time to use, please enter the default password, then click the **<Apply>** button. The login process now is completed.

In the switch, it supports a simple user management function allowing only one administrator to configure the system at the same time.

To optimize the display effect, we recommend you use Microsoft IE and have the resolution 1024x768.

Here is the whole function tree with web user interface and we will travel it through this chapter.

Fig. 4-1

4-1. Web Management Home Overview

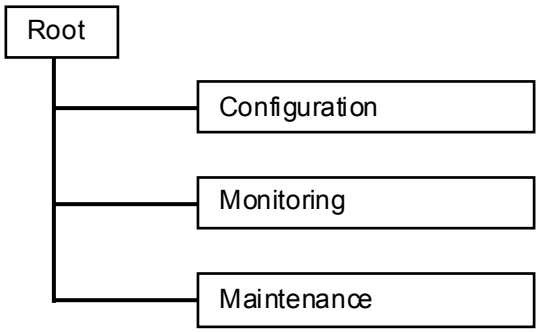
After you login, the switch shows you the system status information as Fig. 4-2. This page is default and tells you the basic information of the system, including “Switch Status”, “TP Port Status”, “Fiber Port Status”, “Aggregation”, “VLAN”, “Mirror”, “Trap Event”, and “Maximum Packet Length”. With this information, you will know the software version used, MAC address, how many ports good and so on. This is helpful while malfunctioning. For more details, please refer to Section 4-4-1.

Fig. 4-2

- **The Information of Page Layout**

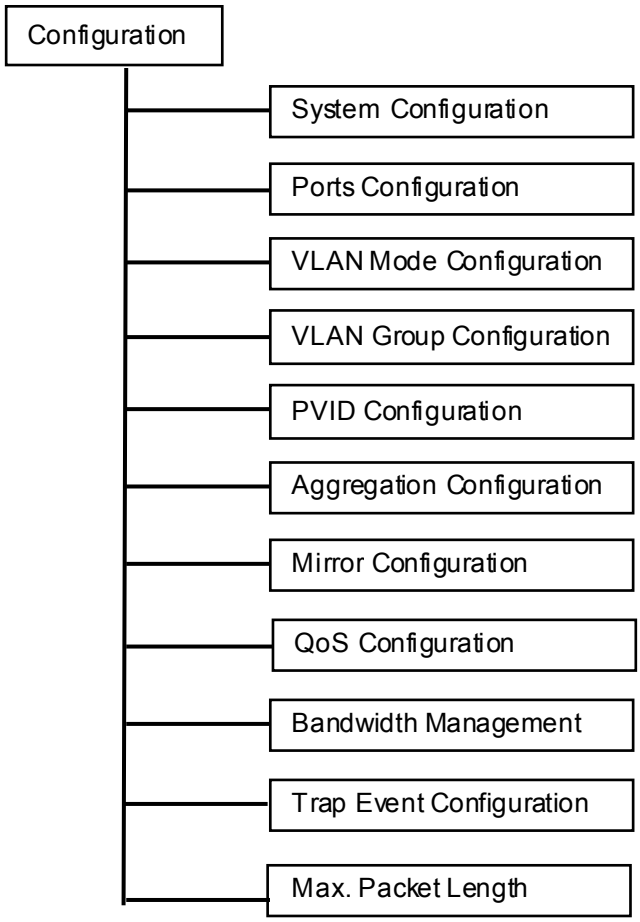
  On the top side, it shows the front panel of the switch. In the front panel, the linked ports will display green; as to the ports, which are link off, they will be dark. For the optional modules, the slot will show only a cover plate if no module exists and will show a module if a module is present. The image of module depends on the one you inserted. The same, if disconnected, the port will show just dark, if linked, green.

  On the left side, the main menu tree for web is listed in the page. According to the function name in boldface, all functions can be divided into three parts, including "Configuration", "Monitoring" and "Maintenance". The functions of each folder are described in its corresponded section respectively. As to the function names in normal type are the sub-functions. When clicking it, the function is performed. The following list is the main function tree for web user interface.



4-2. Configuration

Eleven functions, including System Configuration, Ports Configuration, VLAN Mode Configuration, VLAN Group Configuration, PVID Configuration, Aggregation Configuration, Mirror Configuration, QoS Configuration, Bandwidth Management, Trap Event Configuration and Max. Packet Length are contained in this function folder for system and network management. Each of them will be described in detail orderly in the following sections.



4-2-1. System Configuration

System configuration is one of the most important configurations in the switch. Without the proper setting, network manager will not be able to manage or view the device. The switch supports manual IP address setting. When IP address is changed, you must reboot the switch to have the setting taken effect and use the new IP to browse for web management.

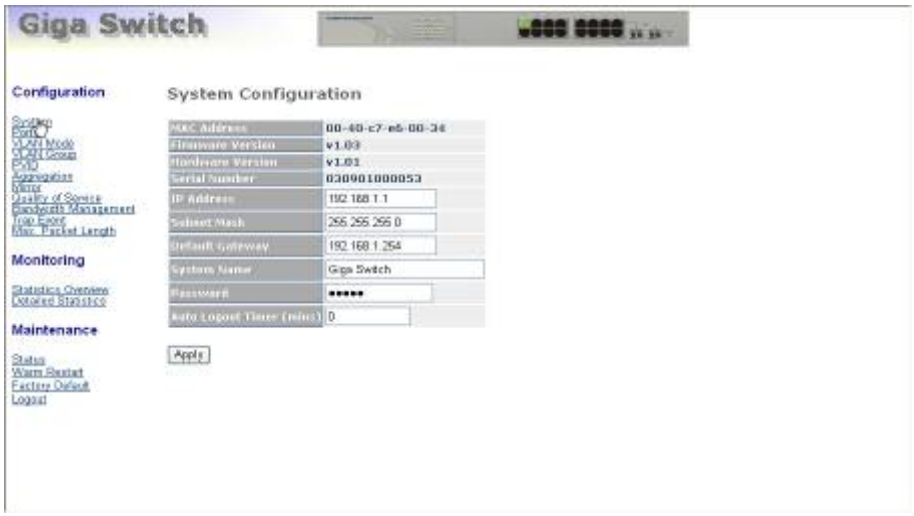


Fig. 4-3

Function name:

System Configuration

Function description:

Set IP address, subnet mask, default gateway, system name, password and auto logout timer for the switch.

Parameter description:

MAC Address:

It is the Ethernet MAC address of the management agent in this switch.

Firmware Version:

The firmware version of this switch.

Hardware Version:

The hardware version of this switch.

Serial Number:

The serial number is assigned by the manufacturer.

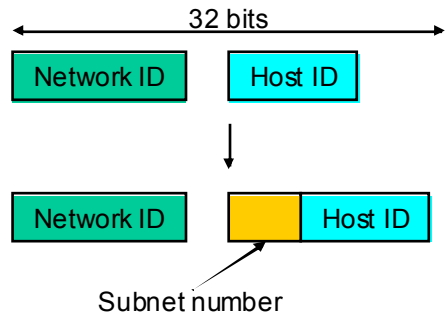
IP Address:

Users can configure the IP settings and fill in new values. Then, click **<Apply>** button to update.

Default: 192.168.1.1

Subnet Mask:

Subnet mask is made for the purpose to get more network address because any IP device in a network must own its IP address, composed of Network address and Host address, otherwise can't communicate with other devices each other. But unfortunately, the network classes A, B, and C are all too large to fit for almost all networks, hence, subnet mask is introduced to solve this problem. Subnet mask uses some bits from host address and makes an IP address looked Network address, Subnet mask number and host address. It is shown in the following figure. This reduces the total IP number of a network able to support, by the amount of 2 power of the bit number of subnet number (2^(bit number of subnet number)).



Subnet mask is used to set the subnet mask value, which should be the same value as that of the other devices resided in the same network it attaches.

For more information, please also see the Section 2-1-4 "IP Address Assignment" in this manual.

Default: 255.255.255.0

Default Gateway:

Set an IP address for a gateway to handle those packets that do not meet the routing rules predefined in the device. If a packet does not meet the criteria for other pre-defined path, it must be forwarded to a default router on a default path. This means any packet with undefined IP address in the routing table will be sent to this device unconditionally.

Default: 192.168.1.254

System Name:

Set a special name for this switch. Up to 16 characters are allowed in this parameter. Any alphanumeric character and null are acceptable.

Default: Giga Switch

Password:

Set a password for this switch. Up to 16 characters are allowed in this parameter. Any alphanumeric character is acceptable.

Default: admin

Auto Logout Timer:

Set the auto-logout timer. The valid value is 0 ~ 60 in the unit of minute and a decimal point is not allowed. The value 0 means auto-logout timer is disabled.

Default: 0

4-2-2. Ports Configuration

Function name:

Ports Configuration

Function description:

Ports Configuration is applied to change the setting of each port. In this configuration function, you can set/reset the following parameters, Mode and Flow Control. All of them are described in detail below.

Parameter description:

Mode:

Set the speed and duplex of the port. If the media is 1Gbps fiber, there are three modes to choose: Auto Speed, 1000 Full and Disable. If the media is TP, the Speed/Duplex is comprised of the combination of speed mode, 10/100/1000Mbps, and duplex mode, full duplex and half duplex. The following table summarized the function the media supports.

Media type	NWay	Speed	Duplex
1000M TP	ON/OFF	10/100/1000M	Full for all, Half for 10/100
1000M Fiber	ON/OFF	1000M	Full

In Auto Speed mode, no default value. In Forced mode, default value depends on your setting.

Flow Control:

There are two modes to choose in flow control, including Enable and Disable. If flow control is set Enable, both parties can send PAUSE frame to the transmitting device(s) if the receiving port is too busy to handle. When it is set Disable, there will be no flow control in the port. It drops the packet if too much to handle. Default: Enable

Fig. 4-4

4-2-3. VLAN Mode Configuration

The switch supports Port-based VLAN and Tag-based VLAN (802.1q). Support 16 active VLANs and VLAN ID 1~4094. VLAN configuration is used to partition your LAN into small ones as your demand. Properly configuring it, you can gain not only improving security and increasing performance but greatly reducing VLAN management.

Function name:

VLAN Mode Setting

Function description:

The VLAN Mode Selection function includes four modes: Port-based, Tag-based, Metro mode or Disable, you can choose one of them by pulling down list and pressing the **<Downward>** arrow key. Then, dick **<Apply>** button, the settings will take affect immediately.

Parameter description:

VLAN Mode:

Disable:

Stop VLAN function on the switch. In this mode, no VLAN is applied to the switch. This is the default setting.

Port-based:

Port-based VLAN is defined by port. Any packet coming in or outgoing from any one port of a port-based VLAN will be accepted. No filtering criterion applies in port-based VLAN. The only criterion is the physical port you connect to. For example, for a port-based VLAN named PVLAN-1 contains port members Port 1&2&3&4. If you are on the port 1, you can communicate with port 2&3&4. If you are on the port 5, then you cannot talk to them. Each port-based VLAN you built up must be assigned a group name. This switch can support up to maximal 16 port-based VLAN groups.

Tag-based:

Tag-based VLAN identifies its member by VID. This is quite different from port-based VLAN. If there are any more rules in ingress filtering list or egress filtering list, the packet will be screened with more filtering criteria to determine if it can be forwarded. The switch supports supplement of 802.1q. For more details, please see the section VLAN in Chapter 3.

Each tag-based VLAN you built up must be assigned VLAN name and VLAN ID. Valid VLAN ID is 1-4094. User can create total up to 16 Tag VLAN groups.

Metro Mode:

The Metro Mode is a quick configuration VLAN environment method on Port-based VLAN. It will create 14 or 15 Port-based VLAN groups.

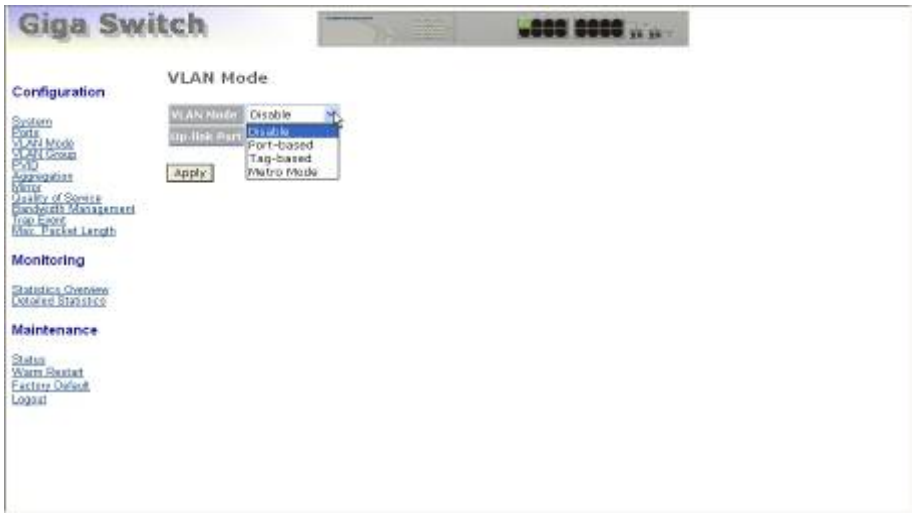


Fig. 4-5

Up-link Port:

This function is enabled only when metro mode is chosen in VLAN mode.

15:

Except Port 15, each port of the switch cannot transmit packets with each other. Each port groups a VLAN with Port 15, thus, total 15 groups consisting of 2 members are formed.

16:

Except Port 16, each port of the switch cannot transmit packets with each other. Each port groups a VLAN with Port 16, thus, total 15 groups consisting of 2 members are formed.

15&16:

Except Port 15 and Port 16, each port of the switch cannot transmit packets with each other. Each port groups a VLAN with Port 15 and Port 16, thus, total 14 groups consisting of 3 members are formed.

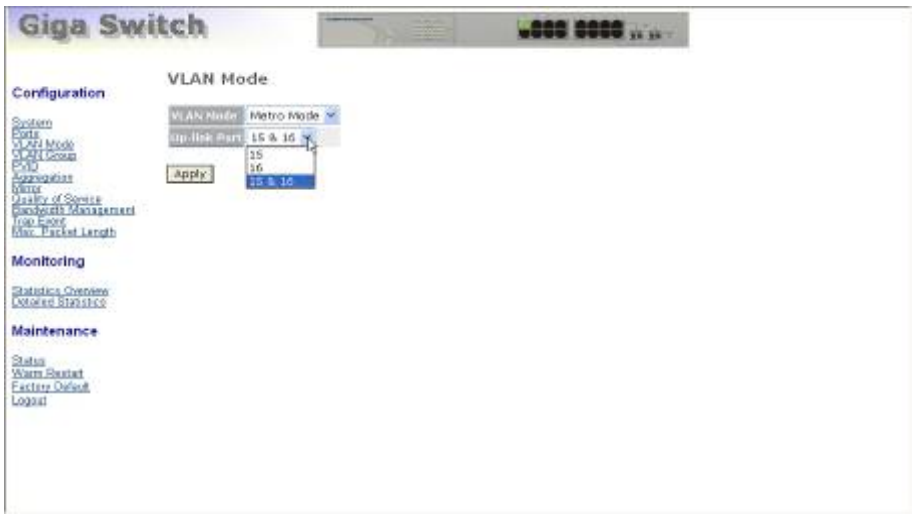


Fig. 4-6

4-2-4. VLAN Group Configuration

Function name:

VLAN Group Configuration

Function description:

It shows the existed information of VLAN Groups List and maintains them, i.e. modify and delete one of them. User also can add a new VLAN group by inputting a new VLAN name and VLAN ID.

If you are in port-based VLAN, it will just show the ID、Description、Member of the existed port-based VLAN group. If you are in tag-based VLAN, it will show the ID、Description、VID、Member of the existed tag-based VLAN group. The switch cannot store the configuration of port-based VLAN and tag-based VLAN separately. When you choose one of VLAN mode, the switch will bring you the responded VLAN configuration which keeps the default data. You can easily create and delete a VLAN group by pressing **<Add Group>** and **<Delete Group>** function buttons, or click the Group ID directly to edit it.

Parameter description:

ID (Group ID):

When you want to edit a VLAN group, you must select the Group ID field. Then, you will enter Tag Base VLAN Group Setting or Port Base VLAN Group Setting page, which depends on your VLAN mode selection.

Description:

The description defined by administrator is associated with a VLAN group.

VID:

VLAN identifier. Each tag-based VLAN group has a unique VID. It appears only in tag-based mode.

Member:

This is used to enable or disable if a port is a member of the new added VLAN, “Enable” means it is a member of the VLAN. Just tick the check box (☑) beside the port x to enable it.

Fig. 4-7

Add Group:

Create a new port-based VLAN or tag-based VLAN, which depends on the VLAN mode you choose in VLAN mode function.

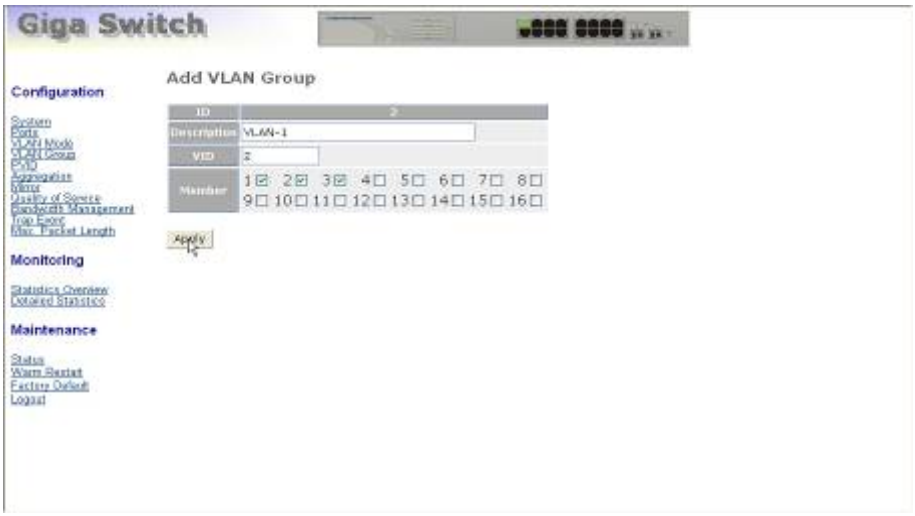


Fig. 4-8

Delete Group:

Just tick the check box (☑) beside the ID, then press the **<Delete Group>** button to delete the group.

Fig. 4-9

4-2-5. PVID Configuration

Function name:

PVID Configuration

Function description:

In VLAN Port VID Setting, user can input VID number to each port. The range of VID number is from 1 to 4094. User also can choose ingress filtering rules to each port. There are two ingress filtering rules which can be applied to the switch. The Ingress Filtering Rule 1 is "forward only packets with VID matching this port's configured VID". The Ingress Filtering Rule 2 is "drop untagged frame".

Parameter description:

Port 1-16:

Port number.

PVID:

This PVID range will be 1-4094. Before you set a number x as PVID, you have to create a Tag-based VLAN with VID x. For example, if port x receives an untagged packet, the switch will apply the PVID (assume as VID y) of port x to tag this packet, the packet then will be forwarded as the tagged packet with VID y.

Rule 1:

Forward only packets with VID matching this port's configured VID. You can apply Rule 1 as a way to a given port to filter unwanted traffic. In Rule 1, a given port checks if the given port is a member of the VLAN on which the received packet belongs to, to determine forward it or not. For example, if port 1 receives a tagged packet with VID=100 (VLAN name=VLAN100), and if Rule 1 is enabled, the switch will check if port 1 is a member of VLAN100. If yes, the received packet is forwarded; otherwise, the received packet is dropped.

Rule 2:

Drop untagged frame. You can configure a given port to accept all frames (Tagged and Untagged) or just receive tagged frame. If the former is the case, then the packets with tagged or untagged will be processed. If the later is the case, only the packets carrying VLAN tag will be processed, the rest packets will be discarded.

Note: If Rule 1 is enabled and port 1, for example, receives an untagged packet, the switch will apply the PVID of port 1 to tag this packet, the packet then will be forwarded. But if the PVID of port 1 is not 100, the packet will be dropped.

Tag:

This is an egress rule of the port. Here you can choose untag or tag. Tag means the outgoing packets must carry VLAN tag header, just tick the check box (☑). Untag means the outgoing packets carry no VLAN tag header.

Untag State:

If you checked this function for a Tag out port, the packet form this port may be tag out. But, the packet would be untag out if the VID of its tag is the same as the value of ”Untag VID” while Untag VID state is Enable.

Untag VID:

Valid range is 0~4094.

Fig. 4-10

4-2-6. Aggregation Configuration

The Aggregation (Port Trunking) Configuration is used to configure the settings of Link Aggregation. You can bundle more than one port with the same speed, full duplex and the same MAC to be a single logical port, thus the logical port aggregates the bandwidth of these ports. This means you can apply your current Ethernet equipments to build the bandwidth aggregation. For example, if there are three Fast Ethernet ports aggregated in a logical port, then this logical port has bandwidth three times as high as a single Fast Ethernet port has.

Function name:

Aggregation Configuration

Function description:

Display the current setup of Aggregation Trunking. With this function, user is allowed to add a new trunking group or modify the members of an existed trunking group.

Parameter description:

Normal:

Set up the ports that do not join any aggregation trunking group.

Group 1~8:

Group the ports you choose together. Up to 8 ports can be selected for each group.

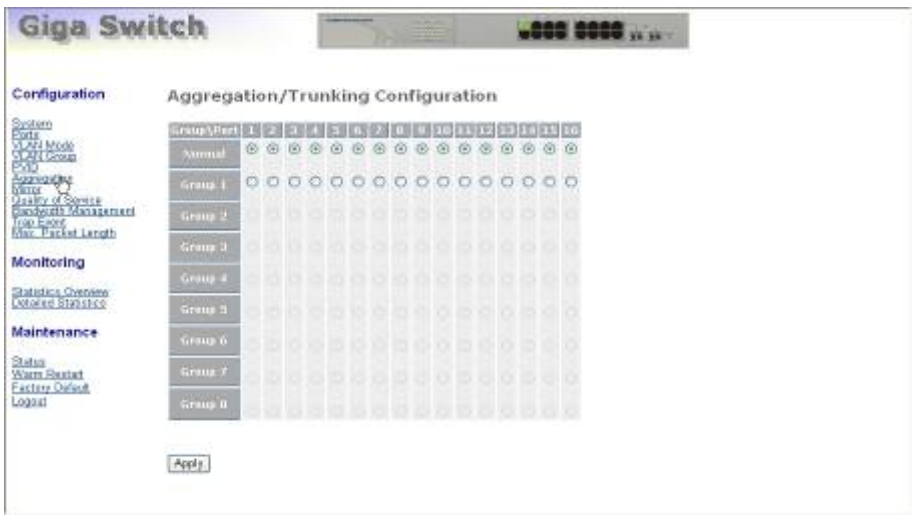


Fig. 4-11

4-2-7. Mirror Configuration

Function name:

Mirror Configuration

Function description:

Mirror Configuration is to monitor the traffic of the network. For example, we assume that Port A and Port B are Sniffer Port and Source Port respectively, thus, the traffic passed by Port B will be copied to Port A for monitoring.

Parameter description:

Sniffer Mode:

Used for the activation or de-activation of Port Mirror function. Default is disable.

Sniffer Port:

Set up the port for monitoring. Valid port is Port 1~16 and default is Port 1.

Source Port:

Set up the port for being monitored. Just tick the check box (☑) under the port x and valid port is Port 1~16.

Fig. 4-12

4-2-8. Quality of Service Configuration

The switch offers powerful QoS function. This function supports VLAN-tagged priority that can make precedence of 8 priorities, TOS field of IP header (equal DSCP High 3 bits) on Layer 3 of network framework, 6 kinds of special network transmission events on Layer 4 and IP DiffServe QoS service.

In Quality of Service (QoS) Configuration, there is one option named" Default Class". As you had selected one of the four QoS functions, then some packets that did not belong to this QoS would be viewed as Default Class. For instance, if you set QoS function as VLAN Tag Priority mode, and then choose Default Class as High, finally, the priority of the packets with no tag will be considered as High priority precedence. The initial value of the Default Class is High.

Fig. 4-13

Function name:

VLAN Tag Priority

Function description:

In vlan tag, there are 3 bits belonging to priority. According to these 3 bits, we could arrange 8 traffics –0 0 0, 0 0 1, 0 1 0, 0 1 0, 1 0 0, 1 0 1, 1 1 0, 1 1 1. We can set High priority or Low priority for each traffic class. For instance, if we let VLAN-tagged priority 0 0 0 be high priority and VLAN-tagged priority 0 0 1 be Low Priority, and then make port 1, 2, 3 be in the vlan 2. We sent in the packets that have vlan-tagged Field appears 0 0 0 and VID equals 2 from the port 2 and the packets that have vlan-tagged Field appears 0 0 1 and VID equals 2 from the port 3. We let the two kinds of packets be transmitted for port 1 until the port results in congestion. The result is that the packets will be dropped partially from the port 3 because the packets that belong to Low Priority. For the use of VLAN Tag Priority function, please press Configure at the right section for setting in advance.

In L4 QoS Configuration, you can enter one of these special network transmission events, for example we use" Down prioritize web browsing, e-mail, FTP and news "L4 QoS Configuration and click apply, and then click Custom L4. We can find Special TCP/UDP port 80,280,443,25,110,20,21,69,119,2009 have already existed and defined for your using but it is fine that you modify this pre-defined TCP/UDP port with other port number you prefer. In " Down prioritize web browsing, e-mail, FTP and news " L4 QoS Configuration with default setting, special defined TCP/UDP port possesses lower QoS traffic than Default class (all other TCP/UDP ports such as port 81,82,83,84,85 etc.). Giving an example, when we transmit TCP packets with port number 80 at each of port 2 and port number 81 at port 3 to port 1 until the congestion happens. The packets from port 3 will be dropped by port 1 because the TCP packets have port number 80 is high priority and will have higher precedence to be sent out from port 1.

Fig. 4-14

Parameter description:

Quality of Service (QoS) Vlan Tag Configuration:

Used for setting up the QoS belongs to Vlan operation.

Port:

User can set up the port (1~16) respectively to let Vlan Tag QoS function work on them. If you would like to set up all ports at a time, user is also allowed to choose "All" in the selection list to simplify the procedure of configuration.

Bit 0, Bit 1, Bit 2:

According to the arrangement of VLAN-tagged priority, it can form 8 kinds of traffics, including 0 0 0, 0 0 1, 0 1 0, 0 1 0, 1 0 0, 1 0 1, 1 1 0 and 1 1 1.

Class:

8 kinds of traffic as mentioned above, user can set up High Priority or Low Priority for each port respectively.

Function name:

IP ToS Classification

Function description:

Another QoS function is the application of Layer 3 on network framework. We focus on TOS field of IP header. There are three bits in TOS field. We means bit 2~4 of TOS field that we will use. According to these 3 bits, we could arrange 8 traffics –0 0 0, 0 0 1, 0 1 0, 0 1 0, 1 0 0, 1 0 1, 1 1 0, 1 1 1. As long as we change bit 5~7 of TOS field of IP header, we will create the 8 traffic packets we meant before. Moreover, we can set High priority or Low priority for each traffic class. For instance, if we let TOS 0 0 0 be high priority and TOS 0 0 1 be Low Priority, we sent in the packets that have bit 5~7 of TOS Field appears 0 0 0 from the port 2 and the packets that have bit 5~7 of TOS Field appears 0 0 1 from the port 3. We let the two kinds of packets be transmitted for port 1 until the port results in congestion. The result is that the packets will be dropped partially from the port 3 because the packets that belong to Low Priority. For the use of TOS Priority function, please press Configure at the right section for setting in advance.

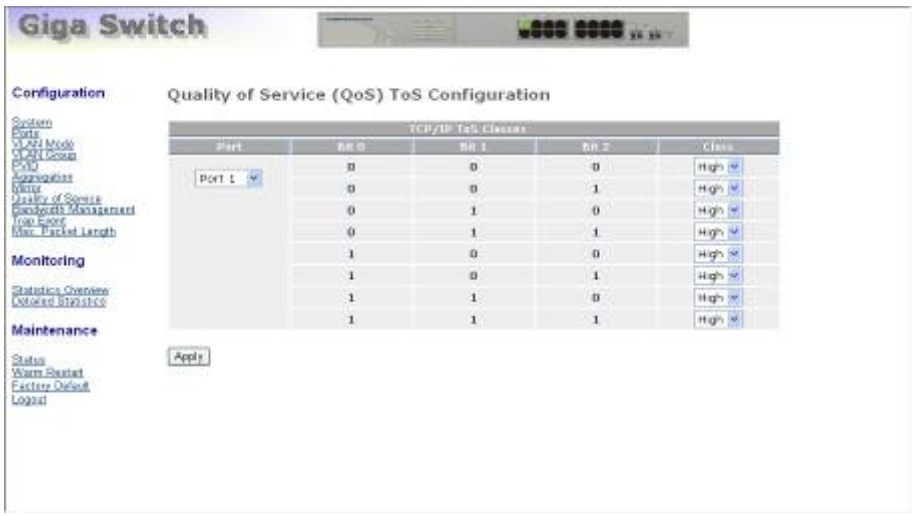


Fig. 4-15

Parameter description:

Quality of Service (QoS) ToS Configuration:

Used for setting up the QoS in Layer 3.

Port:

User can set up the port (1~16) respectively to let TOS QoS function work on them. If you would like to set up all ports at a time, user is also allowed to choose “All” in the selection list to simplify the procedure of configuration.

Bit 0, Bit 1, Bit 2:

According to the arrangement of Bit 5 ~ Bit 7 in TOS Field of IP Header, it can form 8 kinds of traffics, including 0 0 0, 0 0 1, 0 1 0, 0 1 0, 1 0 0, 1 0 1, 1 1 0 and 1 1 1.

Class:

8 kinds of traffic as mentioned above, user can set up High Priority or Low Priority for each port respectively.

Function name:

IP TCP/UDP Port Classification

Function description:

In L4 QoS Configuration, you can enter one of these special network transmission events, for example we use" Down prioritize web browsing, e-mail, FTP and news "L4 QoS Configuration and click apply, and then click Custom L4. We can find Special TCP/UDP port 80,280,443,25,110,20,21,69,119,2009 have already existed and defined for your using but it is fine that you modify this pre-defined TCP/UDP port with other port number you prefer. In " Down prioritize web browsing, e-mail, FTP and news " L4 QoS Configuration with default setting, special defined TCP/UDP port possesses lower QoS traffic than Default class (all other TCP/UDP ports such as port 81,82,83,84,85 etc.). Giving an example, when we transmit TCP packets with port number 80 at each of port 2 and port number 81 at port 3 to port 1 until the congestion happens. The packets from port 3 will be dropped by port 1 because the TCP packets have port number 80 is high priority and will have higher precedence to be sent out from port 1.

Parameter description:

Disable IP TCP/UDP Port Classification:

Belong to the QoS in L4. Just tick the option button and press **<Apply>** button to have this function taken affect. Then, enter Custom L4 to disable IPl TCP/UDP port Classification for QoS.

Down prioritize web browsing, e-mail, FTP and news:

Belong to the QoS in L4. Just tick the option button and press **<Apply>** button to have this function taken affect. Then, enter Custom L4 to set up Special TCP/UDP port for QoS.

Prioritize IP Telephony (VoIP):

Belong to the QoS in L4. Just tick the option button and press **<Apply>** button to have this function taken affect. Then, enter Custom L4 to set up Special TCP/UDP port for QoS.

Prioritize iSCSI:

Belong to the QoS in L4. Just tick the option button and press **<Apply>** button to have this function taken affect. Then, enter Custom L4 to set up Special TCP/UDP port for QoS.

Prioritize web browsing, e-mail, FTP transfers and news:

Belong to the QoS in L4. Just tick the option button and press **<Apply>** button to have this function taken affect. Then, enter Custom L4 to set up Special TCP/UDP port for QoS.

Prioritize Streaming Audio/Video:

Belong to the QoS in L4. Just tick the option button and press **<Apply>** button to have this function taken affect. Then, enter Custom L4 to set up Special TCP/UDP port for QoS.

Prioritize Databases (Oracle, IBM DB2, SQL, Microsoft):

Belong to the QoS in L4. Just tick the option button and press **<Apply>** button to have this function taken affect. Then, enter Custom L4 to set up Special TCP/UDP port for QoS.

Advanced Mode:

Display the TCP/UDP port number in L4 QoS. In "Disable IP TCP/UDP Port Classification" mode, the QoS of L4 is disabled. As to other special L4 QoS events, Special TCP/UDP port number will be took action. Of course, user could be allowed to add or modify the port number at random. For instance, if we choose "Down prioritize web browsing, e-mail, FTP and news" as the QoS of L4 and enter the "Advanced Mode", then we can see that some special port number 80, 280, 443, 25, 110, 20, 21, 69, 119, 2009 have been configured already. User also has the right to modify these port numbers. The display is shown as Fig 4-16.

Special TCP/UDP class:

There are two modes for selection, including Low and High.

Default class (all other TCP/UDP ports):

There are two modes for selection, including Low and High.

Port:

User can set up the port (1~16) respectively to let Special TDP/UDP class function work on them. If you would like to set up all ports at a time, user is allowed to choose "All" selection to simplify the procedure of configuration.

Special UDP/TCP Port Selection:

The following are port numbers defined by six specific networks in L4:

Down prioritize web browsing, e-mail, FTP and news:
port number 80,280,443,25,110,20,21,69,119,2009

Prioritize IP Telephony (VoIP):1718,1719,1720

Prioritize iSCSI:3225,3260,3420

Prioritize web browsing, e-mail, FTP transfers and news:
80,280,443,25,110,20,21,69,119,2009

Prioritize Streaming Audio/Video: 2979,1755,7070,7071,554,8000

Prioritize Databases (Oracle, IBM DB2, SQL,
Microsoft):66,1571,1575,523,118,156,3306,1232,1433,1434

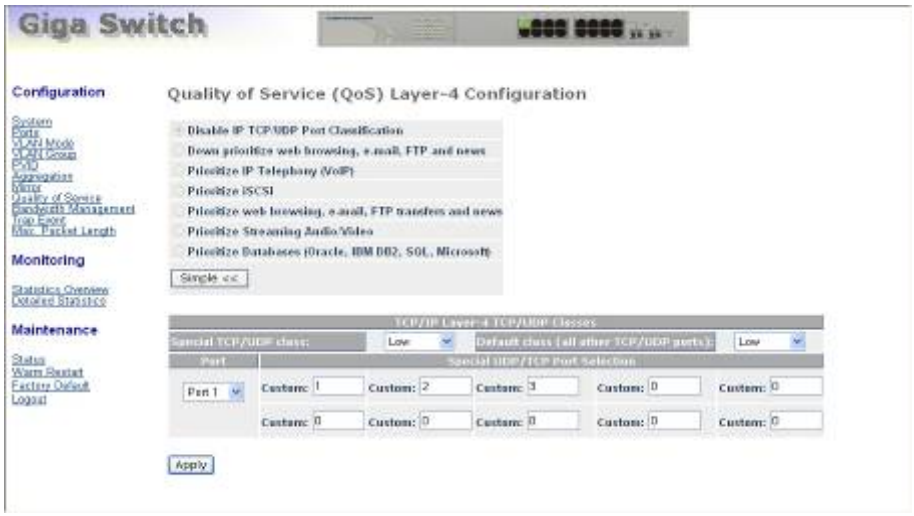


Fig. 4-16 Advanced Mode

Fig. 4-17 Simple Mode

Simple Mode:

Press **<Simple>** button is to return to the screen that all L4 port number will disappear (See Fig 4-17).

Function name:

IP Diffserv Classification

Function description:

IP Diffserve Classification function, it can form total 64 (0~63) kinds of Traffic Class based on the arrangement of 6-bit field in DSCP of the IP packet. In the switch, user is allowed to set up these 64 kinds of Class that belong to High or Low Priority.

Parameter description:

IP Differentiated Services (DiffServ) Configuration:

Used for setting up the IP Differentiated Services Configuration QoS.

Diffserv:

Display 64 (0~63) DiffServ Priority items.

Class:

64 kinds of traffic as mentioned above, user can set up High Priority or Low Priority for each port respectively.

Fig. 4-18

4-2-9. Bandwidth Management

Function name:

Bandwidth Management

Function description:

Bandwidth Management function is used to set up the limit of Ingress and Egress bandwidth for each port.

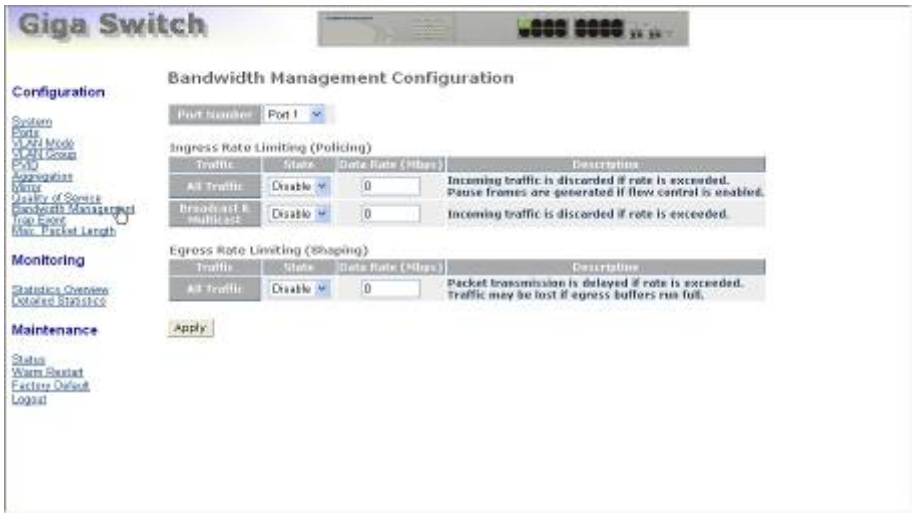


Fig. 4-19

Parameter description:

Port Number:

Choose the port that you would like this function to work on it. Valid range of the port is 1~16. If you would like to set up all ports at a time, user is also allowed to choose “All” in the selection list to simplify the procedure of configuration.

All Traffic for Ingress Rate Limiting:

Set up the limit of Ingress bandwidth for the port you choose. Incoming traffic will be discarded if the rate exceeds the value you set up in Data Rate field. Pause frames are also generated if flow control is enabled. The limited format of the packet includes unicast, broadcast and multicast. Valid range is 0~1000.

Broadcast & Multicasat for Ingress Rate Limiting:

Set up the limit of Ingress bandwidth for the port you choose. Incoming traffic will be discarded if the rate exceeds the value you set up in Data Rate field. The limited format of the packet only includes broadcast and multicast. Valid range is 0~1000.

All Traffic for Egress Rate Limiting:

Set up the limit of Egress bandwidth for the port you choose. Packet transmission will be delayed if the rate exceeds the value you set up in Data Rate field. Traffic may be lost if egress buffers run full. The limited format of the packet includes unicast, broadcast and multicast. Valid range is 0~1000.

4-2-10. Trap Event Configuration

Function name:

Trap Event Configuration

Function description:

The Trap Events Configuration function is used to enable the Advanced Smart Ethernet Switch to send out the trap information while pre-defined trap events occurred.

Switch management offers 7 different trap events and 2 host to users .The message will be sent while users tick (☑) the trap event individually on the web page shown as below. Except Warm Boot and Cold Boot, other trap events offer the counter function to help the user see the times that the trap event had happened.

Parameter description:

These trap functions are as they describe. The traps the switch supports are listed below.

Boot: Warm Boot, Cold Boot

Login: Illegal Login

Link: Link Up, Link Down

Tx/Rx error: Rx error threshold, Tx error threshold

Fig. 4-20

4-2-11. Max. Packet Length

Function name:

Max. Packet Length

Function description:

The switch is capable of dealing with 9k Jumbo Frames, which suits the transmission for a large amount of data in the network environment.

Parameter description:

Max. Frame Size for Jumbo Frame(bytes):

Set up the maximum length of the packet that each port of the switch can accept. Maximum length can be up to 1532 bytes or 9216 bytes. The default is 1518 bytes.

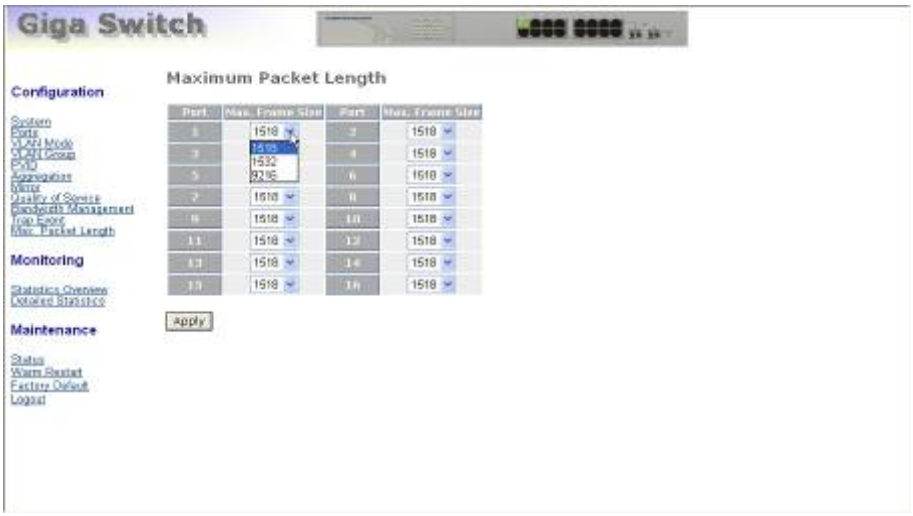
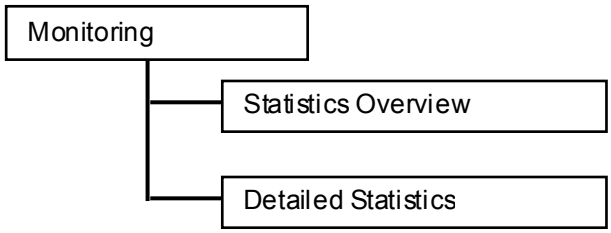


Fig. 4-21

4-3. Monitoring

There are two functions contained in the monitoring function.



4-3-1. Statistics Overview

The function of Statistics Overview collects any information and provides the counting summary about the traffic of the port, no matter the packet is good or bad.

In the Fig. 4-22, the window can show all ports' counter information at the same time. If the counting is overflow, the counter will be reset and restart counting.

Function name:

Statistics Overview

Function description:

Display the summary counting of each port's traffic, including Tx Bytes, Tx Frames, Rx Bytes, Rx Frames, Tx Errors and Rx Errors.

Parameters description:

Tx Bytes:

Total transmitted bytes.

Tx Frames:

The counting number of the packet transmitted.

Rx Bytes:

Total received bytes.

Rx Frames:

The counting number of the packet received.

Tx Errors:

Number of bad packets transmitted.

Rx Errors:

Number of bad packets received.

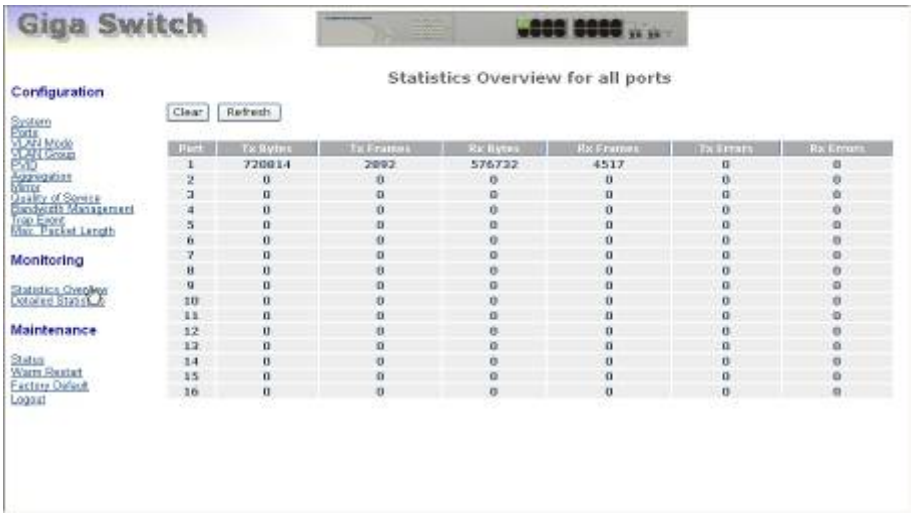


Fig. 4-22

4-3-2. Detailed Statistics

Function name:

Detailed Statistics

Function description:

Display the detailed counting number of each port's traffic. In the Fig. 4-23, the window can show all counter information each port at one time.

Parameter description:

Rx Packets:

The counting number of the packet received.

RX Octets:

Total received bytes.

Rx High Priority Packets:

Number of Rx packets classified as high priority.

Rx Low Priority Packets:

Number of Rx packets classified as low priority.

Rx Broadcast:

Show the counting number of the received broadcast packet.

Rx Multicast:

Show the counting number of the received multicast packet.

Tx Packets:

The counting number of the packet transmitted.

TX Octets:

Total transmitted bytes.

Tx High Priority Packets:

Number of Tx packets classified as high priority.

Tx Low Priority Packets:

Number of Tx packets classified as low priority.

Tx Broadcast:

Show the counting number of the transmitted broadcast packet.

Tx Multicast:

Show the counting number of the transmitted multicast packet.

Rx 64 Bytes:

Number of 64-byte frames in good and bad packets received.

Rx 65-127 Bytes:

Number of 65 ~ 126-byte frames in good and bad packets received.

Rx 128-255 Bytes:

Number of 127 ~ 255-byte frames in good and bad packets received.

Rx 256-511 Bytes:

Number of 256 ~ 511-byte frames in good and bad packets received.

Rx 512-1023 Bytes:

Number of 512 ~ 1023-byte frames in good and bad packets received.

Rx 1024-Bytes:

Number of 1024-max_length-byte frames in good and bad packets received.

Tx 64 Bytes:

Number of 64-byte frames in good and bad packets transmitted.

Tx 65-127 Bytes:

Number of 65 ~ 126-byte frames in good and bad packets transmitted.

Tx 128-255 Bytes:

Number of 127 ~ 255-byte frames in good and bad packets transmitted.

Tx 256-511 Bytes:

Number of 256 ~ 511-byte frames in good and bad packets transmitted.

Tx 512-1023 Bytes:

Number of 512 ~ 1023-byte frames in good and bad packets transmitted.

Tx 1024-Bytes:

Number of 1024-max_length-byte frames in good and bad packets transmitted.

Rx CRC/Alignment:

Number of Alignment errors and CRC error packets received.

Rx Undersize:

Number of short frames (<64 Bytes) with valid CRC.

Rx Oversize:

Number of long frames(according to max_length register) with valid CRC.

Rx Fragments:

Number of short frames (< 64 bytes) with invalid CRC.

Rx Jabber:

Number of long frames(according tomax_length register) with invalid CRC.

Rx Drops:

Frames dropped due to the lack of receiving buffer.

Tx Collisions:

Number of collisions transmitting frames experienced.

Tx Drops:

Number of frames dropped due to excessive collision, late collision, or frame aging.

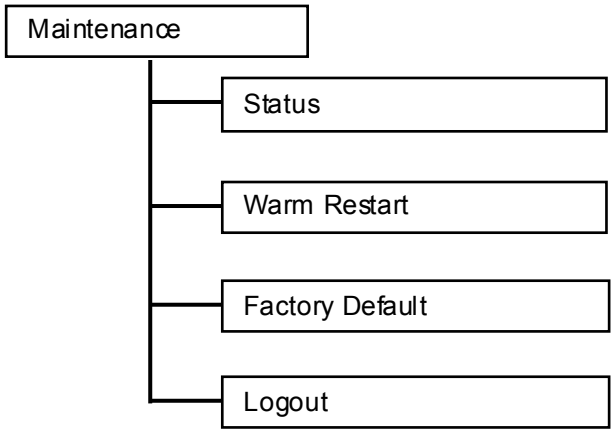
Tx FIFO Drops:

Number of frames dropped due to the lack of transmitting buffer.

Fig. 4-23

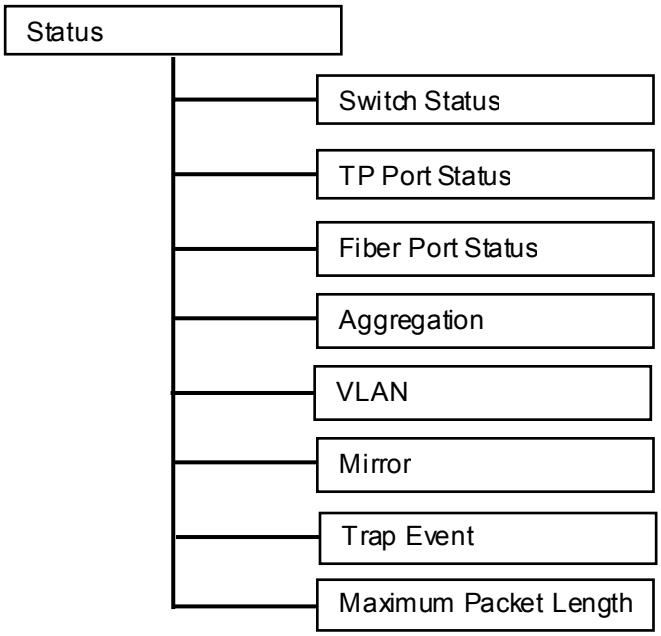
4-4. Maintenance

There are four functions contained in the maintenance function.



4-4-1. Status

Eight functions, including Switch Status, TP Port Status, Fiber Port Status, Aggregation, VLAN, Mirror, Trap Event and Maximum Packet Length are contained in this function folder for port monitor and management. Each of them will be described in detail orderly in the following sections.



4-4-1-1.Switch Status

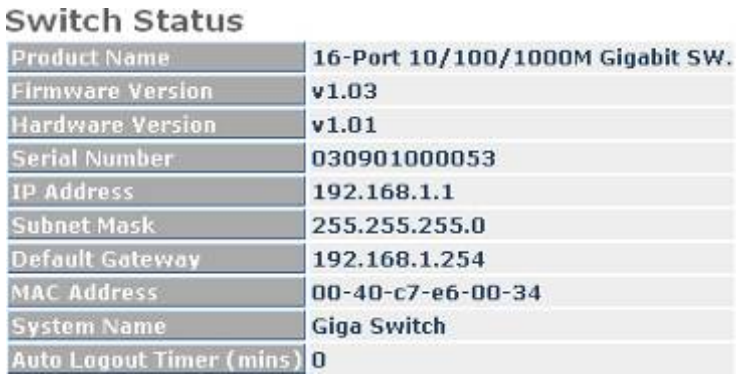


Fig. 4-24

Function name:

Switch Status

Function Description:

Display the status information of this switch.

Parameter Description:

Product Name:

To show the product name of this device.

Firmware Version:

To show the firmware version of this switch.

Hardware Version:

To show the hardware version of this switch.

Serial Number:

The serial number is assigned by the manufacturer.

IP Address:

To show the IP address of this switch.

Subnet Mask:

To show the subnet mask of this switch.

Default Gateway:

To show the default gateway of this switch.

MAC Address:

To show the Ethernet MAC address of this switch.

System Name:

To show the special name for this switch.

Auto Logout Timer:

To show the setting of auto-logout timer in the web UI.

4-4-1-2. TP / Fiber Ports Status

Function name:

TP/Fiber Ports Status

Function description:

TP/Fiber Ports Status function is applied to display the latest updated status of all ports in this switch. In this function, you can view the following setting, link status, speed and flow control. All of them are described in detail below.

TP Port Status

Port	Link Status	Speed	Flow Control	Port	Link Status	Speed	Flow Control
1	100FDX	Auto	Enabled	2	Down	Auto	Enabled
3	Down	Auto	Enabled	4	Down	Auto	Enabled
5	Down	Auto	Enabled	6	Down	Auto	Enabled
7	Down	Auto	Enabled	8	Down	Auto	Enabled
9	Down	Auto	Enabled	10	Down	Auto	Enabled
11	Down	Auto	Enabled	12	Down	Auto	Enabled
13	Down	Auto	Enabled	14	Down	Auto	Enabled
15	Down	Auto	Enabled	16	Down	Auto	Enabled

Fiber Port Status

15	Down	Auto	Enabled	16	Down	Auto	Enabled

Fig. 4-25

Parameter description:

Port:

Display the port number. The number is 1 – 16. Both port 15 and 16 are optional modules.

Link Status:

Show that if the link on the port is active or not. If the link is connected to a working-well device, the Link Status will show the current link speed and duplex. If the connection is broken, it will show “Down”. This is determined by the hardware on both devices of the connection.

No default value.

Speed:

Display the speed and duplex of all port. There are three speeds 10Mbps, 100Mbps and 1000Mbps supported for TP media, and the duplex supported is half duplex and full duplex. If the media is 1Gbps fiber, it is 1000Mbps supported only. The status of speed/duplex mode is determined by 1) the negotiation of both local port and link partner in “Auto Speed” mode or 2) user setting in “Force” mode. The local port has to be preset its capability.

Flow Control:

Show each port's flow control status.

There are two types of flow control in Ethernet, Backpressure for half-duplex operation and Pause flow control (IEEE802.3x) for full-duplex operation. The switch supports both of them.

Default: Enabled

4-4-1-3. Aggregation

Function name:

Aggregation Status

Function description:

Display the current setup of Aggregation Trunking.

Parameter description:

Normal:

Display the ports that do not join any aggregation trunking group.

Group 1~8:

Display the members of the Group.

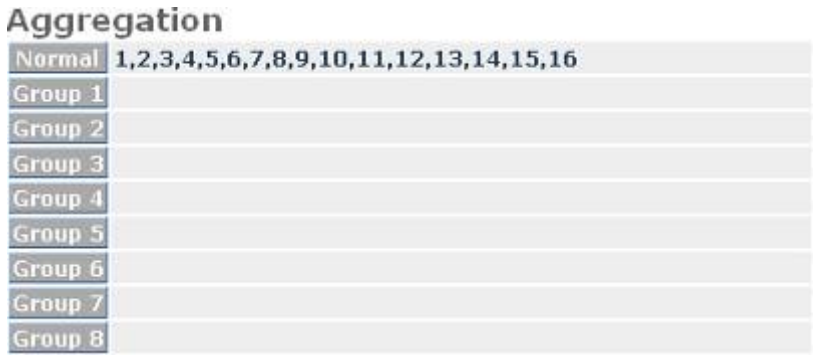


Fig. 4-26

4-4-1-4. VLAN

Function name:

VLAN Status

Function description:

Display the status of VLAN mode and VLAN group setting.

Parameter description:

VLAN Mode:

Display Port-based, Tag-based and metro mode, which depends on the setting in VLAN mode configuration function.

ID:

Display the Group ID.

Description:

Display the description defined by administrator is associated with a VLAN group.

VID:

Display VLAN identifier. Each tag-based VLAN group has a unique VID. It appears only in tag-based mode.

Member:

Display the port members belonging to each VLAN Group.

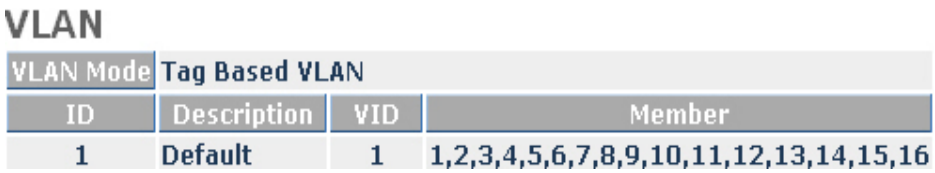


Fig. 4-27 Tag-based VLAN

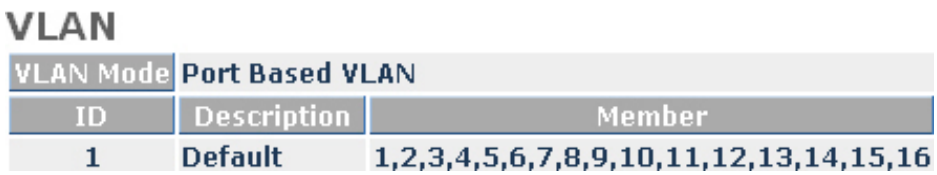


Fig. 4-28 Port-based VLAN

VLAN

VLAN Mode	Metro Mode	
ID	Description	Member
1	Default1	1,15,16
2	Default2	2,15,16
3	Default3	3,15,16
4	Default4	4,15,16
5	Default5	5,15,16
6	Default6	6,15,16
7	Default7	7,15,16
8	Default8	8,15,16
9	Default9	9,15,16
10	Default10	10,15,16
11	Default11	11,15,16
12	Default12	12,15,16
13	Default13	13,15,16
14	Default14	14,15,16

Fig. 4-29 Metro mode VLAN

4-4-1-5. Mirror

Function name:

Mirror Status

Function description:

Mirror Status is to display the setting result of mirror configuration.

Parameter description:

Sniffer Mode:

Display the status the activation or de-activation of Port Mirror function. Default is disable.

Sniffer Port:

Display the port for monitoring. Valid port is Port 1~ 16 and default is Port 1.

Source Port:

Display the port for being monitored. Valid port is Port 1~ 16.

Fig. 4-30

4-4-1-6. Trap Event

Function name:

Trap Event Status

Function description:

The Trap Events status function is used to display the switch's trap information sent out while pre-defined trap events occurred.

Parameter description:

These trap functions are as they describe. The traps that the switch supports are listed below.

Boot: Warm Boot, Cold Boot

Login: Illegal Login

Link: Link Up, Link Down

Tx/Rx error: Rx error threshold, Tx error threshold

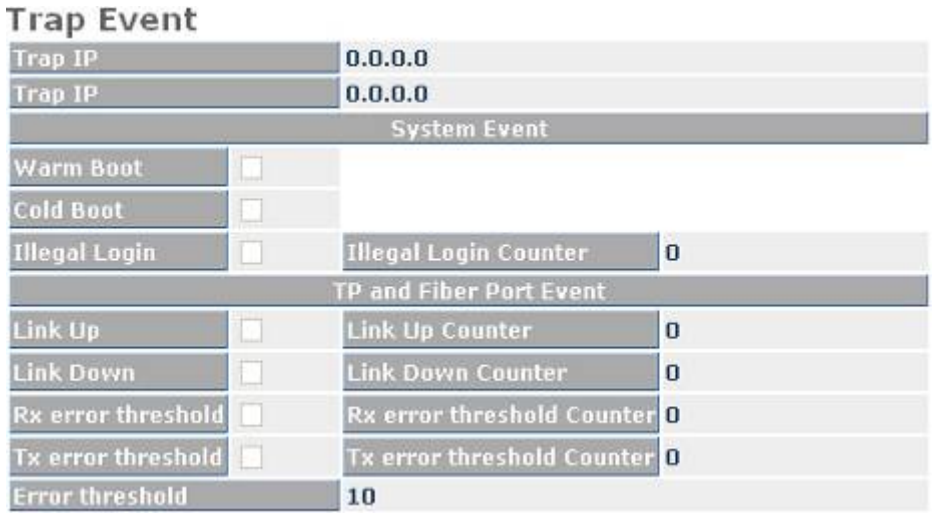


Fig. 4-31

4-4-1-7. Maximum Packet Length

Function name:

Max. Packet Length Status

Function description:

Display the settings of the maximum packet length that each port can accept in this switch.

Parameter description:

Max. Frame Size for Jumbo Frame(bytes):

Display the settings about the maximum length of the packet that each port of the switch can accept. Maximum length can be up to 1532 bytes or 9216 bytes. The default is 1518 bytes.

Maximum Packet Length

Port	Max. Frame Size	Port	Max. Frame Size
1	1518	2	1518
3	1518	4	1518
5	1518	6	1518
7	1518	8	1518
9	1518	10	1518
11	1518	12	1518
13	1518	14	1518
15	1518	16	1518

Fig. 4-32

4-4-2. Warm Restart

We offer you many ways to reboot the switch, including power up, hardware reset and software reset. You can press the RESET button in the front panel to reset the switch and to retrieve default setting. After upgrading software, then you must reboot to have the new configuration taken effect. Here we are discussing is software reset for the “reboot” in the main menu.

Function name:

Warm Restart

Function description:

Reboot the switch. Reboot takes the same effect as the RESET button on the front panel of the switch. Press **<Yes>** button to confirm warm restart function, and it will take around thirty (30) seconds to complete the system boot.

Fig. 4-33

4-4-3. Factory Default

Function name:

Factory Default

Function description:

Factory Default Configuration function can retrieve default setting to replace the working configuration.

Fig. 4-34

4-4-4. Logout

Besides the auto logout function as we mentioned above in the section of system configuration, the switch also allows the user to logout manually by performing the Logout function.

Function name:

Logout

Function description:

The switch allows you to logout the system to prevent other users from the system without the permission. If you do not logout and exit the browser, the switch will automatically have you logout. Besides this manually logout and implicit logout, you can set up the parameter of Auto Logout Timer in system configuration function to explicitly ON/OFF this logout function.

Parameter description:

Auto/Manual Logout:

If no action and no key is stroke as well in any function screen more than the minutes you set up in Auto Logout Timer, the switch will have you logout automatically. Or press the **<Logout>** button in Logout function to exit the system manually.

Fig. 4-35

5. Maintenance

5-1. Resolving No Link Condition

The possible causes for a no link LED status are as follows:

The attached device is not powered on
The cable may not be the correct type or is faulty
The installed building premise cable is faulty
The port may be faulty

5-2. Q&A

1. Computer A can connect to Computer B, but cannot connect to Computer C through the 16 Gigabit Web Smart Switch.

The network device of Computer C may fail to work. Please check the link/act status of Computer C on the LED indicator. Try another network device on this connection.

The network configuration of Computer C may be something wrong. Please verify the network configuration on Computer C.

2. The uplink connection function fails to work.

The connection ports on another must be connection ports. Please check if connection ports are used on that 16 Gigabit Web Smart Switch.

Please check the uplink setup of the 16 Gigabit Web Smart Switch to verify the uplink function is enabled.

3. The console interface cannot appear on the console port connection.

16 Gigabit Web Smart Switch has no console port, so you cannot use console interface to connect with 16 Gigabit Web Smart Switch.

4. How to configure the 16 Gigabit Web Smart Switch.

User can use IE browser program in window series of computer to control the web smart functions in 16 Gigabit Web Smart Switch. First, choose any port in 16 Gigabit Web Smart Switch. Then, use IE and type default IP address, 192.168.1.1, to connect to 16 Gigabit with RJ45 network line. Finally, the login screen will appear at once.

Appendix A
Technical Specifications

Features

14 (10/100/1000Mbps) Gigabit Ethernet (TP) switching ports are compliant with IEEE802.3, 802.3u, 802.3z and 802.3ab.
2 Gigabit TP/SFP fiber are dual media ports with auto detected function.
Non-blocking store-and-forward shared-memory Web-Smart switched.
Supports auto-negotiation for configuring speed, duplex mode.
Supports 802.3x flow control for full-duplex ports.
Supports collision-based and carrier-based backpressure for half-duplex ports.
Any ports can be in disable mode, force mode or auto-polling mode.
Supports Head of Line (HOL) blocking prevention.
Supports broadcast storm filtering.
Web-based management provides the ability to completely manage the switch from any web browser.
Supports Port-based VLAN and Protocol-based (IEEE802.1Q) VLAN.
Auto-aging with programmable inter-age time.
Supports 802.1p Class of Service with 2-level priority queuing.
Supports port trunking with flexible load distribution and failover function.
Supports port sniffer function
Programmable maximum Ethernet frame length of range from 1518 to 9216 bytes jumbo frame.
Supports port-based VLAN, 802.1Q tag-based VLAN.
Efficient self-learning and address recognition mechanism enables forwarding rate at wire speed.

Publication date: January, 2005
Revision A1

Hardware Specifications

- **Standard Compliance:** IEEE802.3/802.3ab / 802.3z / 802.3u / 802.3x
- **Network Interface:**

Configuration	Mode	Connector	Port
10/100/1000Mbps Gigabit TP	NWay	TP (RJ-45)	1 - 16
1000Base-SX Gigabit Fiber	1000 FDX	*SFP	15,16(Option)
1000Base-LX Gigabit Fiber	1000 FDX	*SFP	15,16(Option)
1000Base-LX Single Fiber WDM (BiDi)	1000 FDX	*SFP	15,16(Option)

*Port 15, 16 are TP/SFP fiber dual media ports with auto detected function
*Optional SFP module supports LC or BiDi SC transceiver

- **Transmission Mode:** 10/100Mbps support full or half duplex
  1000Mbps support full duplex only
- **Transmission Speed:** 10/100/1000Mbps for TP
  1000Mbps for Fiber
- **Full Forwarding/Filtering Packet Rate:** PPS (packets per second)

Forwarding Rate	Speed
1,488,000PPS	1000Mbps
148,800PPS	100Mbps
14,880PPS	10Mbps

- **MAC Address and Self-learning:** 8K MAC address
  4K VLAN table entries,
- **Buffer Memory:** Embedded 400 KB frame buffer
- **Flow Control:** IEEE802.3x compliant for full duplex
  Backpressure flow control for half duplex
- **Cable and Maximum Length:**

TP	Cat. 5 UTP cable, up to 100m
1000Base-SX	Up to 220/275/500/550m, which depends on Multi-Mode Fiber type
1000Base-LX	Single-Mode Fiber, up to10/30/50Km
1000Base-LX WDM (BiDi)	Single-Mode Single Fiber, up to 20Km

- **Diagnostic LED:**

  System LED : Power
  Per Port LED:
  10/100/1000M TP Port 1 to 16 : LINK/ACT, 10/100/1000Mbps
  1000M SFP Fiber Port 15,16 : SFP(LINK/ACT)

- **Power Requirement** **:** AC Line

  Voltage : 100~240 V
  Frequency : 50~60 Hz
  Consumption : 30W
- **Ambient Temperature** **:** 0° to 50°C
- **Humidity** **:** 5% to 90%
- **Dimensions** **:** 44(H) × 442(W) × 209(D) mm
- **Comply with FCC Part 15 Class A & CE Mark Approval**

Management Software Specifications

System Configuration	Auto-negotiation support on 10/100Base-TX ports, Web browser or console interface can set transmission speed (10/100Mbps) and operation mode (Full/Half duplex) on each port, enable/disable any port, set VLAN group, set Trunk Connection.
VLAN Function	Port-Base / 802.1Q-Tagged, allowed up to 256 active VLANs in one switch.
Trunk Function	Ports trunk connections allowed
Bandwidth Control	Supports by-port Egress/Ingress rate control
Quality of Service (QoS)	Referred as Class of Service (CoS) by the IEEE 802.1P standard Two queues per port
Network Management	Web browser support based on HTTP Server

Note: Any specification is subject to change without notice.

Appendix B
MIB Specifications

MIB II Enterprise MIB brief description is listed as below. A MIB file in a readable electronic media (floppy disk or CD-ROM) is packed with the product box.

```
PRIVATE-GS1116C-MIB DEFINITIONS ::= BEGIN

IMPORTS
   mib-2, DisplayString,ifIndex                          FROM RFC1213-MIB
   enterprises,Counter, TimeTicks, Gauge,IpAddress       FROM RFC1155-SMI
   OBJECT-TYPE                                           FROM RFC-1212
   TRAP-TYPE                                             FROM RFC-1215;

privatetech          OBJECT IDENTIFIER ::= { enterprises 5205 }

switch       OBJECT IDENTIFIER ::= { privatetech 2 }

gs1116cProductId      OBJECT IDENTIFIER ::= { switch 8 }

gs1116cProduces       OBJECT IDENTIFIER ::= { gs1116cProductId 1 }

gs1116cIllegalLogin  TRAP-TYPE
        ENTERPRISE gs1116cProductId
        DESCRIPTION
        "Send this trap when the illegal user try to login the Web management UI. "
        ::= 1

gs1116cRxErrorThreshold  TRAP-TYPE
        ENTERPRISE gs1116cProductId
        VARIABLES   { ifIndex }
        DESCRIPTION
        "Send this trap when the number of the Rx bad packet over the Rx Error
Threshold.
        The OID value means the port number. "
        ::= 2

gs1116cTxErrorThreshold  TRAP-TYPE
        ENTERPRISE gs1116cProductId
        VARIABLES   { ifIndex }
        DESCRIPTION
        "Send this trap when the number of the Tx bad packet over the Tx Error
Threshold.
        The OID value means the port number. "
        ::= 3
END
```