DrayTek

VigorSwitch G1241

24 Gigabit Port Web Smart Switch

Your reliable networking solutions partner

User's Guide

V1.2

VigorSwitch G1241
24 Gigabit Port Web Smart Switch
User's Guide

Version: 1.2

Firmware Version: V1.2

Date: March 31, 2016

(For future update, please visit DrayTek web site for further information)

Intellectual Property Rights (IPR) Information

Trademarks   The following trademarks are used in this document:
- Microsoft is a registered trademark of Microsoft Corp.
- Windows, Windows 95, 98, Me, NT, 2000, XP, 7 and Explorer are trademarks of Microsoft Corp.
- Apple and Mac OS are registered trademarks of Apple Inc.
- Other products may be trademarks or registered trademarks of their respective manufacturers.

Caution and Electronic Emission Notices

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.

Warranty   We warrant to the original end user (purchaser) that the device will be free from any defects in workmanship or materials for a period of **one (1)** years from the date of purchase from the dealer. Please keep your purchase receipt in a safe place as it serves as proof of date of purchase. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, we will, at our discretion, repair or replace the defective products or components, without charge for either parts or labor, to whatever extent we deem necessary tore-store the product to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal value, and will be offered solely at our discretion. This warranty will not apply if the product is modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions. The warranty does not cover the bundled or licensed software of other vendors. Defects which do not significantly affect the usability of the product will not be covered by the warranty. We reserve the right to revise the manual and online documentation and to make changes from time to time in the contents hereof without obligation to notify any person of such revision or changes.

Be a Registered Owner   Web registration is preferred. You can register your Vigor device via http://www.draytek.com.

Firmware & Tools Updates   Due to the continuous evolution of DrayTek technology, all devices will be regularly upgraded. Please consult the DrayTek web site for more information on newest firmware, tools and documents.

http://www.draytek.com

Dray Tek

European Community Declarations

Manufacturer: DrayTek Corp.
Address: No. 26, Fu Shing Road, HuKou township, HsinChu Industrial Park, Hsin-Chu, Taiwan 303
Product: VigorSwitch Series Device

The product conforms to the requirements of Electro-Magnetic Compatibility (EMC) Directive 2004/108/EC by complying with the requirements set forth in EN55022/Class A and EN55024/Class A.

The product conforms to the requirements of Low Voltage (LVD) Directive 2006/95/EC by complying with the requirements set forth in EN6095-1.

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.

All trade names and trademarks are the properties of their respective companies.

GPL Notice

This DrayTek product uses software partially or completely licensed under the terms of the GNU GENERAL PUBLIC LICENSE. The author of the software does not provide any warranty. A Limited Warranty is offered on DrayTek products. This Limited Warranty does not cover any software applications or programs.

To download source codes please visit:

http://gplsource.draytek.com

GNU GENERAL PUBLIC LICENSE:

https://gnu.org/licenses/gpl-2.0

Version 2, June 1991

For any question, please feel free to contact DrayTek technical support at support@draytek.com for further information.

Table of Contents

DrayTek

1 Introduction

1.1 Overview

The 24-port Gigabit Web Smart Switch is a standard switch that meets all IEEE 802.3/u/x/z Gigabit, Fast Ethernet specifications. The switch has 20 10/100/1000Mbps TP ports. It supports console, telnet, http and SNMP interface for switch 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.

Others the switch increases support the Power saving for reduce the power consumption with "ActiPHY Power Management" and "PerfectReach Power Management" two techniques. It could efficient saving the switch power with auto detect the client idle and cable length to provide different power.

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.

Below shows key features of this device:

QoS

The switch offers powerful QoS function. This function supports 802.1p VLAN tag priority and DSCP on Layer 3 of network framework.

VLAN

Support Port-based VLAN and IEEE802.1Q Tag VLAN. Support 24 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.

Power Saving

The Power saving using the "ActiPHY Power Management" and "PerfectReach Power Management" two techniques to detect the client idle and cable length automatically and provides the different power. It could efficient to save the switch power and reduce the power consumption.

1.2 Features

The VigorSwitch G1241, 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

- 24 10/100/1000Mbps Auto-negotiation Gigabit Ethernet TP ports

- 512KB on-chip frame buffer

- Jumbo frame support 9KB

- Programmable classifier for QoS (Layer 2/Layer 3)

- 8K MAC address and support VLAN ID(1~4094)

- Per-port shaping, policing, and Broadcast Storm Control

- Power Saving with "ActiPHY Power Management" and "Perfect Reach Power Management" techniques.

- IEEE802.1ad Q-in-Q nested VLAN support

- Full-duplex flow control (IEEE802.3x) and half-duplex backpressure

- Extensive front-panel diagnostic LEDs; System: Power, TP Port1-24: LINK/ACT, 10/100/1000Mbps

Management

- 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 three users to login

- Maximal packet length can be up to 9600 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 3

- Built-in web-based management and CLI management, providing a more convenient UI for the user

1.3 Packing List

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

- VigorSwitch G1241

- AC Power Cord

- CD & Quick Start Guide

- Rubber feet

- Rack mount kit

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

1.4 LED Indicators and Connectors

Before you use the Vigor device, please get acquainted with the LED indicators and connectors first.

There are 24 TP Fast Ethernet ports on the front panel of the switch. LED display area, locating on the front panel, contains a ACT, Power LED and 24 ports working status of the switch.

LED Explanation
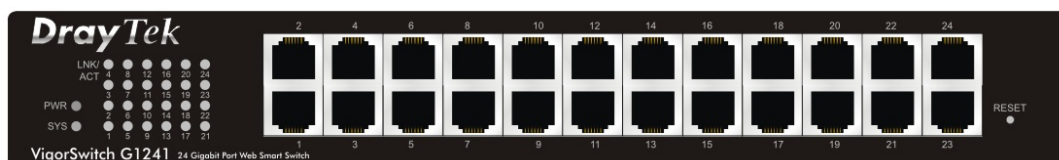
LED	Color	Explanation
PWR	Steady Green	The switch is powered on.
	Off	The switch is powered off.
SYS	Steady Green	The switch is on and functioning properly.
	Blinking Green	The switch is rebooting and performing self-diagnostic tests.
	Off	The power is off or the system is not ready / malfunctioning.
Link/ACT	Steady Green	The link to a 10/100/1000 Mbps Ethernet network is up.
	Blinking Green	The system is transmitting / receiving to/from a 10/100/1000Mbps Ethernet network.
	Off	Port disconnected.

Connector Explanation

Interface	Description
Reset Button	Reset the switch to its factory default configuration via the RESET button. Press the RESET button for three seconds and release. The switch automatically reboots and reloads its factory configuration file. The RESET button is on the front panel of the switch.
LAN P1 – P24	Giga Ethernet Port.

User Interfaces on the Rear Panel

(

24-PORT GBE WEB SMART SWITCH

1.5 Hardware Installation

Case 1: All switch ports are in the same local area network.

Every port can access each other. (*The switch image is sample only.)

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.

Case 2: Port-based VLAN -1 (*The switch image is sample only.)
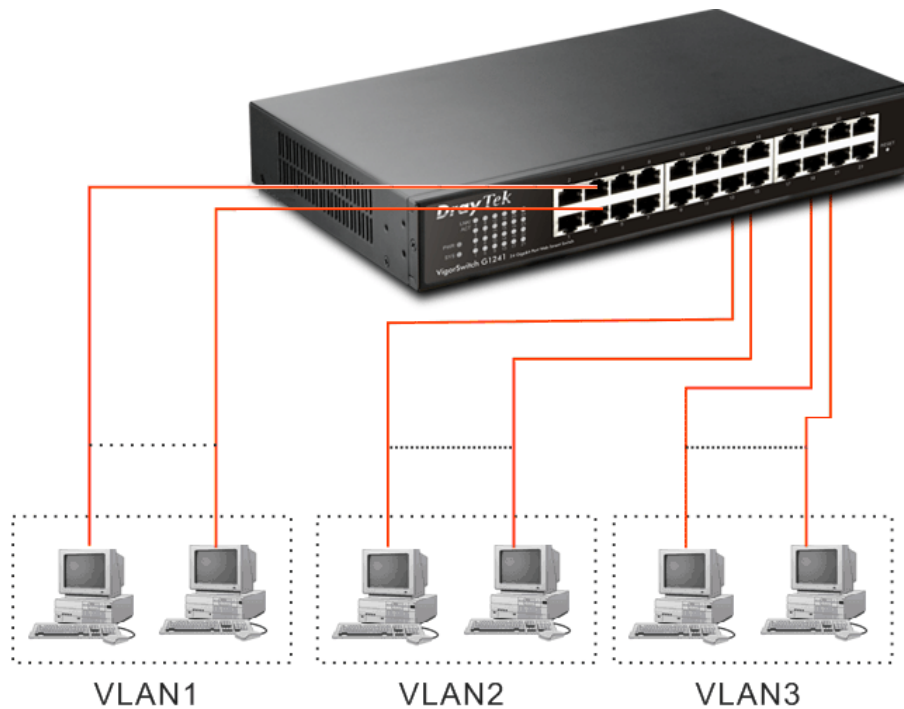
- The same VLAN members could not be in different switches.
- Every VLAN members could not access VLAN members each other.
- The switch manager has to assign different names for each VLAN groups at one switch.

Desktop Installation

1. Install the switch on a level surface that can support the weight of the unit and the relevant components.
2. Plug the switch with the female end of the provided power cord and plug the male end to the power outlet.

Rack-mount Installation

The switch may be standalone, or mounted in a rack. Rack mounting facilitate to an orderly installation when you are going to install series of networking devices.

Procedures to Rack-mount the switch:

1. Disconnect all the cables from the switch before continuing.
2. Place the unit the right way up on a hard, flat surface with the front facing you.
3. Locate a mounting bracket over the mounting holes on one side of the unit.
4. Insert the screws and fully tighten with a suitable screwdriver.
5. Repeat the two previous steps for the other side of the unit.
6. Insert the unit into the rack and secure with suitable screws.
7. Reconnect all the cables.

DrayTek

Installing Network Cables

● Crossover or straight-through cable: All the ports on the switch support Auto-MDI/MDI-X functionality. Both straight-through or crossover cables can be used as the media to connect the switch with PCs as well as other devices like switches, hubs or router.

● Category 3, 4, 5 or 5e, 6 UTP/STP cable: To make a valid connection and obtain the optimal performance, an appropriate cable that corresponds to different transmitting/receiving speed is required. To choose a suitable cable, please refer to the following table.

| Media	Speed	Wiring
10/100/1000 Mbps copper	10 Mbps	Category 3,4,5 UTP/STP
	100Mbps	Category 5 UTP/STP
	1000 Mbps	Category 5e, 6 UTP/STP

Dray Tek

1.5.5 Configuring the Management Agent of Switch

Users can monitor and configure the switch through the following procedures.

Configuring the Management Agent of VigorSwitch G1241 through the 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. We just introduce the first type of management interface. Web-based UI for the switch is an interface in a highly friendly way.
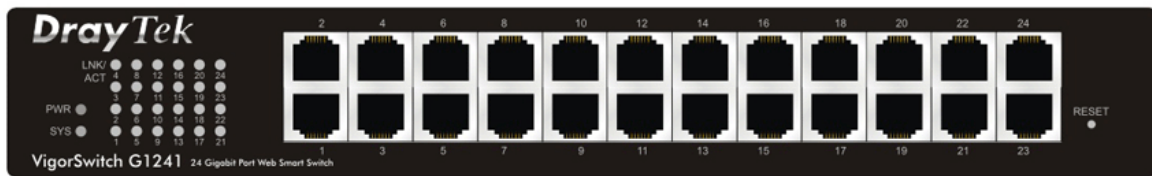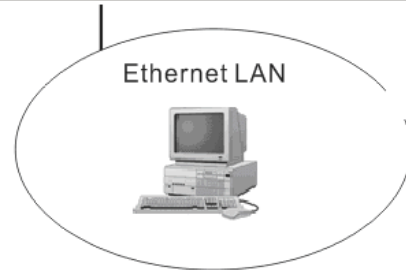
Managing VigorSwitch G1241 through Ethernet Port

Before start using the switch, the IP address setting of the switch should be done, then perform the following steps:

1. 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 the above figure about the 24-Port GbE Web Smart Switch default IP address information.

2. Run web browser and follow the menu. Please refer to Chapter 3.
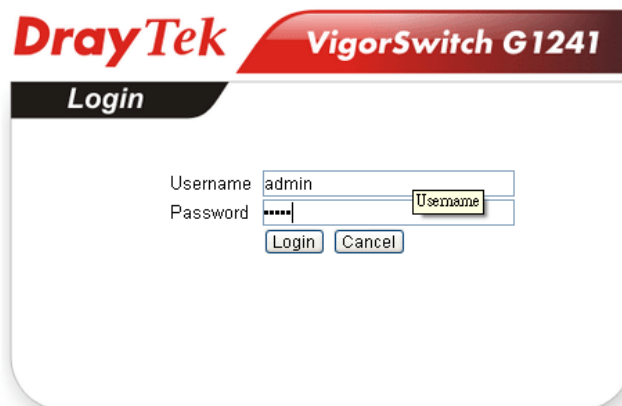
1.5.6 IP Address Assignment

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 below. 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.

Network identifier	Host identifier

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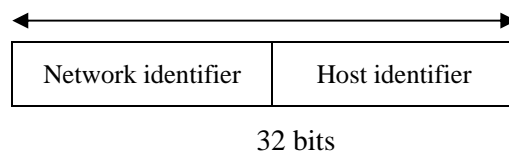
With the classful addressing, it divides IP address into three classes, class A, class B and class C. The rest of IP addresses are for multicast and broadcast. The bit length of the network prefix is the same as that of the subnet mask and is denoted as IP address/X, for example, 192.168.1.0/24. Each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

Bit # 0 1   7 8   31

| 0 | Network address | Host address |
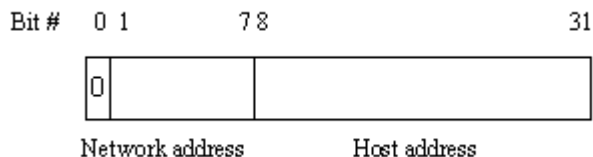
Class B:

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.

Bit # 01 2   15 16   31

| 10 | Network address | Host address |

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.

Bit # 0 1 2 3   23 24   31

```
+-----+-------------------+-----------+
| 110 |                   |           |
+-----+-------------------+-----------+
   Network address            Host address
```
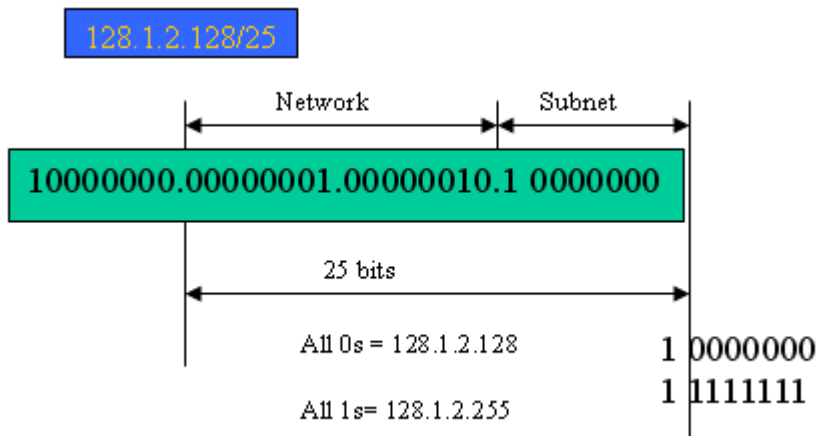
Class D and E:

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.

Dray Tek

128.1.2.128/25

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

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. The gateway setting is used for Trap Events Host only in the switch.

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.
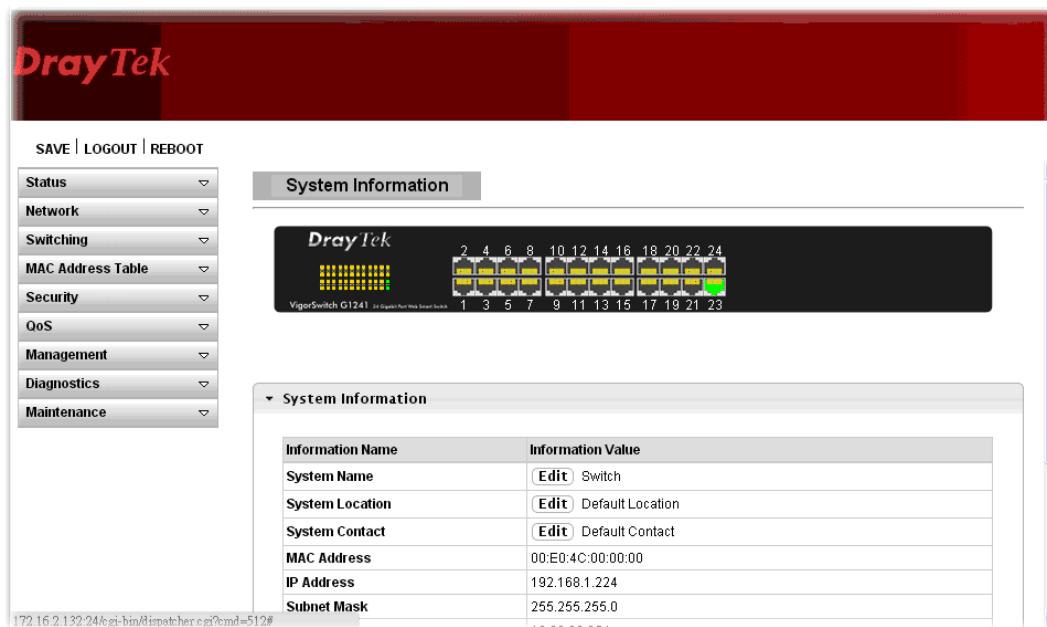
First, IP Address: as shown above, enter "192.168.1.224", for instance. For sure, an IP address such as 192.168.1.x must be set on your PC.

Second, Subnet Mask: as shown above, enter "255.255.255.0". Any subnet mask such as 255.255.255.x is allowable in this case.

> **Note**: The DHCP Setting is enabled in default.

1.6 Typical Applications

The 24-Port L2 Managed Fast Ethernet Switch with 2 SFP Dual Media implements 24 Fast Ethernet TP ports with auto MDIX and 2 Gigabit dual media ports with SFP for removable module supported comprehensive fiber types of connection, including LC, BiDi LC for SFP. For more details on the specification of the switch, please refer to Appendix A.

The switch is suitable for the following applications.

It is a system wide basic reference connection diagram. This diagram demonstrates how the switch and the various devices form the network infrastructure in a large-scale network.

Peer-to-peer application is used in two remote offices
(* The switch image is sample only.)
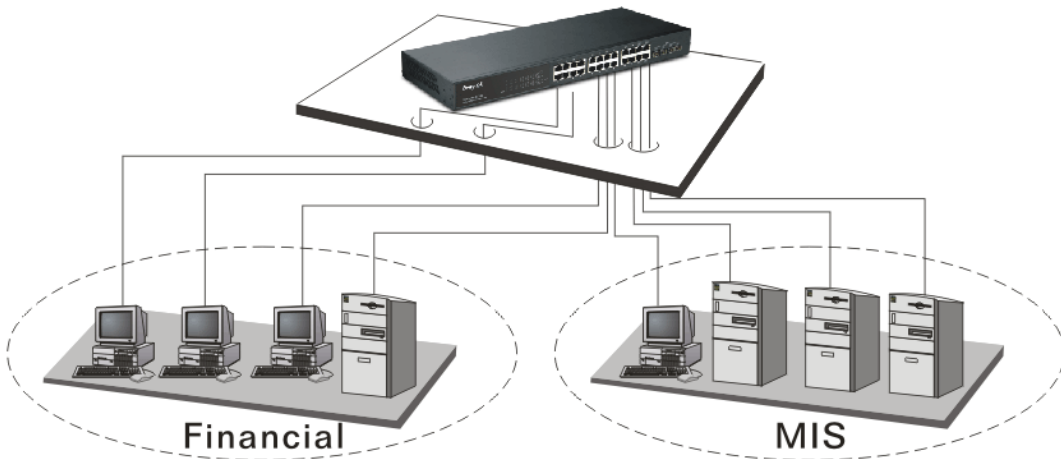
➢ Office Network Connection
(* The switch image is sample only.)

2 Basic Concept and Management

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

2.1 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.
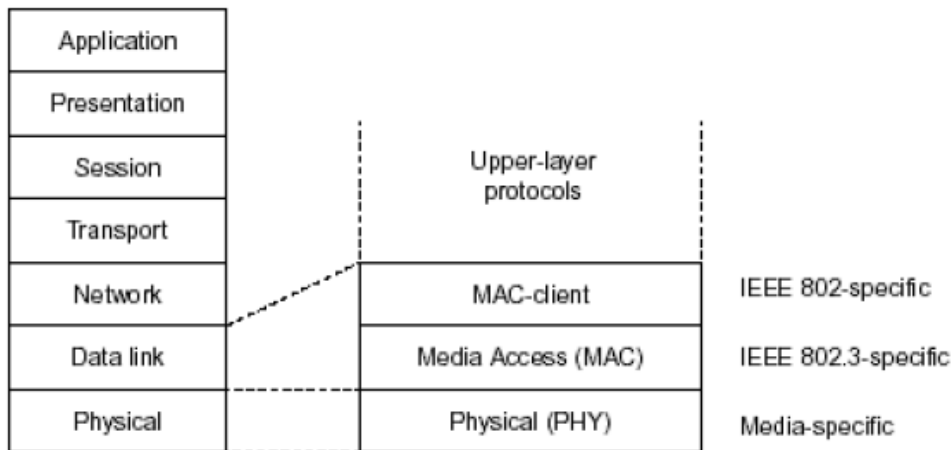
In the above figure, we can see that Ethernet locates at the Data Link layer and Physical layer and comprises three portions, including logical link control (LLC), media access control (MAC), and physical layer. The first two comprises Data link layer, which performs splitting data into frame for transmitting, receiving acknowledge frame, error checking and re-transmitting when not received correctly as well as provides an error-free channel upward to network layer.
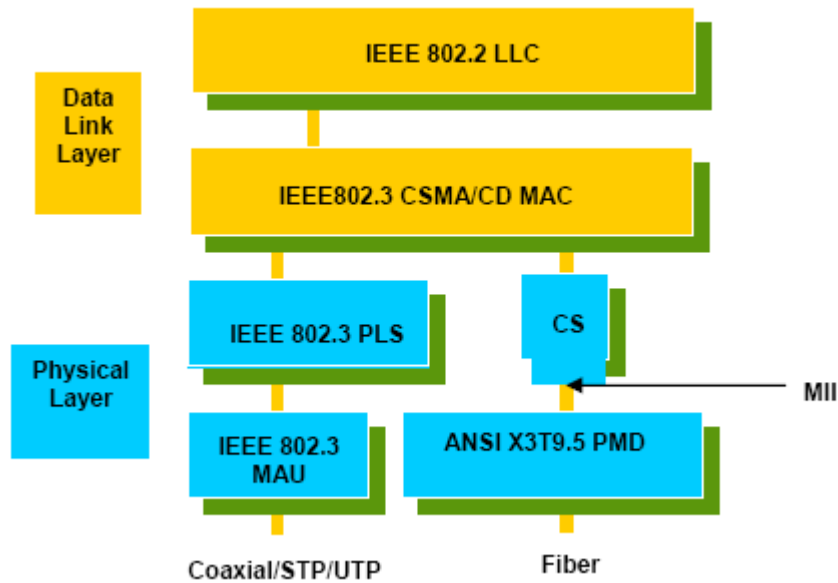
This above diagram shows the Ethernet architecture, LLC sub-layer and MAC sub-layer, which are responded to the Data Link layer, and transceivers, which are responded to the Physical layer in OSI model. In this section, we are mainly describing the MAC sub-layer.

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 rot (see 5.2)]
Information	=	Information field
*	=	Mulliplication
M	=	An integer value equal to or greater than 0. (Upper bound of M is a function of the medium access control methodology used.)

The table above 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

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 defnition
X1SSSSSS   Reserved for ISO defnition

2.2 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.

Dray Tek

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	

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

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 cyclic 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

Dray Tek

the data field and FCS field in turn. The followings summarize what a MAC does before transmitting a frame.

1. 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.

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

3. 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.

4. 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 halfduplex 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 worstcase, 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.
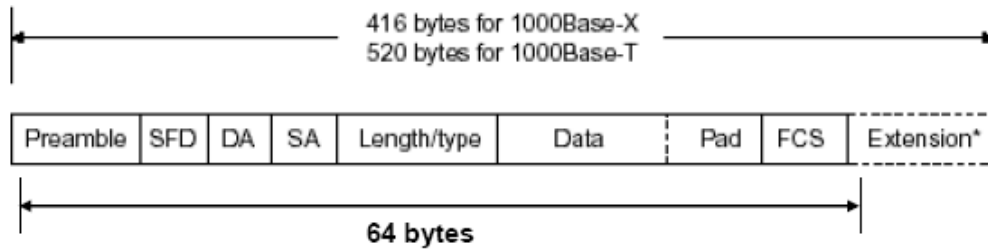
Parameter value/LAN	10Base	100Base	1000Base
Max. collision domain DTE to DTE	100 meters	100 meters for UTP 412 meters for fiber	100 meters for UTP 316 meters for fiber
Max. collision domain with repeater	2500 meters	205 meters	200 meters
Slot time	512 bit times	512 bit times	512 bit times
Interframe 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
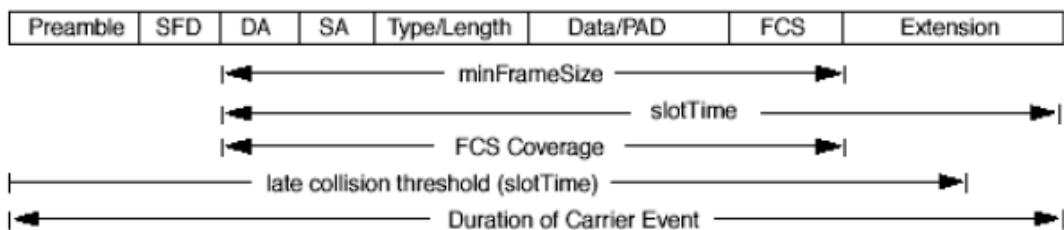
In full-duplex operation mode, both transmitting and receiving frames are processed simultaneously. This doubles the total bandwidth. Full duplex is much easier than half duplex because it does not involve media contention, collision, retransmission schedule, padding bits for short frame. The rest functions 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.

Dray Tek

2.3 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. 24-Port GbE 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 undiscriminated. 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:

1. 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.

2. 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.

3. If the frame is too long. If yes, throws it away and reports frame Too Long.

4. 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.

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

6. 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

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.

2.4 How does a switch work?

The switch is a layer 2 Ethernet Switch equipped with 24 Fast Ethernet ports. Each port on it is an independent LAN segment and thus has 24 LAN segments and 24 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 the figure listed below, 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. (* The switch image is sample only.)
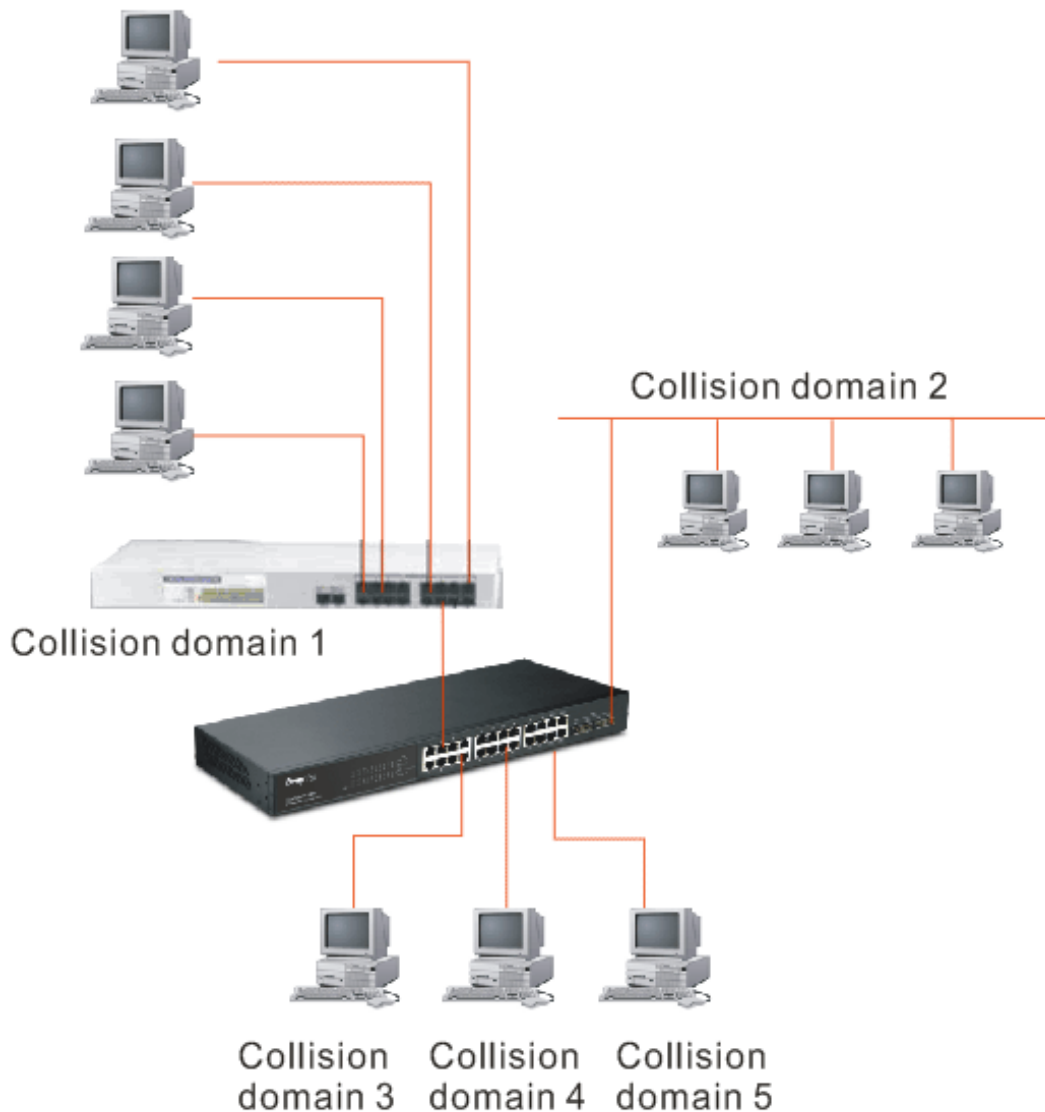
Micro-segmentation:

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.

Extended Distance Limitations:

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. (* The switch image is sample only.)

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. (* The switch image is sample only.)
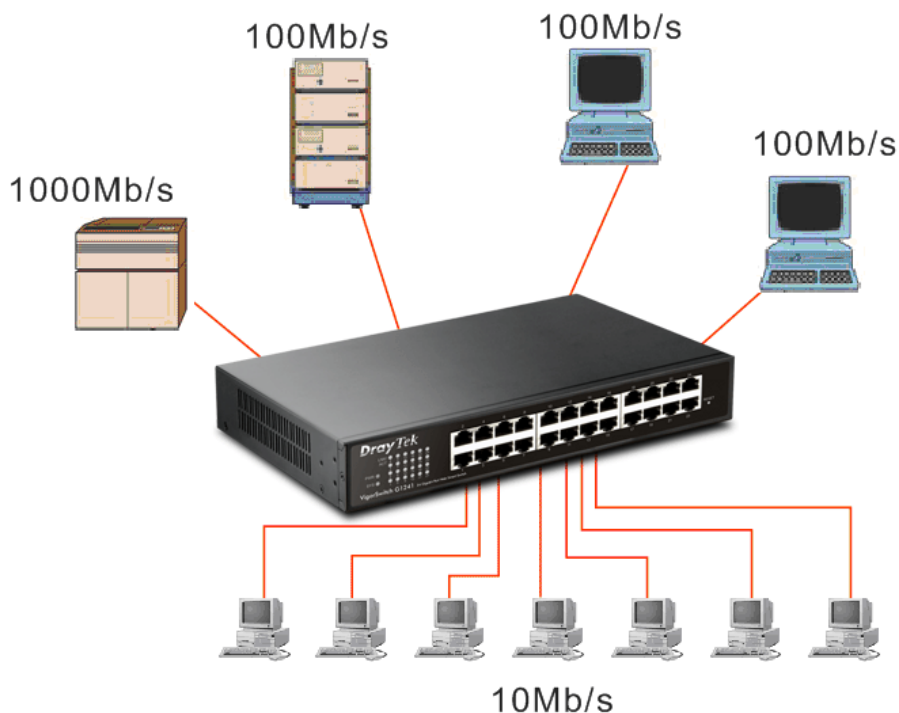
How does a switch operate?

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.

2.5 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.

(* The switch image is sample only.)

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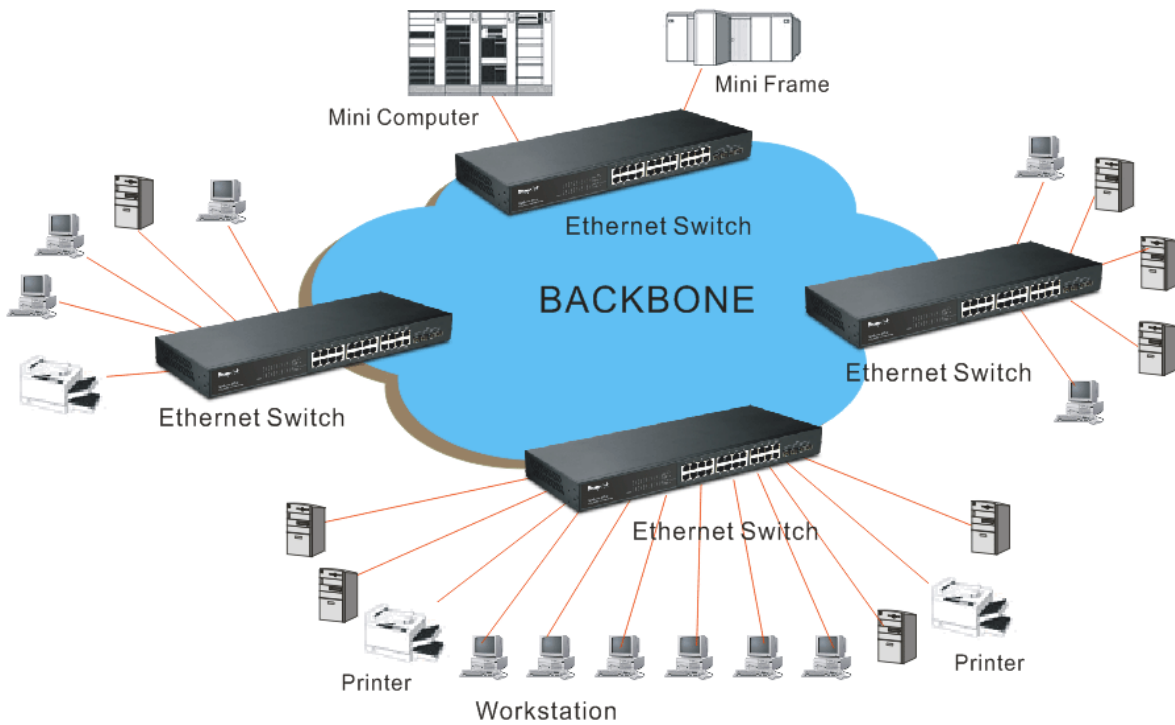
In the figure above, all stations are within the same broadcast domain. For these stations, it is obviously that the traffic is getting congested while adding more stations on it. With the more and more users joining the LAN, broadcast traffic will rapidly decrease the performance of the network. Finally,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

(* The switch image is sample only.)
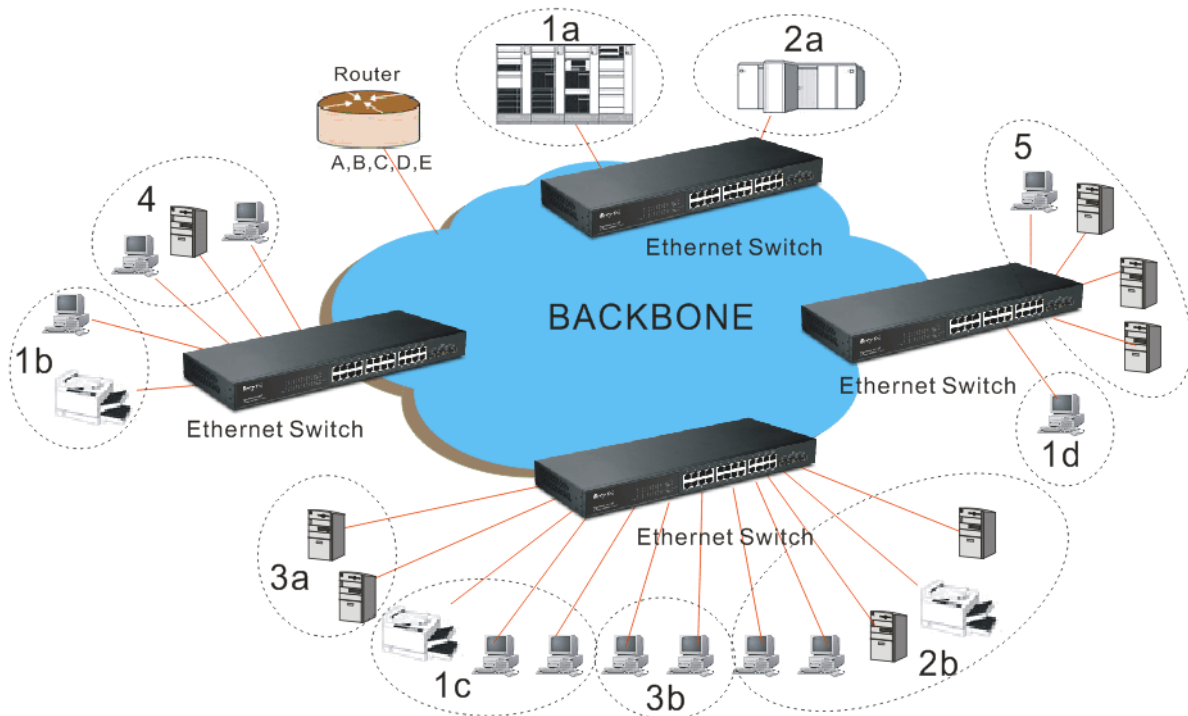
Now we apply VLAN technology to configure the system shown as the figure above. We can partition the users into the different logical networks which have their own broadcast domain. The traffic will not disturb among these logical networks. The users 1x (x denotes a ~ d) are members of VLAN 1. Any traffic 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.
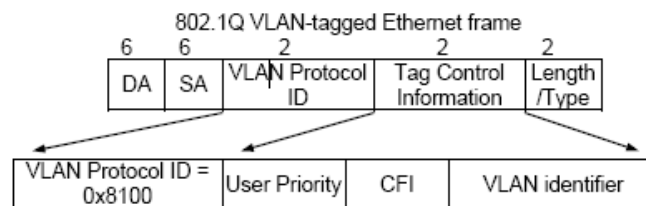
VLAN Protocol ID: 8100 is reserved for VLAN-tagged frame.

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.

Dray Tek

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:

    a. 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.

    b. 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 24-Port GbE 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

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	Port Members
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

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

3 **Operation of Web-based Management**

This chapter would introduce how to manage your Web Smart Switch and how to configure the 10/100/1000Mbps TP Ports on the switch via web user interfaces. Web Smart Switch provides 24 fixed Gigabit Ethernet TP ports. With this facility, you can easily access and monitor the status like MIBs, port activity, and multicast traffic through any ports on the switch.

The default values of the Switch are listed in the figure below:
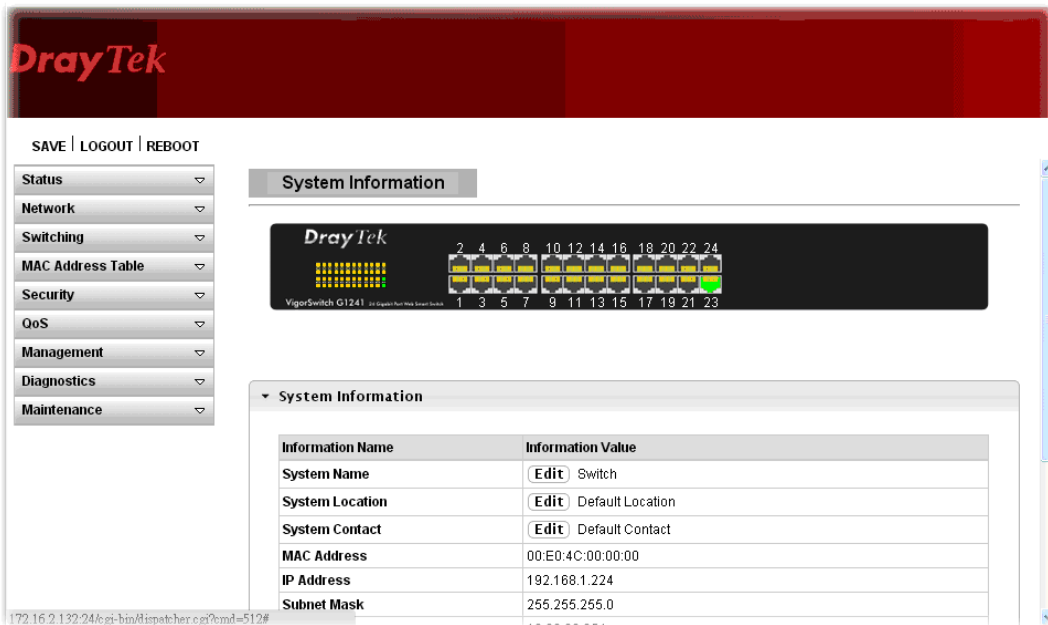
When the configuration of your Web Smart Switch is finished, you can browse it by the IP address you set up. For instance, uncheck the **Enable** box of DHCP Setting first (it is enabled in default). Next, type http://192.168.1.224 in the address row in a browser, then the following screen would show up and ask for your password input for login and access authentication. The default password is "admin". For the first time access, please enter the default password, and click <Apply> button. The login process now would be completed.

Web Smart Switch supports a simplified user management function which allows only one administrator to configure the switch at one time.

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

3.1 Web Management Home Overview

After login, System Information would be displayed as the following illustration. This page lists default values and shows you the basic information of the switch, including "Switch Status", "TP Port Status", "Fiber Port Status", "Aggregation", "VLAN", "Mirror", "SNMP", and "Maximum Packet Length". With this information, you will know the software version, MAC address, ports available and so on. It would be helpful while malfunction occurred. For more details, please refer to Section 3.1.1.

3.1.1 The Information of Page Layout

On the top part of the information page, it shows the front panel of the switch. Linked ports will be displayed in green color, and linked-off ones will be in black. For the optional modules, the slots with no module will only show covered plates, the other slots with installed modules would present modules. The images of modules would depend on the ones you insert. Vice versa, if ports are disconnected, they will show just in black.

On the left side, the main menu tree for web is listed in the page. 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.

3.2 Status

3.2.1 System Information

Function name:

System Information

Function description:

System configuration is one of the most important functions. Without a proper setting, network administrator would not be able to manage the device. The switch supports manual IP address setting.

Show system description, firmware version, hardware version, MAC address, IP address, MAC address, active subnet mask, active gateway, and etc.

▾ System Information	
Information Name	**Information Value**
System Name	[Edit] Switch
System Location	[Edit] Default Location
System Contact	[Edit] Default Contact
MAC Address	00:E0:4C:00:00:00
IP Address	10.28.60.24
Subnet Mask	255.255.255.0
Gateway	10.28.60.254
Loader Version	1.0.0.48161
Loader Date	Aug 15 2014 - 10:33:59
Firmware Version	1.2
Firmware Date	Sep 03 2014 - 13:57:58
System Object ID	1.3.6.1.4.1.27282.3.2.10
System Up Time	13 days, 22 hours, 47 mins, 57 secs
PCB/HW Version	switch

Parameter description:

System Name	System name of the switch. This name will also use as CLI prefix of each line. ("Switch>" or "Switch#")
System Location	Set the location of the switch where it was located.
System Contact	System contact of the switch. For easily managing and maintaining device, you may write down the contact person and phone here for getting help soon. You can configure this parameter through the device's user interface or SNMP.
MAC address	It is the Ethernet MAC address of the management agent in this switch.
IP address	The IP address of the switch.
Subnet Mask	Display the active subnet mask of this switch.
Gateway	Display the active gateway of this switch.
Loader Version	Display the boot loader version in this switch.

Loader Date	Display the date of the loader released.
Firmware Version	Display the firmware version in this switch.
Firmware Date	Display the date of the firmware released.

3.2.2 Logging Message

Function name:

Logging Message

Function description:

Display the switch logs.

Parameter description:

Target	Select the log message source to show on the table. **buffered**: Logs store in the device buffer. **file**: Logs store in file.
Severity	Select severity to filter log messages.
Category	Select category to filter log messages.
Logging Information	Display the name and value selected.
Logging Messages	● **Clear buffered messages** ● **Refresh** – Refresh current status page.

3.2.3 Port

3.2.3.1 Port Counters

Function name:

Port Counters

Function description:

Display port summary and status information.

Parameter description:

Port	This identifies the Ethernet port.

3.2.3.2 Bandwidth Utilization

Function name:

Bandwidth Utilization

Function description:

Display the Bandwidth Utilization information.
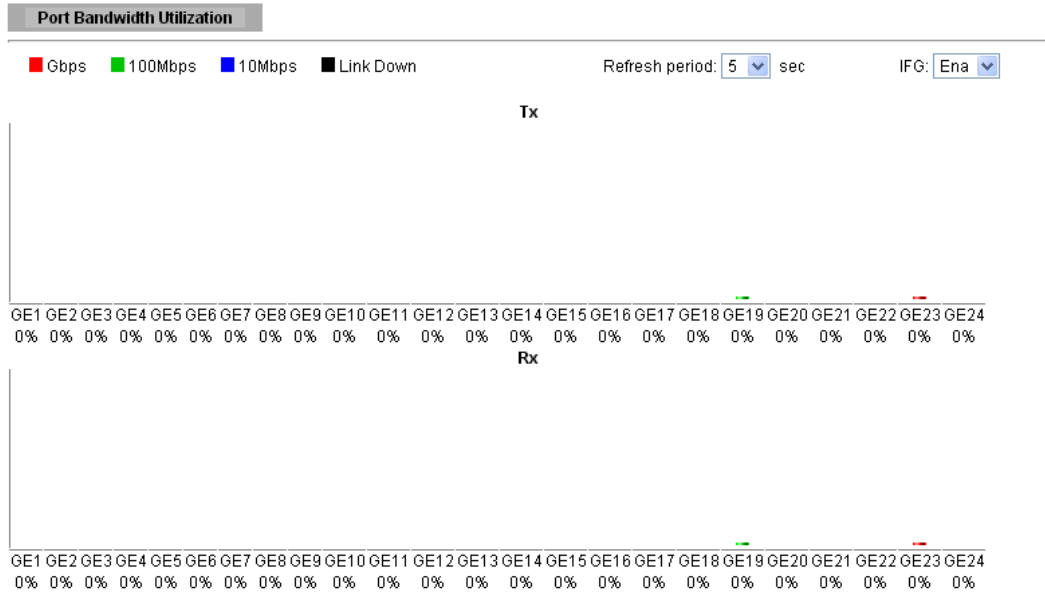
Parameter description:

Refresh Period	Refresh the web page every period of seconds
IFG	Inter frame gap in bandwidth calculation ● **Enable:** Add inter frame gap to bandwidth calculation. ● **Disable:** Remove inter frame gap to bandwidth calculation.

3.2.4 Link Aggregation

Function name:

Link Aggregation (LAG)

Function description:

Parameter description:

LAG Status

LAG	LAG Name.
Name	LAG port description.
Type	The type of the LAG. ● **Static:** The groups of ports assigned to a static LAG are always active members. ● **LACP:** The groups of ports assigned to dynamic LAG are candidate ports. LACP determines which candidate ports are active member ports.
Link State	LAG port link status.
Active Member	Active member ports of the LAG.
Standby Member	Inactive or candidate member ports of the LAG.

3.2.5 LLDP Statistics

Function name:

LLDP Statistics

Function description:

Parameter description:

LLDP Global Statistics

Insertions	The number of times the complete set of information advertised by a particular MAC Service Access Point (MSAP)has been inserted into tables associated with the remote systems.
Deletions	The number of times the complete set of information advertised by MSAP has been deleted from tables associated with the remote systems.
Drops	The number of times the complete set of information advertised by MSAP could not be entered into tables associated with the remote systems because of insufficient resources.
Age Outs	The number of times the complete set of information advertised by MSAP has been deleted from tables

	associated with the remote systems because the information timeliness interval has expired.
LLDP Port Statistics	
Port	Interface or port number.
TX Frames Total	Number of LLDP frames transmitted on the corresponding port.
RX Frames Total	Number of LLDP frames received by this LLDP agent on the corresponding port, while the LLDP agent is enabled.
RX Frames Discarded	Number of LLDP frames discarded for any reason by the LLDP agent on the corresponding port.
RX Frames Errors	Number of invalid LLDP frames received by the LLDP agent on the corresponding port, while the LLDP agent is enabled.
RX TLVs Discarded	Number of TLVs of LLDP frames discarded for any reason by the LLDP agent on the corresponding port.
RX TLVs Unrecognized	Number of TLVs of LLDP frames that are unrecognized while the LLDP agent is enabled
RX Ageouts Total	Number of age out LLDP frames.

3.2.6 IGMP Snooping Statistics

Function name:

IGMP Snooping Statistics

Function description:

IGMP snooping is the process of listening to Internet Group Management Protocol (IGMP) network traffic. The feature allows a network switch to listen in on the IGMP conversation between hosts and routers. By listening to these conversations the switch maintains a map of which links need which IP multicast streams. Multicasts may be filtered from the links which do not need them and thus controls which ports receive specific multicast traffic.

IGMP Snooping Statistics

- IGMP Snooping Statistics

Clear	Refresh	
Statistics Packets	Counter
Total RX	0
Valid RX	0
Invalid RX	0
Other RX	0
Leave RX	0
Report RX	0
General Query RX	0
Specail Group Query RX	0
Specail Group & Source Query RX	0
Leave TX	0
Report TX	0
General Query TX	0
Specail Group Query TX	0
Specail Group & Source Query TX	0

Parameter description:

Total RX	This field displays the total amount of RX
Valid RX	This field displays the total amount of valid RX.
Invalid RX	This field displays the total amount of invalid RX.
Other RX	This field displays the total amount of other RX.
Leave RX	This field displays the total amount of leave RX.
Report RX	This field displays the total amount of report RX.
General Query RX	This field displays the total amount of general query RX.
Special Group Query RX	This field displays the total amount of Special Group query RX.
Special Group & Source Query RX	This field displays the total amount of Special Group& Source query RX.
Leave TX	This field displays the total amount of leave TX.
Report TX	This field displays the total amount of report TX.
General Query TX	This field displays the total amount of general query TX.
Special Group Query TX	This field displays the total amount of Special Group query TX.
Special Group & Source Query TX	This field displays the total amount of Special Group& Source query TX.

3.3 Network

Configure settings for the switch network interface. Offer how the switch connects to a remote server to get services.

3.3.1 IP Address

Function name:

IP Address

Function description:

Use the IP Setting screen to configure the switch IP address and the default gateway device. The gateway field specifies the IP address of the gateway (next hop) for outgoing traffic.

The switch needs an IP address for it to be managed over the network. The factory default IP address is 192.168.1.224. The subnet mask specifies the network number portion of an IP address. The factory default subnet mask is 255.255.255.0.

Parameter description:

Mode	Select the mode of network connection ● **Static**: Enable static IP address. ● **DHCP**: Enable DHCP to obtain IP information from a DHCP server on the network.
IP Address	Enter the IP address of your switch in dotted decimal notation for example 192.168.1.224. If static mode is enabled, enter IP address in this field.
Subnet Mask	Enter the IP subnet mask of your switch in dotted decimal notation for example 255.255.255.0. If static mode is enabled, enter subnet mask in this field.
Gateway	Enter the IP address of the gateway in dotted decimal notation. If static mode is enabled, enter gateway address in this field.

DNS Server 1	If static mode is enabled, enter primary DNS server address in this field.
DNS Server 2	If static mode is enabled, enter secondary DNS server address in this field.
Apply	Save the settings or changes to the switch.

3.3.2 IPv6 Address

Function name:

IPv6 Address

Function description:

Parameter description:

IPv6 Address Setting

Auto Configuration	Select **Enable** or **Disable** this function.
IPv6 Address	Enter the IPv6 address of your switch. If auto configuration mode is disabled, enter IPv6 address in this field.
Gateway	Enter the IP address of the gateway in dotted decimal notation. If auto configuration mode is disabled, enter IPv6gateway address in this field.
DHCPv6 Client	DHCPv6 client state. ● **Enable**: Enable DHCPv6 client function. ● **Disable**: Disable DHCPv6 client function
Apply	Save the settings or changes to the switch.

IPv6 Information

Auto Configuration	Display whether the auto configuration function is opened or not.

IPv6 In Use Address	Display the in use address information of IPv6.
IPv6 In Use Router	Display the in use router information of IPv6.
IPv6 Static Address	Display the static address of IPv6.
IPv6 Static router	Display the static router of IPv6.
DHCPv6 Client	Display the DHCPv6 Client Status.

3.3.3 Management VLAN

Function name:

Management VLAN

Function description:

Parameter description:

Management VLAN	This allows the entry of a VLAN from which a management station will be allowed to manage the device using TCP/IP (in-band via web manager or Telnet). Management stations that are on VLANs other than the one selected here will not be able to manage the Switch. The default management VLAN is VLAN 1.
Apply	Save the settings or changes to the switch.

3.3.4 Time Settings

3.3.4.1 System Time

Function name:

Time Settings

Function description:

Parameter description:

Enable SNTP	Select the radio button to enable or disable using SNTP server.
Manual Time	Specify static time.
Time Zone	Select a time zone
Daylight Saving Time	Select the mode of daylight saving time. ● **Disable**: Disable daylight saving time. ● **Recurring**: Using recurring mode of daylight saving time. ● **Non-Recurring**: Using non-recurring mode of daylight saving time. ● **USA**: Using daylight saving time in the United States that starts on the second Sunday of March and ends on the first Sunday of November ● **European**: Using daylight saving time in the

	Europe that starts on the last Sunday
Daylight Saving Time Offset	Specify the adjust offset of daylight saving time.
Recurring From	Specify the starting time of recurring daylight saving time. This field available when selecting "Recurring" mode.
Recurring To	Specify the ending time of recurring daylight saving time. This field available when selecting "Recurring" mode.
Non-recurring From	Specify the starting time of non-recurring daylight saving time. This field available when selecting "Non-Recurring" mode.
Non recurring To	Specify the ending time of recurring daylight saving time. This field available when selecting "Non-Recurring" mode.
Apply	Save the settings or changes to the switch.

3.3.4.2 SNTP Settings

Function name:

SNTP Settings

Function description:

Parameter description:	
SNTP/NTP Server Address	Input IP address or hostname of time server.
Server port	Input time server port number. Default is 123.
Apply	Save the settings or changes to the switch.

3.4 Switching

This menu item is used to configure settings for the switch ports, trunk, Layer 2 protocols and other switch features.

3.4.1 Port Setting

Function name:

Port Setting

Function description:

It is used to configure switch port settings and show port current status.

Parameter description:

Port Select	Select the port(s) from the list box that you will change the port settings for.
Enabled	Select **Enable** from the drop-down box to enable a port. The factory default for all ports is enabled. A port must be enabled for data transmission to occur. Select **Disable** to not use a port.
Speed	Port speed capabilities: ● **Auto:** Auto speed with all capabilities. ● **Auto-10M:** Auto speed with 10M ability only. ● **Auto-100M:** Auto speed with 100M ability only. ● **Auto-1000M:** Auto speed with 1000M ability only. ● **Auto-10/100M:** Auto speed with 10/100M ability. ● **10M:** Force speed with 10M ability. ● **100M:** Force speed with 100M ability. ● **1000M:** Force speed with 1000M ability. Selecting Auto (auto-negotiation) allows one port to negotiate with a peer port automatically to obtain the connection speed and duplex mode that both ends

	support. When auto-negotiation is turned on, a port on the switch negotiates with the peer automatically to determine the connection speed and duplex mode. If the peer port does not support auto-negotiation or turns off this feature, the switch determines the connection speed by detecting the signal on the cable and using half duplex mode. When the switch's auto-negotiation is turned off, a port uses the pre-configured speed and duplex mode when making a connection, thus requiring you to make sure that the settings of the peer port are the same in order to connect.
Duplex	Port duplex capabilities: ● **Auto:** Auto duplex with all capabilities. ● **Half:** Auto speed with 10/100M ability only. ● **Full:** Auto speed with 10/100/1000M ability only.
Flow Control	A concentration of traffic on a port decreases port bandwidth and overflows buffer memory causing packet discards and frame losses. Flow Control is used to regulate transmission of signals to match the bandwidth of the receiving port. The switch uses IEEE802.3x flow control in full duplex mode and backpressure flow control in half duplex mode. IEEE802.3x flow control is used in full duplex mode to send a pause signal to the sending port, causing it to temporarily stop sending signals when the receiving port memory buffers fill. Back Pressure flow control is typically used in half duplex mode to send a "collision" signal to the sending port (mimicking a state of packet collision) causing the sending port to temporarily stop sending signals and resend later. Select "**Enabled**" to enable it. Or select "**Disabled**" to disable it.
Apply	Save the settings or changes to the switch.
Flow Control Config	The Config column displays if Flow Control has been configured to be turned On or Off for the port.
Flow Control Status	The column displays the port's current Flow Control status.

3.4.2 Mirror

Function name:

Local Mirror Setting

Function description:

The Mirror function copies all the packets that are transmitted by the source port to the destination port. It allows administrators to analyze and monitor the traffic of the monitored ports.

Mirror Setting	
Mirror Setting	
Session ID	Select Session
Monitor session state	portbase-enabl
Destination Port	GE1
allow-ingress	Disable
Sniffer RX Ports	Select RX Ports
Sniffer TX Ports	Select TX Ports

Apply

Session ID	Destination Port	Ingress State	Source TX Port	Source RX Port
1	N/A	N/A	N/A	N/A
2	N/A	N/A	N/A	N/A
3	N/A	N/A	N/A	N/A
4	N/A	N/A	N/A	N/A

Parameter description:

Session ID	Select mirror session ID.
Monitor session state	Select mirror session state: portbase-enabled or Disable.
Destination Port	Select mirror session destination port.
Allow-ingress	Enable or Disable.
Sniffer RX ports	Select mirror session source RX ports only select port based-enabled state, this field is valid only when "**Monitor session state**" is portbase-enabled mirror.
Sniffer TX ports	Select mirror session source TX ports only select port based-enabled state, this field is valid only when "**Monitor session state**" is portbase-enabled mirror.
Apply	Save the settings or changes to the switch.

3.4.3 Link Aggregation

3.4.3.1 LAG Setting

Function name:

LAG Setting

Function description:

Parameter description:

Load Balance Algorithm	Select the LAG load balance distribution algorithm ● **MAC Address**: Based on source and destination MAC address for all packets ● I**P/MAC Address**: Based on source and destination IP addresses for IP packet, and source and destination MAC address for non-IP packets.
Apply	Save the settings or changes to the switch.

3.4.3.2 LAG Management

Function name:

LAG Management

Function description:

Parameter description:	
LAG Management	
LAG	Select the LAG to be configured.
Name	LAG port description.
Type	Select the type of the LAG. ● **Static**: The group of ports assigned to a static LAG will be always active members. ● **LACP**: The group of ports assigned to dynamic LAG will be candidate ports. LACP determines which candidate ports are active member ports.
Ports	Select the trunk member ports in this field. There are the following limitations for choosing the member ports: ● All ports in a LAG must be of the same media type. ● To add a port to the LAG, it cannot belong to any VLAN except the default VLAN. ● Ports in a LAG must not be assigned to another LAG. ● Ports in a LAG must not be a mirroring port. ● No more than eight ports are assigned to a LAG. ● When a port is added to a LAG, the configuration of the LAG is applied to the port. When the port is removed from the LAG, its original configuration is reapplied.

	● There could be at most 8 member ports in a trunk.
Apply	Save the settings or changes to the switch.

LAG Management Information

LAG	LAG Name.
Name	LAG port description.
Type	Select the type of the LAG. ● **Static**: The group of ports assigned to a static LAG will be always active members. ● **LACP**: The group of ports assigned to dynamic LAG will be candidate ports. LACP determines which candidate ports are active member ports.
Link State	LAG port link status.
Active Member	Active member ports of the LAG.
Standby Member	Inactive or candidate member ports of the LAG.
Modify	Click "Edit" button to edit LAG.

3.4.3.3 LAG Port Setting

Function name:

LAG Port Setting

Function description:

LAG Port Setting

LAG Port settings

LAG Select	Enabled	Speed	Flow Control
Select LAGs ▾	⦿Enabled ○Disabled	Auto ▾	○Enabled ⦿Disabled

Apply

▾ **LAG Port Status**

LAG	Description	Port Type	Enable State	Link Status	Speed	Duplex	FlowCtrl Config	FlowCtrl Status
LAG1			Enabled		Auto	Auto	Disabled	Disabled
LAG2			Enabled		Auto	Auto	Disabled	Disabled
LAG3			Enabled		Auto	Auto	Disabled	Disabled
LAG4			Enabled		Auto	Auto	Disabled	Disabled
LAG5			Enabled		Auto	Auto	Disabled	Disabled
LAG6			Enabled		Auto	Auto	Disabled	Disabled
LAG7			Enabled		Auto	Auto	Disabled	Disabled
LAG8			Enabled		Auto	Auto	Disabled	Disabled

Parameter description:

LAG Port settings

LAG	Select the LAG to be configured.
Name	LAG port description.
Enabled	Port admin state.

	● Enabled: Enable the port.
	● Disabled: Disable the port.
Speed	Port speed capabilities.
	● **Auto**: Auto speed with all capabilities.
	● **Auto-10M**: Auto speed with 10M ability only.
	● **Auto-100M**: Auto speed with 100M ability only.
	● **Auto-1000M**: Auto speed with 1000M ability only.
	● **Auto-10M/100M**: Auto speed with 10M/100M.
	● **10M**: Force speed with 10M ability.
	● **100M**: Force speed with 100M ability.
	● **1000M**: Force speed with 1000M ability.
Flow Control	Port flow control.
	● **Enabled**: Enable flow control ability.
	● **Disabled**: Disable flow control ability.
Apply	Save the settings or changes to the switch.
LAG Port Status	
LAG	LAG Name.
Description	LAG port description.
Port Type	Member port media type.
Enable	LAG port admin state.
Link Status	LAG port link status.
Speed	Current LAG port speed.
Duplex	Current LAG port duplex.
Flow Control Config	LAG port flow control configuration.
Flow Control Status	Current LAG port flow control state.

3.4.3.4 LACP Setting

Function name:

LACP Setting

Function description:

It is a Trunk mechanism can aggregate several physical ports to a logical port for higher bandwidth. The device provides at most 8 groups of trunk configuration. Each trunk group can aggregate at most 8 ports. For trunk ports traffic balancing, a hash function is applied and the hash parameters can be configured by user. There are 2 sets of hash algorithm configurations, each trunk group can bind to a set of configuration. The device also provide traffic separation mechanism to choose the link maximum id member port dedicated for known multicast traffic or flooding traffic.

LACP

LACP Setting

System Priority	32768	(1-65535)

Apply

▾ **LACP Information**

Information Name	Information Value
System Priority	32768

Parameter description:

LACP Setting

System Priority	Configure the system priority of LACP. This decides the system priority field in LACP PDU.
Apply	Save the settings or changes to the switch.

LACP Information

System Priority	LACP system priority value

3.4.3.5 LACP Port Setting

Function name:

LACP Port Setting

Function description:

Port id could be physical port id or logical port id (trunk id). Mirror, ingress and egress bandwidth control module base on physical port not logic port, however, almost all of the other modules, such as storm filter, VLAN, L2 table and so on, port id means logical port.

Parameter description:

Port Select	Select one or multiple ports to configure
Priority	Enter the LACP priority value of the port
Timeout	Select the periodic transmissions of LACP PDUs. ● **Long**: Transmit LACP PDU with slow periodic (30s). ● **Short**: Transmit LACPP DU with fast periodic (1s).
Apply	Save the settings or changes to the switch.

3.4.4 VLAN Management

A virtual local area network, virtual LAN or VLAN, is a group of hosts with a common set of requirements that communicate as if they were attached to the same broadcast domain, regardless of their physical location. A VLAN has the same attributes as a physical local area network (LAN), but it allows for end stations to be grouped together even if they are not located on the same network switch. VLAN membership can be configured through software instead of physically relocating devices or connections.

3.4.4.1 Create VLAN

Function name:

Create VLAN

Function description:

It allows a user to add, edit or delete VLAN settings.

Parameter description:

VLAN LIST	Specify the VLAN list to apply the operation (add/delete/edit).
VLAN Action	Select the action of operation. To add/delete/edit the VLANs.
VLAN Name Prefix	Specify the prefix string of the VLAN name for new created VLANs. This field is only available with add action.
Apply	Save the settings or changes to the switch.
Modify	Click "Edit" button to edit VLAN. Click "Delete" button to remove VLAN.

3.4.4.2 Interface Settings

Function name:

Interface Settings

Function description:

This page allows a user to configure VLAN Interface related settings.

A PVID (Port VLAN ID) is a tag that adds to incoming untagged frames received on a port so that the frames are forwarded to the VLAN group that the tag defines.

DrayTek

Interface Settings

Edit Interface Setting

Port Select	Interface VLAN Mode	PVID	Accepted Type	Ingress Filtering
Select Ports ▾	◉Hybrid ○Access ○Trunk	1 (1 - 4094)	◉All ○Tag Only ○Untag Only	◉Enabled ○Disabled

Apply

▾ **Port VLAN Status**

Port	Interface VLAN Mode	PVID	Accept Frame Type	Ingress Filtering
GE1	Hybrid	1	ALL	Enabled
GE2	Hybrid	1	ALL	Enabled
LAG6	Hybrid	1	ALL	Enabled
LAG7	Hybrid	1	ALL	Enabled
LAG8	Hybrid	1	ALL	Enabled

Parameter description:

Port Select	Select specified port or all ports to configure Interface Settings.
Interface VLAN Mode	Select the VLAN mode of the interface. ● **Hybrid**: Support all functions as defined in IEEE 802.1Qspecification. ● **Access**: Accepts only untagged frames and join an untagged VLAN. ● **Trunk**: An untagged member of one VLAN at most, and is a tagged member of zero or more VLANs.
PVID	Specify the port-based VLAN ID (1-4094). It's only available with Hybrid and Trunk mode.
Accepted Type	Specify the acceptable-frame-type of the specified interfaces. It's only available with Hybrid mode.
Ingress Filtering	Specify the status of ingress filtering. It's only available with Hybrid mode.
Apply	Save the settings or changes to the switch.

3.4.4.3 Port to VLAN

Function name:

Port to VLAN

Function description:

This page allows user to configure VLAN port setting.

Parameter description:

VLAN ID	Select specified VLAN ID to configure Port to VLAN Settings.
Interface VLAN Mode	Display the interface VLAN mode of this port.
Membership	Select the membership for this port with the specified VLAN ID. ● **Forbidden**: Specify the port is forbidden in the VLAN. ● **Excluded**: Specify the port is excluded in the VLAN. ● **Tagged**: Specify the port is tagged in the VLAN. ● **Untagged**: Specify the port is untagged in the VLAN.
PVID	Check this checkbox to select the VLAN ID to be the port-based VLAN ID for this port.
Apply	Save the settings or changes to the switch.

3.4.4.4 Port VLAN Membership

Function name:

Port VLAN Membership

Function description:

This page allows user to configure Port VLAN Membership setting.

Parameter description:

Port	Display the interface of this port entry.
Mode	Display the interface VLAN mode of this port.
Administrative VLANs	Display the administrative VLAN list of this port.
Operational VLANs	Display the operational VLAN list of this port.
Modify	Click the `Edit` button to edit the VLAN membership of this port.
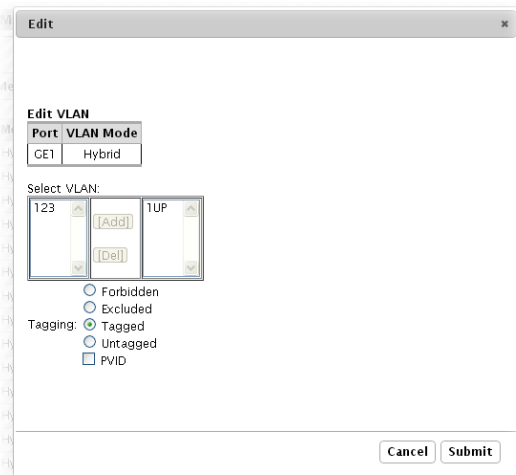
Select VLAN-Select the left available VLANs to add or the right used VLANs to delete for this port.

Tagging-Select the VLAN membership of the specified left VLANs for this port.

PVID-Check this checkbox to select the VLAN ID to be the port-based VLAN ID for this port.

3.4.4.5 Voice VLAN

Function name:

Voice VLAN >>Properties

Function description:

Parameter description:

Voice VLAN State	Select Voice VLAN state. Enable –Voice VLAN is enabled. Disable –Voice VLAN is disabled.
Voice VLAN ID	Select Voice VLAN ID.
Remark Cos/802.1p	Select a value of vpt that will be advertised by LLDP-MED.
1p remark	Select 1p remark state.
Aging Time (30~65536 min)	Select value of aging time.
Apply	Save the settings or changes to the switch.

Function name:

Voice VLAN >>Telephony OUI Mac Setting

Function description:

Telephony OUI Mac setting

Voice VLAN OUI Setting

OUI Address	00:00:00
Description	

[Add]

▾ **Voice VLAN OUI Group**

OUI Address	Description	Modify
00:E0:BB	3COM	[Edit] [Delete]
00:03:6B	Cisco	[Edit] [Delete]
00:E0:75	Veritel	[Edit] [Delete]
00:D0:1E	Pingtel	[Edit] [Delete]
00:01:E3	Siemens	[Edit] [Delete]
00:0F:E2	H3C	[Edit] [Delete]
00:09:6E	Avaya	[Edit] [Delete]

Parameter description:

OUI Address	Select OUI address.
Description	Description of the specified MAC address to the voice VLAN OUI table.

Function name:

Voice VLAN >>Telephony OUI Port Setting

Function description:

Telephony OUI Port Setting

Voice VLAN Port Setting

Port	State	Cos Mode
Select Ports ▾	○Enabled ⦿Disabled	○All ⦿Src

[Apply]

▾ **Voice VLAN Port State**

Port	State	Cos Mode
GE1	Disabled	Src
GE2	Disabled	Src
GE3	Disabled	Src
GE4	Disabled	Src
LAG6	Disabled	Src
LAG7	Disabled	Src
LAG8	Disabled	Src

Parameter description:

Port	Select one or multiple ports to configure.
State	Ingress/Egress type value.

Cos Mode	Select port cos mode.
	Src QoS attributes are applied to packets with OUIs in the source MAC address.
	All QoS attributes are applied to packets that are classified to the Voice VLAN.

3.4.5 EEE

Function name:

EEE

Function description:

This page allows user to enable or disable port EEE (Energy Efficient Ethernet) function.

Parameter description:

Port	Select one or multiple ports to configure
State	Port EEE function.
	● **Enabled**: Enable EEE function
	● **Disabled**: Disable EEE function
Apply	Save the settings or changes to the switch.

3.4.6 Multicast

3.4.6.1 Properties

Function name:

Multicast>>Properties

Function description:

DrayTek

Properties

PropertiesSetting

| Unknown Multicast Action | ○ Drop ⊙ Flood ○ Router Port |

Apply

▾ Properties Informations

Information Name	Information Value
Unknown Multicast Action	Flood
Forwarding Method For IPv4	mac

Parameter description:

Unknown Multicast Action	Set the unknown multicast action ● **Drop**: drop the unknown multicast data. ● **Flood**: flood the unknown multicast data. ● **Router port**: forward the unknown multicast data to router port.
IPv4 Forward Method	Set the ipv4 multicast forward method. ● **MAC**: forward method dmac+vid. ● **Src-Dst-Ip**: forward method dip+sip.
Apply	Save the settings or changes to the switch.

3.4.6.2 IGMP Snooping

Function name:

Multicast>>IGMP Snooping>>IGMP Setting

Function description:

IGMP snooping is the process of listening to Internet Group Management Protocol (IGMP) network traffic. The feature allows a network switch to listen in on the IGMP conversation between hosts and routers. By listening to these conversations the switch maintains a map of which links need which IP multicast streams. Multicasts may be filtered from the links which do not need them and thus controls which ports receive specific multicast traffic.

IGMP Snooping

IGMP Snooping

IGMP Snooping Status	⊙ Enable ○ Disable
IGMP Snooping Version	⊙ v2 ○ v3
IGMP Snooping Report Suppression	⊙ Enable ○ Disable

Apply

▾ IGMP Snooping Informations
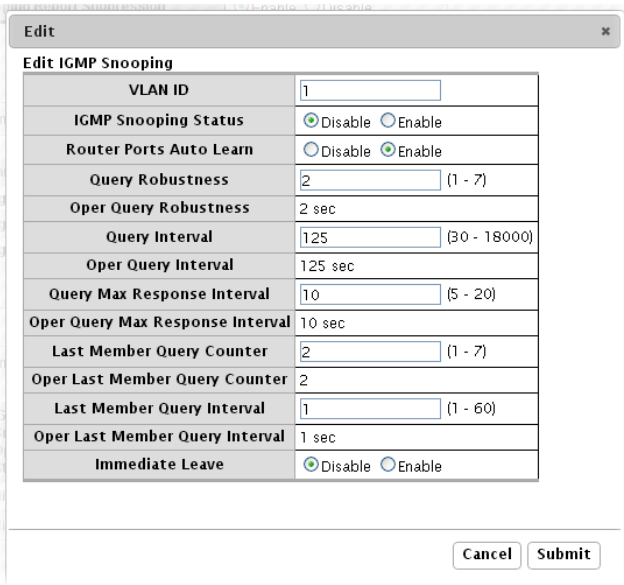
Information Name	Information Value
IGMP Snooping Status	Enable
IGMP Snooping Version	v2
IGMP Snooping V2 Report Suppression	Enable

▾ IGMP Snooping Table

Entry No.	VLAN ID	IGMP Snooping Operation Status	Router Ports Auto Learn	Query Robustness	Query Interval(sec.)	Query Max Response Interval(sec.)	Last Member Query count	Last Member Query Interval(sec)	Immediate Leave	Modify
1	1	disabled	enabled	2	125	10	2	1	disabled	Edit
2	123	disabled	enabled	2	125	10	2	1	disabled	Edit

Parameter description:

IGMP Snooping Status	Set the enabling status of IGMP functionality. ● **Enable**: Enable IGMP Snooping. ● **Disable**: Disable IGMP Snooping.
IGMP Snooping Version	Set the IGMP snooping version. ● **v2**: Only support process IGMP v2 packet. ● **v3**: Support v3 basic and v2.
IGMP Snooping Report Suppression	Set the enabling status of IGMP v2 report suppression. ● **Enable**: Enable IGMP Snooping v2 report suppression. ● **Disable**: Disable IGMP Snooping v2 report suppression.
Apply	Save the settings or changes to the switch.
Entry No	The IGMP entry number.
VLAN ID	The IGMP entry VLAN ID.
IGMP Snooping Operation Status	The enable status of IGMP VLAN functionality. ● **Enabled**: when IGMP Snooping enable and IGMP VLAN enable and multicast filtering enable. ● **Disabled**: when IGMP Snooping disable or IGMP VLAN disable or multicast filtering disable.
Router Ports Auto Learn	Set the enabling status of IGMP router port learning. ● **Enable**: Enable learning router port by query and PIM, DVRMP.

	● **Disable**: Disable learning dynamic router port.
Query Robustness	The Robustness Variable allows tuning for the expected packet loss on a subnet.
Query Interval(sec.)	The interval of queries send general query.
Query Max Response Interval(sec.)	In Membership Query Messages, it specifies the maximum allowed time before sending a responding report in units of 1/10 second.
Last Member Query count	The count that Querier-switch sends Group-Specific Queries when it receives a Leave Group message for a group.
Last Member Query Interval(sec.)	The interval that Querier-switch sends Group-Specific Queries when it receives a Leave Group message for a group.
Immediate leave	Leave the group when receive IGMP Leave message. ● **Enable**: Enable Fastleave. ● **Disable**: Disable Fastleave.
Modify	Click **Edit** to edit the IGMP Snooping Table. **VLAN ID-**The IGMP VLAN ID. **IGMP Snooping Status-**The admin enable status of IGMP VLAN functionality. ● **Enable**: IGMP VLAN enable. ● **Disable**: IGMP VLAN disable. **Router Ports Auto Learn-**Set the enabling status of IGMP router port learning. ● **Enable**: Enable learning router port by query and PIM, DVRMP. ● **Disable**: Disable learning dynamic router port. **Robustness Variable-**The Robustness Variable allows tuning for the expected packet loss on a subnet.

	Query Interval-The admin query interval.
	Oper Query Interval-The operation query interval.
	Query Max Response Interval-The admin query max response interval.
	Oper Query Max Response Interval-The operating query max response interval.
	Last Member Query count-The admin last member query count.
	Oper Last Member Query count-The operating last member query count.
	Last Member Query Interval -The admin last member query interval.
	Oper Last Member Query Interval-The operation last member query interval.
	Immediate leave-Leave the group when receive IGMP Leave message.
	● **Enable**: Enable Fastleave. ● **Disable**: Disable Fastleave.
	Cancel-Click **Cancel** to cancel the change to switch.
	Submit-Click **Submit** to submit the change to switch.

Function name:

Multicast>>IGMP Snooping>>IGMP Querier Setting

Function description:

This page allows user to configure querier settings on specific VLAN of IGMP Snooping.

Parameter description:

VLAN ID	Select the VLANs to configure.
Querier State	Set the enabling status of IGMP Querier Election on the chose VLANs. ● **Enable**: Enable IGMP Querier.

	⚫ **Disable**: Disable IGMP Querier.
Snooping State	Set the query version of IGMP Querier Election on the choseVLANs. ⚫ **v2**: Querier version 2. ⚫ **v3**: Querier version 3.
Apply	Save the settings or changes to the switch.

Function name:

Multicast>>IGMP Snooping>>IGMP Static Group

Function description:

Parameter description:	
VLAN ID	Select the VLANs to configure.
Group IP Address	The IP address of this group.
Member Ports	The member ports of this group.
Add	Click **Add** to add IGMP Group to the switch.
Edit	Click **Edit** to edit the IGMP Static Group.

	VLAN ID-The VLAN ID of static group.
	Group Address-The group address.
	Include Ports Select-The static member ports.
	Cancel-Click Cancel to cancel the change to switch.
	Submit-Click Submit to submit the change to switch.
Delete	Click **Delete** to edit the IGMP Static Group.

Function name:

Multicast>>IGMP Snooping>>IGMP Group Table

Function description:

This page allows user to browse IGMP group information of IGMP Snooping.

IGMP Group Table

▾ IGMP Group Table				
VLAN ID	**Group IP Address**	**Member Ports**	**Type**	**Life(Sec)**
1	224.1.1.11	GE1-2	Static	--

Parameter description:

VLAN ID	The VLAN ID of this group.
Group IP Address	The group IP address of this group.
Member Port	The member ports of this group.
Type	The type of this group. Static or Dynamic.
Life(Sec)	The life time of this group.

Function name:

Multicast>>IGMP Snooping>>IGMP Router Table

Function description:

IGMP Router Table

▾ Dynamic Router Table		
VLAN ID	**Port**	**Expiry Time (Sec)**

Parameter description:

VLAN ID	The VLAN ID of this group.
Port	The member ports of this group.
Expiry Time(Sec)	The expiry time of this group.

3.4.7 Jumbo Frame

Function name:

Jumbo Frame

Function description:

This page allows user to configure switch port jumbo frame settings.

Parameter description:

Jumbo Frame (Bytes)	Jumbo frame size. The valid range is 1526 bytes – 9216 bytes.
Apply	Save the settings or changes to the switch.

3.4.8 STP

3.4.8.1 STP Global Setting

Function name:

STP Global Setting

Function description:

The Spanning Tree Protocol (STP) is a network protocol that ensures a loop-free topology for any bridged Ethernet local area network. This page is used to activate one of the STP modes on the switch.

Parameter description:

Enabled	Specify the STP status to be enabled/disabled on the switch.
BPDU Forward	Specify the BPDU forwarding action when the global STP is disabled.
PathCost Method	Specify the Cost Method of STP.
Force Version	Set the operating mode of STP: ● **STP**-Compatible: IEEE 802.1D STP operation. ● **RSTP**-Operation: IEEE 802.1w operation.
Apply	Save the settings or changes to the switch.

3.4.8.2 STP Port Setting

Function name:

STP Port Setting

Function description:

This page allows user to configure general setting of STP port and browser CIST port status.

Parameter description:

Port Select	Select the port(s) to change spanning tree protocol settings for.
Path Cost	Path cost is the cost of transmitting a frame on to a LAN through that port. It is recommended to assign this value according to the speed of the bridge. The slower the media, the higher the cost. Entering 0 means the switch will automatically assign a value.
EdgePort	Set the edge port configuration: ● **No:** Force to false state (as link to a bridge). ● **Yes:** Force to true state (as link to a host).
P2P MAC	Set the Point-to-Point port configuration: ● **No:** Force to false state. ● **Yes:** Force to true state.
Migrate	Force to try to use the new MST/RST BPDUs, and hence to test the hypothesis that all legacy systems that do not understand the new BPDU formats have been removed from the LAN segment on the port(s).
Apply	Save the settings or changes to the switch.

3.4.8.3 STP Bridge Setting

Function name:

STP Bridge Setting

Function description:

Parameter description:

Priority	Set the STP Bridge Priority in the instance.
Max Hops	Set the value of the maximum number of hops in the region.
Forward Delay	Set the delay time an interface takes to converge from blocking state to forwarding state.
Max Age	Set the time any switch should wait before trying to change the STP topology after unhearing Hello BPUD.
Tx Hold Count	Set the Transmit Hold Count used to limit BPDU transmission rate.
Hello Time	Set the interval between periodic transmissions of BPDU by Designated Ports.
Apply	Save the settings or changes to the switch.

3.4.8.4 STP Port Advanced Setting

Function name:

STP Port Advanced **Setting**

Function description:

This page allows user to configure general setting of STP CIST port and browser CIST port status.

Parameter description:

Port Select	Select the port list to specify which ports should apply this setting.
Priority	Set the Port Priority to the selected ports in the CIST instance.
Apply	Save the settings or changes to the switch.

3.4.8.5 STP Statistics

Function name:

STP Statistics

Function description:

This page allows user to browser general statistics of STP.

STP Statistics

Parameter description:

Port	It displays the port number.
Configuration BDPUs Received	It displays the configuration BDPUs received.
TCN BDPUs Received	It displays the TCN BDPUs received.
Configuration BDPUs Transmitted	It displays the configuration BDPUs transmitted.
TCN BDPUs Transmitted	It displays the Multiple Spanning Tree Protocol (MSTP) BDPUs transmitted.

3.5 MAC Address Table

MAC Address Table is used to show dynamic MAC table and configure settings for static MAC entries.

3.5.1 Static MAC Setting

Function name:

Static MAC Setting

Function description:

Parameter description:

MAC Address	Enter the MAC address in valid MAC address format, that is, six hexadecimal character pairs. Static MAC addresses do not age out.
VLAN	Enter the VLAN identification number the MAC address belongs to.
Type	There are two types of MAC entry: ● **Unicast:** add a unicast MAC entry. ● **Multicast:** add a multicast MAC entry.
Port	If Type is unicast, select the port number of the MAC entry; If Type is multicast, select the port list of the MAC entry.
Add	Click **Add** to add any port into the static MAC address table.
No.	This is the index number for the MAC address forwarding entries.
Delete	To delete any selected MAC address entries.

3.5.2 Dynamic Address Setting

Function name:

Dynamic Address Setting

Function description:

Parameter description:

Aging Time	<10-630> The Dynamic MAC address aging out value.
Apply	Save the settings or changes to the switch.

3.5.3 Dynamic Learned

Function name:

Dynamic Learned

Function description:

Parameter description:

Port	Select the port number to show or clear dynamic MAC entries. If not select any port, VLAN and MAC address,

Dray Tek

	the whole dynamic MAC table will be displayed or cleared.
VLAN	This is the VLAN group to which the MAC address belongs. Select the VLAN to show or clear dynamic MAC entries. If not select any port, VLAN and MAC address, the whole dynamic MAC table will be displayed or cleared.
MAC Address	This field displays the MAC address that will be forwarded. Select the MAC address to show or clear dynamic MAC entries. If not select any port, VLAN and MAC address, the whole dynamic MAC table will be displayed or cleared.
View	Click the View button to display the logs according the criteria specified in the fields above.
Clear	Click this button to remove any dynamically learned MAC address forwarding entries.
Type	This shows whether the MAC address is **Dynamic** (learned by the Switch) or **Static Unicast** (manually entered in the **Static MAC Forwarding** screen).
Port	This field displays the port where the MAC address will be forwarded.
Add to Static MAC table	Click this button to add any port into the static MAC table.

3.6 Security

Security pages are used to configure settings for the switch security features.

3.6.1 Storm Control

3.6.1.1 Global Setting

Function name:

Global Setting

Function description:

Storm Control Global

Storm Control Global Setting

Unit	○ pps ● bps
Preamble & IFG	● Excluded ○ Included

Apply

▾ Storm Control Global Information

Information Name	Information Value
Unit	bps
Preamble & IFG	Excluded

Parameter description:

Mode	Select the mode of storm control ● pps: storm control rate calculates by packet-based ● bps: storm control rate calculates by octet-based
Preamble &IFG	Select the rate calculates w/o preamble & IFG (20 bytes) ● Excluded: exclude preamble & IFG (20 bytes) when count ingress storm control rate. ● Included: include preamble & IFG (20 bytes) when count ingress storm control rate.
Apply	Save the settings or changes to the switch.

3.6.1.2 Port Setting

Function name:

Port Setting

Function description:

Storm Control

Storm Control Setting

Port	Port State	Action	Type Enable	Rate (Kbps)
Select Ports ▾	⦿ Disable ◯ Enable	drop ▾	☐ Broadcast ☐ Unknown Multicast ☐ Unknown Unicast	10000 10000 10000

[Apply]

▾ **Storm Control Information**

Port	Port State	Broadcast (Kbps)	Unknown Multicast (Kbps)	Unknown Unicast (Kbps)	Action
GE1	disabled	Off (10000)	Off (10000)	Off (10000)	Drop
GE2	disabled	Off (10000)	Off (10000)	Off (10000)	Drop
GE22	disabled	Off (10000)	Off (10000)	Off (10000)	Drop
GE23	disabled	Off (10000)	Off (10000)	Off (10000)	Drop
GE24	disabled	Off (10000)	Off (10000)	Off (10000)	Drop

Parameter description:

Port	Select the setting ports.
Port State	Select the state of setting. ● **Disable**: Disable the storm control function. ● **Enable**: Enable the storm control function.
Action	Select the state of setting. ● **Drop**: Packets exceed storm control rate will be dropped. ● **Shutdown**: Port exceeds storm control rate will be shutdown.
Type Enable	Select the type of storm control. ● **Broadcast**: Broadcast packet. ● **Unknown Unicast**: Unknown unicast packet. ● **Unknown Multicast**: Unknown multicast packet.
Rate (Kbps)	Value of storm control rate, Unit: pps (packet per-second) or Kbps. (Kbits per-second) depends on global mode setting. The range is from 0 to 1000000.
Apply	Save the settings or changes to the switch.

3.6.2 Protected Ports

Function name:

Protected Ports

Function description:

This page allows user to configure protected port setting to prevent the selected ports from communicate with each other.

Protected Ports

Protected Ports Settings

Port List	Port Type
Select Protect⤷	⊙ Unprotected ○ Protected

Apply

▾ **Protected Ports Status**

Protected Type	Port List
Protected Ports	
Unprotected Ports	all

Parameter description:

Port List	Select the port to be protected.
Port Type	Configure port protect type: ● **Unprotected:** Unprotected port can communicate with all ports. ● **Protected:** Prevent protected ports from communicate with each other.
Apply	Save the settings or changes to the switch.

3.6.3 DoS

3.6.3.1 DoS Global Setting

Function name:

DoS Global Setting

Function description:

This page allows user to configure DoS setting to enable/disable DoS function for Global Setting.

DoS Global Setting

Global DoS Setting

DMAC = SMAC	⊙ Enabled ○ Disabled
Land	⊙ Enabled ○ Disabled
UDP Blat	⊙ Enabled ○ Disabled
TCP Blat	⊙ Enabled ○ Disabled
POD	⊙ Enabled ○ Disabled
IPv6 Min Fragment	⊙ Enabled ○ Disabled Byte: 1240 (0-65535)
ICMP Fragments	⊙ Enabled ○ Disabled
IPv4 Ping Max Size	⊙ Enabled ○ Disabled
IPv6 Ping Max Size	⊙ Enabled ○ Disabled
Ping Max Size Setting	Byte: 512 (0-65535)
Smurf Attack	⊙ Enabled ○ Disabled Netmask Length: 0 (0-32)
TCP Min Hdr Size	⊙ Enabled ○ Disabled Bytes: 20 (0-31)
TCP-SYN(SPORT<1024)	⊙ Enabled ○ Disabled
Null Scan Attack	⊙ Enabled ○ Disabled
X-Mas Scan Attack	⊙ Enabled ○ Disabled
TCP SYN-FIN Attack	⊙ Enabled ○ Disabled
TCP SYN-RST Attack	⊙ Enabled ○ Disabled
TCP Fragment (Offset = 1)	⊙ Enabled ○ Disabled

Apply

▾ DoS Informations

Information Name	Information Value
DMAC = SMAC	Enabled
Land Attack	Enabled
UDP Blat	Enabled
TCP Blat	Enabled
POD (Ping of Death)	Enabled
IPv6 Min Fragment Size	Enabled (1240 Bytes)

Parameter description:

DMAC = SMAC	Both the source and the destination MAC addresses are the same. ● **Disabled**: Disable the item DoS setting. ● **Enabled**: Enable the item DoS setting.
Land	Both the source and the destination IPv4/IPv6 addresses are the same. ● **Disabled**: Disable the item DoS setting. ● **Enabled**: Enable the item DoS setting.
UDP Blat	Both the source and the destination UDP port are the same. ● **Disabled**: Disable the item DoS setting. ● **Enabled**: Enable the item DoS setting.
TCP Blat	Both the source and the destination TCP port are the

	same.
	● **Disabled**: Disable the item DoS setting.
	● **Enabled**: Enable the item DoS setting.
POD	Ping packets that length are larger than 65535 bytes.
	● **Disabled**: Disable the item DoS setting.
	● **Enabled**: Enable the item DoS setting.
IPv6 Min Fragment	IPv6 fragmented packets (not including the last one) that payload length less than 1240 bytes, and the Min length can be configured if needed.
	● **Disabled**: Disable the item DoS setting.
	● **Enabled**: Enable the item DoS setting.
ICMP Fragments	Fragmented ICMP packets.
	● **Disabled**: Disable the item DoS setting.
	● **Enabled**: Enable the item DoS setting.
IPv4 Ping Max Size	IPv4 PING packet with the length.
	● **Disabled**: Disable the item DoS setting.
	● **Enabled**: Enable the item DoS setting.
Ipv6 Ping Max Size	IPv6 PING packet with the length.
	● **Disabled**: Disable the item DoS setting.
	● **Enabled**: Enable the item DoS setting.
Ping Max Size Setting	Ping packet Max Size Setting. The default value is 512Bytes, it can be configured if needed.
Smurf Attack	ICMP echo request packet that destination IPv4 address is broadcast address. The default Netmask length is 0, and it can be configured if needed.
	● **Disabled**: Disable the item DoS setting.
	● **Enabled**: Enable the item DoS setting.
TCP Min Hdr Size	TCP packet that header length is less than the configured value.
	The default TCP Min Hdr Size is 20, it can be configured if needed.
	● **Disabled**: Disable the item DoS setting.
	● **Enabled**: Enable the item DoS setting.
TCP-SYN(SPORT<1024)	TCP SYN packets with source port less than 1024.
	■ **Disabled**: Disable the item DoS setting.
	■ **Enabled**: Enable the item DoS setting.
Null Scan Attack	TCP sequence number is zero, and all control flags are zeroes.
	● **Disabled**: Disable the item DoS setting.
	● **Enabled**: Enable the item DoS setting.
X-Mas Scan Attack	TCP sequence number is zero, and the FIN/URG/PSH flags are set.
	● **Disabled**: Disable the item DoS setting.

Dray Tek

	● **Enabled**: Enable the item DoS setting.
TCP SYN-FIN Attack	A TCP packet with the SYN and FIN flags set.
	● **Disabled**: Disable the item DoS setting.
	● **Enabled**: Enable the item DoS setting.
TCP SYN-RST Attack	A TCP packet with the SYN and RST flags set.
	● **Disabled**: Disable the item DoS setting.
	● **Enabled**: Enable the item DoS setting.
TCP Fragment (Offset=1)	Fragmented TCP packets.
	● **Disabled**: Disable the item DoS setting.
	● **Enabled**: Enable the item DoS setting.
Apply	Save the settings or changes to the switch.

3.6.3.2 DoS Port Setting

Function name:

DoS Port Setting

Function description:

Parameter description:

Port Select	Select one or multiple ports to configure.
DoS Protection	Configure port protect state
	● **Disabled**: Disable port DoS Protection function.
	● **Enabled**: Enable port DoS Protection function.
Apply	Save the settings or changes to the switch.

3.6.4 Access

3.6.4.1 Telnet

Function name:

Telnet

Function description:

Telnet is the TCP/IP standard protocol for remote terminal service. TELNET allows a user at one site to interact with a remote timesharing system at another site as if the user's keyboard and display connected directly to the remote machine.

Telnet Settings

Telnet Settings	
Telnet Service	Disabled

Apply   Disconnect

- Telnet Information

Information Name	Information Value
Telnet Service	Disabled
Current Telnet Sessions Count	0

Parameter description:

Telnet Service	Set Enabled to access telnet service or Disabled not to access telnet service.
Apply	Save the settings or changes to the switch.
Disconnect	Click **Disconnect** to disconnect Telnet connection.

3.6.4.2 HTTP

Function name:

HTTP

Function description:

HTTP is the acronym of HyperText Transfer Protocol.

HTTP Settings

HTTP Settings

HTTP Service	⊙ Enabled ○ Disabled
Session Timeout	10 (0-86400) minutes

Apply

▾ HTTP Information

Information Name	Information Value
HTTP Service	Enabled
Session Timeout	10

Parameter description:

HTTP Service	Support HTTP service ● **Enable**: Enable HTTP service. ● **Disable**: Disable HTTP service.
Session Timeout	Set session timeout minutes for user access WEB from HTTP protocol. If user does not response after session timeout minute, WEBUI will logout automatically. 0 minutes means never timeout.
Apply	Save the settings or changes to the switch.

3.6.4.3 HTTPS

Function name:

HTTPS

Function description:

HTTPS is the acronym of Hypertext Transfer Protocol over Secure Socket Layer.

HTTPS Settings

HTTPS Settings

HTTPS Service	⊙ Enabled ○ Disabled
Session Timeout	10 (0-86400) minutes

Apply

▾ HTTPS Information

Information Name	Information Value
HTTPS Service	Enabled
Session Timeout	10

Parameter description:

HTTPS Service	Support HTTPS service **Enable**: Enable HTTPS service. **Disable**: Disable HTTPS service.

Session Timeout	Set session timeout minutes for user access WEB from HTTPS protocol. If user does not response after session timeout minute, WEB UI will logout automatically. 0 minutes means never timeout.
Apply	Save the settings or changes to the switch.

3.7 QoS

Use the QoS pages to configure settings for the switch QoS interface and how the switch connects to a remote server to get services.

3.7.1 General

3.7.1.1 QoS Properties

Function name:

QoS Properties

Function description:

It is used to configure settings for both basic and advanced modes.

Parameter description:

QoS Mode	Select the QoS operation mode.
	● **Disable**: Disable QoS.
	● **Basic**: Set QoS to basic mode.
Apply	Save the settings or changes to the switch.

3.7.1.2 Port Settings

Function name:

Port Settings

Function description:

Parameter description:

Port	Select one or multiple ports to configure.
CoS Value	Set default CoS/802.1p priority value for the selected ports.
Remark CoS	Enable/Disable CoS remark.
Remark DSCP	Enable/Disable DSCP remark.
Remark IP Precedence	Enable/Disable IP Precedence remark.
Apply	Save the settings or changes to the switch.

3.7.1.3 Queue Settings

Function name:

Queue Settings

Function description:

Queue Setting

Queue Table

Queue	Scheduling Method			
	Strict Priority	WRR	Weight	% of WRR Bandwidth
1	◉	○	1	
2	◉	○	2	
3	◉	○	3	
4	◉	○	4	
5	◉	○	5	
6	◉	○	9	
7	◉	○	13	
8	◉	○	15	

Apply

Queue Information

Information Name	Information Value
Strict Priority Queue Number	8

Parameter description:

Queue	Queue ID to configure.
Strict Priority	Set queue to strict priority type.
WRR	Set queue to Weight round robin type.
Weight	If the queue type is WRR, set the queue weight for the queue.
Apply	Save the settings or changes to the switch.

3.7.1.4 CoS Mapping

Function name:

CoS Mapping

Function description:

Parameter description:

CoS to Queue Mapping

Class of service	Class of service value.
Queue	Select queue ID for the CoS value.

Queue of CoS Mapping

Queue	Queue ID.
Class of service	Select CoS Value for the Queue ID.
Apply	Save the settings or changes to the switch.

3.7.1.5 DSCP Mapping

Function name:

DSCP Mapping

Function description:

Parameter description:

DSCP to Queue Mapping

DSCP	Select the DSCP value to mapping to the priority and drop precedence. The DSCP range is 0 to 63.
Queue	Select queue ID for the DSCP value.

Queue to DSCP Mapping

Queue	Queue ID.
DSCP	Select DSCP Value for the Queue ID.
Apply	Save the settings or changes to the switch.

3.7.1.6 IP Precedence Mapping

Function name:

IP Precedence Mapping

Function description:

Parameter description:

IP Precedence to Queue Mapping

IP Precedence	IP Precedence value.
Queue	Select queue ID for the IP Precedence value.

Queue to IP Precedence Mapping

Queue	Queue ID.
IP Precedence	Select IP Precedence value for the queue ID.
Apply	Save the settings or changes to the switch.

3.7.2 QoS Basic Mode

3.7.2.1 Global Settings

Function name:

Global Settings

Function description:

It is used to configure settings for QoS basic mode.

Parameter description:	
Trust Mode	Select the QoS operation mode. ● **CoS/802.1p**: Traffic is mapped to queues based on the CoS field in the VLAN tag, or based on the per-port default CoS value if there is no VLAN tag on the incoming packet. ● **DSCP**: All IP traffic is mapped to queues based on the DSCP field in the IP header. If traffic is not IP traffic, it is mapped to the lowest priority queue. ● **CoS/802.1p-DSCP**: All IP traffic is mapped to queues based on the DSCP field in the IP header. If traffic is not IP but has VLAN tag, mapped to queues based on the CoS value in the VLAN tag. ● **IP Precedence**: All IP traffic is mapped to queues based on the IP Precedence field in the IP header. If traffic is not IP traffic, it is mapped to the lowest priority queue. ● **None**: All traffic is mapped to the lowest priority queue.
Apply	Save the settings or changes to the switch.

3.7.2.2 Port Settings

Function name:

Port Settings

Function description:

Parameter description:

Port	Select one or multiple ports to configure.
Trust	Select the port trust state. ● **Enabled**: Traffic from this port will follow the global trust type. ● **Disabled**: Traffic will always go to the lowest priority queue.
Apply	Save the settings or changes to the switch.

3.7.3 Rate Limit

3.7.3.1 Ingress Bandwidth Control

Function name:

Ingress Bandwidth Control

Function description:

Parameter description:

Port	Select one or multiple ports to configure.
State	Enable/Disable ingress bandwidth control.
Rate	Rate value,<0-1000000>,unit:16 Kbps.
Apply	Save the settings or changes to the switch.

3.7.3.2 Egress Bandwidth Control

Function name:

Egress Bandwidth Control

Function description:

Parameter description:

Port	Select one or multiple ports to configure.
State	Enable/Disable egress bandwidth control.
Rate	Rate value,<0-1000000>,unit:16 Kbps.
Apply	Save the settings or changes to the switch.

3.7.3.3 Egress Queue

Function name:

Egress Queue

Function description:

Egress Queue Bandwidth Control

Egress Queue Bandwidth Control Settings

Port	Queue	State	CIR(Kbps)
GE1	1	⊙ Disable ○ Enable	(16-1000000, must a multiple of 16)

Apply

▾ **GE1 Egress Per Queue Status**

Queue Id	Rate Limit (Kbps)
1	off
2	off
3	off
4	off
5	off
6	off
7	off
8	off

Parameter description:

Port	Select one or multiple ports to configure.
Queue	Select one queue to configure.
State	Enable/Disable egress bandwidth control.
CIR(Kbps)	Rate value,<0-1000000>,unit:16 Kbps.
Apply	Save the settings or changes to the switch.

3.8 Management

3.8.1 LLDP

LLDP is a one-way protocol; there are no request/response sequences. Information is advertised by stations implementing the transmit function, and is received and processed by stations implementing the receive function. The LLDP category contains LLDP and LLDP-MED pages.

3.8.1.1 LLDP Global setting

Function name:

LLDP Global setting

Function description:

LLDP Global Setting

Global Settings

Enabled	⦿ Enabled ◯ Disabled
LLDP PDU Disable Action	◯ Filtering ◯ Bridging ⦿ Flooding
Transmission Interval	30 (5-32767)
Holdtime Multiplier	4 (2-10)
Reinitialization Delay	2 (1-10)
Transmit Delay	2 (1-8191)

[Apply]

▾ LLDP Global Config

Config Name	Config Value
LLDP Enabled	Enabled
LLDP PDU Disable Action	Flooding
Transmission Interval	30 Secs
Holdtme Multiplier	4
Reinitialization Delay	2 Secs
Transmit Delay	2 Secs

Parameter description:

Enabled	Enable/ Disable LLDP protocol on this switch.
LLDP PDU Disable Action	Select LLDP PDU handling action to be filtered, bridging or flooded when LLDP is globally disabled.
Transmission Interval	Select the interval at which frames are transmitted. The default is 30 seconds, and the valid range is 5–32768seconds.
Holdtime Multiplier	Select the multiplier on the transmit interval to assign to TTL (range 2–10, default = 4).
Reinitialization Delay	Select the delay before a re-initialization (range 1–10 seconds, default = 2).
Transmit Delay	Select the delay after an LLDP frame is sent (range

	1–8192 seconds, default = 3).
Apply	Save the settings or changes to the switch.

3.8.1.2 LLDP Port Setting

Function name:

LLDP Port Setting

Function description:

Select specified port or all ports to configure LLDP state.

Parameter description:

LLDP Port Configuration

Port Select	Select specified port or all ports to configure LLDP state.

Dray Tek

State	Select the transmission state of LLDP port interface.
	● **Disable**: Disable the transmission of LLDP PDUs.
	● **RX Only**: Receive LLDP PDUs only.
	● **TX Only**: Transmit LLDP PDUs only.
	TX&RX: Transmit and receive LLDP PDUs both.

Optional TLVs Selection

Port Select	Select specified port or all ports to configure optional TLVs.
	Within data communication protocols, optional information may be encoded as a type-length-value or TLV element inside a protocol. TLV is also known as tag-length value.
	The type and length are fixed in size (typically 1-4 bytes), and the value field is of variable size.
Optional TLV Select	Select the LLDP optional TLVs to be carried (multiple selection is allowed).
	● System Name
	● Port Description
	● System Description
	● System Capability
	● 802.3 MAC-PHY
	● 802.3 Link Aggregation
	● 802.3 Maximum Frame Size
	● Management Address
	● 802.1 PVID

VLAN Name TLV VLAN Selection

Port Select	To carry VLAN information for LLDP to identify and place a device (like IP phone) on the correct VLAN meant for it, automatically.
	Select specified port or all ports to configure VLAN Name.
VLAN Select	Select the VLAN Name ID to be carried (multiple selection is allowed).
Apply	Save the settings or changes to the switch.

3.8.1.3 LLDP Local Device

Function name:

LLDP Local Device

Function description:

This page is used to view LLDP local device information. Click "Detail" on the page to view detailed information of the selected port.

3.8.1.4 LLDP Remote Device

Function name:

LLDP Remote Device

Function description:

This page is used to view LLDP neighbors information.

Parameter description:	
Detail	Click "Detail" to view selected neighbor detailed information.

3.8.1.5 LLDP Overloading

Function name:

LLDP Overloading

Function description:

Parameter description:

Interface	This label shows the port you are viewing.
Total (Bytes)	This field displays the total in bytes.
Left to Send (Bytes)	This field displays what is left to send in bytes.
Status	This field displays whether the Switch is overloading or not.
Mandatory TLVs	This field displays how many bytes used by mandatory TLVs.
802.3 TLVs	This field displays how many bytes used by 802.3 TLVs.
Optional TLVs	This field displays how many bytes used by optional TLVs.
802.1 TLVs	This field displays how many bytes used by 802.1 TLVs.

3.8.2 SNMP

Simple Network Management Protocol (SNMP) is an "Internet-standard protocol for managing devices on IP networks". Devices that typically support SNMP include routers, switches, servers, workstations, printers, modem racks and more.

SNMP is used mostly in network management systems to monitor network-attached devices for conditions that warrant administrative attention.

SNMP is a component of the Internet Protocol Suite as defined by the Internet Engineering Task Force (IETF). It consists of a set of standards for network management, including an application layer protocol, a database schema, and a set of data objects.

An SNMP-managed network consists of three key components:

● Managed device

● Agent — software which runs on managed devices

● Network management station (NMS) — software which runs on the manager

A managed device is a network node that implements an SNMP interface that allows unidirectional (read-only) or bidirectional (read and write) access to node-specific information. Managed devices exchange node-specific information with the NMSs. Sometimes called network elements, the managed devices can be any type of device, including, but not limited to, routers, access servers, switches, bridges, hubs, IP telephones, IP video cameras, computer hosts, and printers.

An agent is a network-management software module that resides on a managed device. An agent has local knowledge of management information and translates that information to or from an SNMP-specific form.

A network management station (NMS) executes applications that monitor and control managed devices. NMSs provide the bulk of the processing and memory resources required for network management. One or more NMSs may exist on any managed network.

3.8.2.1 SNMP Setting

Function name:

SNMP Setting

Function description:

Parameter description:

State	SNMP daemon state:
	● Select **Enabled** to activate SNMP daemon.
	● Select **Disabled** to not use SNMP daemon.
Apply	Save the settings or changes to the switch.

3.8.2.2 SNMP Community

Function name:

SNMP Community

Function description:

Dray Tek

SNMP Community

Community Setting

Community Name	Access Right
	⦿ read-only ○ read-write

[Add]

▾ Community Status

No.	Community Name	Access Right	Action

Parameter description:

Community Name	Enter a Community string. This will act as a password for requests from the management station.
Access Right	SNMP community type: ● **Read-Only:** Read all objects only, it can allow the SNMP manager using this string to collect information from the switch. ● **Read-Write:** Read and write all objects, it can allow the SNMP manager using this string to create or edit MIBs (configure settings on the switch).
Add	Click **Add** to add any other community.
Delete	Click **Delete** to remove any selected community strings.

3.8.2.3 SNMP Trap Host

Function name:

SNMP Trap Host

Function description:

This page allow user to add or delete SNMP trap receiver IP address and community name.

SNMP Trap Host

Trap Host Setting

IP Address	Community Name	Version
	▾	v1 ▾

[Add]

▾ Trap Host Status

No.	IP Address	Community Name	Version	Action

Parameter description:

IP Address	Enter the IP addresses to send your SNMP traps to.
Community Name	Enter a Community string, which is the password sent

	with each trap to the SNMP manager.
Version	Indicates the SNMP trap supported version. Possible versions are:
	● **v1**: Set SNMP trap supported version 1.
	● **v2c**: Set SNMP trap supported version 2c.
Add	Click **Add** to add any trap receiver.
Delete	Click **Delete** to remove any selected trap receiver entries.

3.9 Diagnostics

Use the Diagnostics pages to configure settings for the switch diagnostics feature or operating diagnostic utilities.

3.9.1 Cable diagnostics

3.9.1.1 Copper Test

Function name:

Copper Test

Function description:

Parameter description:

Port	The Selected Port ID.
Copper Test	Click it to start the test.

3.9.2 Ping Test

Function name:

Ping Test

Function description:

Parameter description:

IP Address	Enter the IP addresses of the test destination.
Count	It displays how many times to send ping request packet.
	Enter a number between 1 and 5 as the count and the default configuration is 4.
Interval	It displays time interval between each ping request packet.
	Enter a number between 1 and 5 as the interval and the default configuration is 1.
Size	It displays the size of ping packet.
	Enter a number between 0 and 5120 as the size and the default configuration is 56.
Ping Results	After ping finished, results will show in this field.
Apply	Save the settings or changes to the switch.

3.9.3 IPv6 Ping Test

Function name:

IPv6 Ping Test

Function description:

Parameter description:

IPv6 Address	Enter the IPv6 addresses of the test destination.
Count	It displays how many times to send ping request packet.
	Enter a number between 1 and 5 as the count and the default configuration is 4.
Interval	It displays time interval between each ping request packet.
	Enter a number between 1 and 5 as the interval and the default configuration is 1.
Size	It displays the size of ping packet.
	Enter a number between 0 and 5120 as the size and the default configuration is 56.
Ping Results	After ping finished, results will show in this field.
Apply	Save the settings or changes to the switch.

Dray Tek

3.9.4 Logging Setting

3.9.4.1 Logging Service

Function name:

Logging Service

Function description:

It is used to display the switch logs.

Parameter description:

Logging Service	Enable / disable logging system.
Apply	Save the settings or changes to the switch.

3.9.4.2 Local Logging

Function name:

Local Logging

Function description:

It is used to display the switch logs.

Parameter description:

Target	Select the target to store log message **Buffered**: Store log messages in device buffer. All log messages will disappear after system reboot. **FLASH**: Store log messages in FLASH. All log messages will not disappear after system reboot.
Severity	Select severity of log messages which will be stored.
Status	It displays the status of local log settings.
Delete	Click **Delete** to delete the target chose.
Apply	Save the settings or changes to the switch.

3.9.4.3 Remote Logging

Function name:

Remote Logging

Function description:

This page allows user to configure remote logging server information. The configured result will be displayed on Remote Logging Setting Status table.

Parameter description:

Server Address	The IP address of remote log server.
Server Port	Enter a number between 1 and 65535 as the server port.
Severity	Select severity of log messages which will be sent.
Facility	Select facility of log messages which will be sent.
Apply	Save the settings or changes to the switch.

3.9.5 Factory Default

Function name:

Factory Default

Function description:

It is used to restore the switch back to the factory defaults.

Factory Default

Restore

Parameter description:	
Restore	Restore all switch configurations to the factory defaults.

3.9.6 Reboot Switch

Function name:

Reboot Switch

Function description:

It is used to restart the switch without physically turning the power off.

Reboot Switch

Reboot

Parameter description:	
Reboot	Reboot the switch.

3.10 Maintenance

3.10.1 Backup Manager

Function name:

Backup Manager

Function description:

This page allows user to backup the firmware image or configuration file on the switch to remote TFTP server or host file system through HTTP protocol.

Backup files with TFTP Page

Backup files with HTTP Page

Parameter description:

Backup Method	Select backup method: ● **TFTP**: Use TFTP to backup. ● **HTTP**: Use HTTP to backup.
Server IP	IP address of the TFTP server. If the TFTP backup method is selected, the IP address of the TFTP server must be assigned.
Backup Type	Select backup type: ● **Image**: Firmware image of current system. ● **Running Configuration**: Running Configuration file. ● **Startup Configuration**: Startup Configuration file.
Backup	Click Backup to save the switch configuration/image to the local address specified.

3.10.2 Upgrade Manager

Function name:

Upgrade Manager

Function description:

This page allows user to upgrade new firmware image or configuration file to the switch from remote TFTP server or select file from web browser.

Upgrade with TFTP Page

Upgrade with HTTP Page

Parameter description:

Upgrade Method	Select upgrade method: ● **TFTP:** Use TFTP to upgrade. ● **HTTP:** Use HTTP to upgrade.
Server IP	IP address of the TFTP server. If the TFTP upgrade method is selected, the IP address of the TFTP server must be assigned.
File Name	Firmware image or configuration file name on remote TFTP server. If the TFTP upgrade method is selected, the file name must be specified.
Browse File	If the HTTP upgrade method is selected, the browse file field allows you to select any file on host operating system.
Upgrade Type	Select upgrade type: ● **Image:** Firmware image of current system.

	● **Running Configuration**
	● **Startup Configuration**
Upgrade	Click **Upgrade** to update the file specified above and install the new firmware.

3.10.3 Configuration Manager

Function name:

Configuration Manager

Function description:

This page allows user to save either the running configuration or the startup configuration to the existing configuration file as the startup configuration.

Parameter description:

Source File	Select upgrade method
	● **Running configuration**: Running configuration file.
	● **Startup configuration**: Startup configuration file.
Destination File	Select Upgrade Type.
	● **Startup Configuration**: Startup configuration file
Apply	Click **Apply** to save the running or the startup configuration to the startup configuration file.

Dray Tek

3.10.4 Account Manager

Function name:

Account Manager

Function description:

This page allows user to add or delete local user on switch database for authentication. The default user is "admin".

Parameter description:

Username	Enter your username for new account.
Password Type	Select password type for new account: ● **Clear Text:** Password without encryption. ● **Encrypted:** Password with encryption. ● **No Password:** No password for new account.
Password	If the password type is not "No Password", the password must be specified.
Retype Password	Retype password to make sure the password is exactly you typed before in "Password" field.
Privilege Type	Select privilege level for new account. ● **Admin:** Allow to change switch settings. ● **User:** See switch settings only. Not allow to change it.
Apply	Save the settings or changes to the switch.
Modify	Click **Delete** to delete the added user.

4 **Trouble Shooting**

4.1 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

4.2 Q & A

Q1.How to configure the switch to support loop detection:

Answer:

Vigor switch support loop detection in default. If you want to disable loop detection, you can simply set STP --> STP Global Setting --> Global Setting --> BPDU Forward --> flooding to filter.

Q2. Where is Rapid Spanning Tree, Where can I find it?

Answer:

RSTP equals to Rapid Spanning Tree. Please follow the following direction to choose it: STP --> STP Global Setting --> Global Setting --> Force Version --> RSTP.

DrayTek