Smarter. Greener. Together.

Industrial Automation Headquarters

Delta Electronics, Inc.
Taoyuan Technology Center
No.18, Xinglong Rd., Taoyuan City,
Taoyuan County 33068, Taiwan
TEL: 886-3-362-6301 / FAX: 886-3-371-6301

Asia

Delta Electronics (Jiangsu) Ltd.
Wujiang Plant 3
1688 Jiangxing East Road,
Wujiang Economic Development Zone
Wujiang City, Jiang Su Province, P.R.C. 215200
TEL: 86-512-6340-3008 / FAX: 86-769-6340-7290

Delta Greentech (China) Co., Ltd.
238 Min-Xia Road, Pudong District,
ShangHai, P.R.C. 201209
TEL: 86-21-58635678 / FAX: 86-21-58630003

Delta Electronics (Japan), Inc.
Tokyo Office
2-1-14 Minato-ku Shibadaimon,
Tokyo 105-0012, Japan
TEL: 81-3-5733-1111 / FAX: 81-3-5733-1211

Delta Electronics (Korea), Inc.
1511, Byucksan Digital Valley 6-cha, Gasan-dong,
Geumcheon-gu, Seoul, Korea, 153-704
TEL: 82-2-515-5303 / FAX: 82-2-515-5302

Delta Electronics Int'l (S) Pte Ltd.
4 Kaki Bukit Ave 1, #05-05, Singapore 417939
TEL: 65-6747-5155 / FAX: 65-6744-9228

Delta Electronics (India) Pvt. Ltd.
Plot No 43 Sector 35, HSIIDC
Gurgaon, PIN 122001, Haryana, India
TEL : 91-124-4874900 / FAX : 91-124-4874945

Americas

Delta Products Corporation (USA)
Raleigh Office
P.O. Box 12173,5101 Davis Drive,
Research Triangle Park, NC 27709, U.S.A.
TEL: 1-919-767-3800 / FAX: 1-919-767-8080

Delta Greentech (Brasil) S.A.
Sao Paulo Office
Rua Itapeva, 26 - 3° andar Edificio Itapeva One-Bela Vista
01332-000-São Paulo-SP-Brazil
TEL: 55 11 3568-3855 / FAX: 55 11 3568-3865

Europe

Delta Electronics (Netherlands) B.V.
Eindhoven Office
De Witbogt 20, 5652 AG Eindhoven, The Netherlands
TEL : +31 (0)40-8003800 / FAX : +31 (0)40-8003898

2017-01-12

DVS Managed Industrial Rack Mount Ethernet Switch User Manual

DVS Managed Industrial Rack Mount Ethernet Switch User Manual

Product Model:
DVS-328 series

www.deltaww.com

Smarter. Greener. Together.

DVS Managed Industrial

Rack Mount Ethernet Switch User Manual

Table of Contents

Chapter 1 Introduction

Table of Contents

FCC Interference Statement

This equipment has been tested and found to comply with the limits for a class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.
This equipment generates radio frequency signal and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:
---Reorient or relocate the receiving antenna.
---Increase the separation between the equipment and receiver.
---Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
---Consult the dealer or an experienced radio/TV technician for help.

CE Declaration of Conformity

The DVS series switches are CE certificated products. They could be used in any kind of the environments under CE environment specification. For keeping more safe application, we strongly suggest to use the CE-compliant industrial enclosure products.

1.1 Feature

Thank you for purchasing the DVS Managed Industrial Ethernet Switches. The DVS series switches including Unmanaged and Managed switches. Except the DVS-005I00, the DVS series switches are equipped with the intelligent alarm function, and allow the wide range of operating temperature (-40 to 85℃ or -20 to 70℃). The DVS series switches are designed to support the application in any rugged environment and comply with UL, CE and FCC standards.

1.1.1 High Performance Network Technology

- 10/100Base-T(X) (RJ45), 10/100/1000Base-T (RJ45), 100/1000Base-SFP Fiber
- IEEE 802.3/802.3u/802.3ab/802.3z
- Auto negotiation speed
- Auto MDI/MDI-X

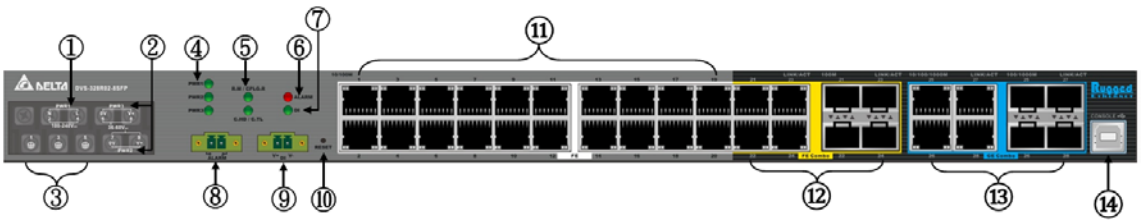
1.1.2 Industrial Grade Reliability

- 1 set of AC power input and 2 set of DC power inputs
- 1 set of Digital Input
- 1 set of Relay Alarm

1.1.3 Robust Design

- Operating temperature: -20~70℃
- Storage temperature: -40~85 ℃
- Humidity: 0%~95% (non-condensing)
- Protection: IP40

1.1.4 Front Panel Ports and LEDs



No	Description
1	AC power input.
2	Redundant DC power input
3	Grounding Screw
4	Power LED
5	ONE RING / ONE CHAIN / ONE COUPLING LED
6	Alarm LED
7	DI LED
8	Relay alarm port
9	Digital Input
10	Reset button
11	Fast Ethernet ports
12	Fast Ethernet Combo ports
13	Gigabit Ethernet Combo ports
14	USB CONSOLE port

1.2 SFP Module Installation

Insert:
Insert SFP Module into the SFP combo port.

Remove:
Pull the tab on the module, and then pull out it.

Note:
Delta has LCP-155 and LCP-1250 series SFP module. DVS switch can promise 100% compatible with Delta SFP module.

Note:
The actual link distance of a particular fiber optic link given the optical budget, the number of connectors and splices, and cabling quantity. Please measure and verify the actual link loss values once the link is established to identify any potential performance issues.

1.3 Package Checklist

- Delta DVS series Managed Rack Mount Ethernet Switch
- Protective Caps for unused RJ45 ports and fiber ports (inserted to the switch)
- USB Type A to Type B console cable
- User manual and software CD
- Instruction Sheet
- Rack bracket*4
- M4 screw*20
- M5 screws*6
- T4 screw*6 and anchor screw*6
- Rubber feet*4
- Rubber Plug*16(Inserted to the switch)

1.4 MTBF (Mean Time Between Failures)

More than 1,100,000 hours.

MEMO

Chapter 2 User Interface Introduction

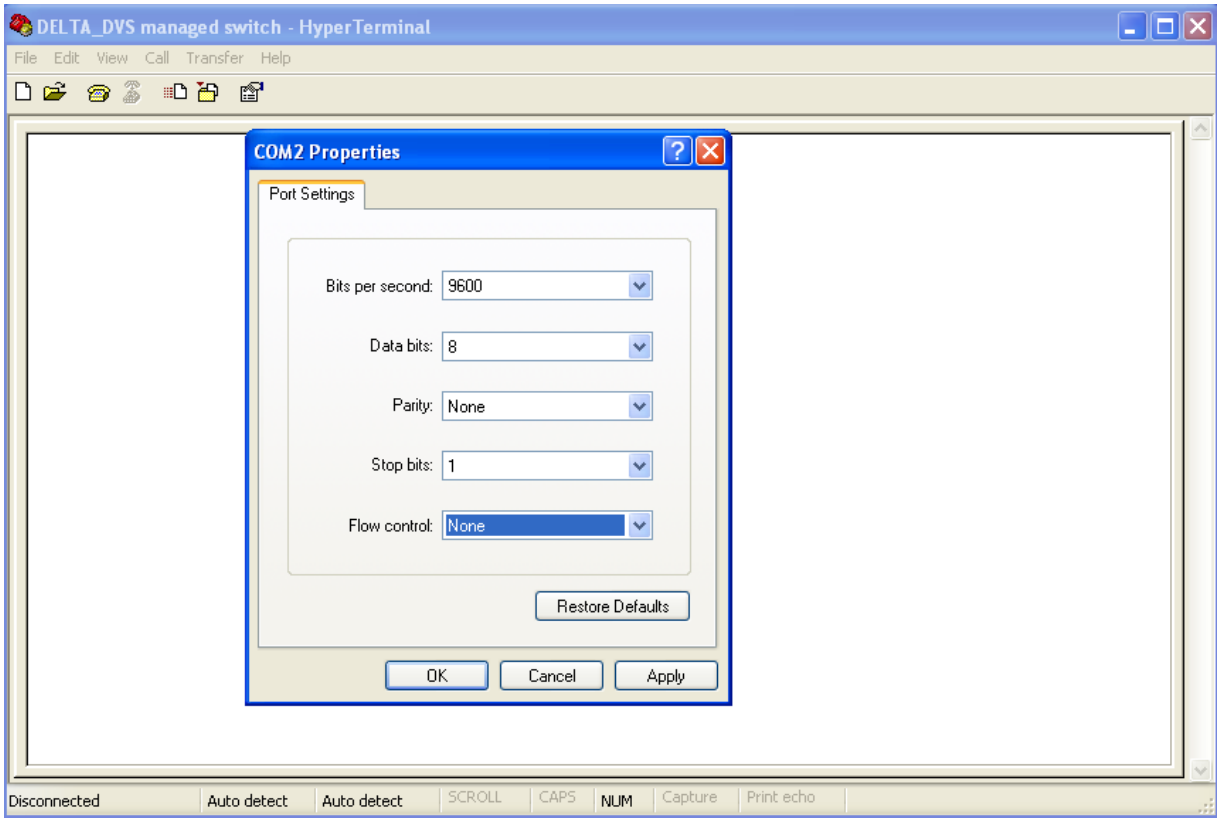
Table of Contents

2.1 USB Console Configuration

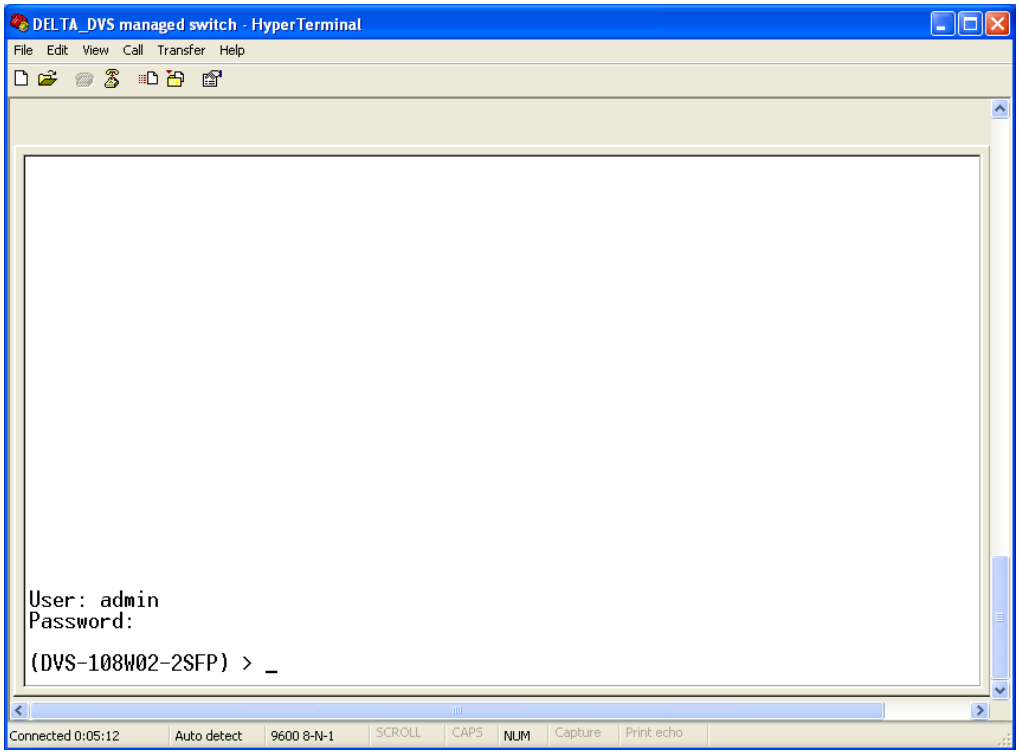
A Delta switch supports configuration using the CLI interface, available on the USB port with the baud rate 9600. You can use the terminal software to connect to a Delta switch. The inactivity timeout value on a serial port connection can be configured between 0 and 160 minutes. (Value 0: disable the timeout.)

1. Open the terminal software, and select an appropriate COM port for **Console Connection**, **9600** for **Baud Rate**, **8** for **Data Bits**, **None** for **Parity**, and **1** for **Stop Bits, None** for **Flow Control**.

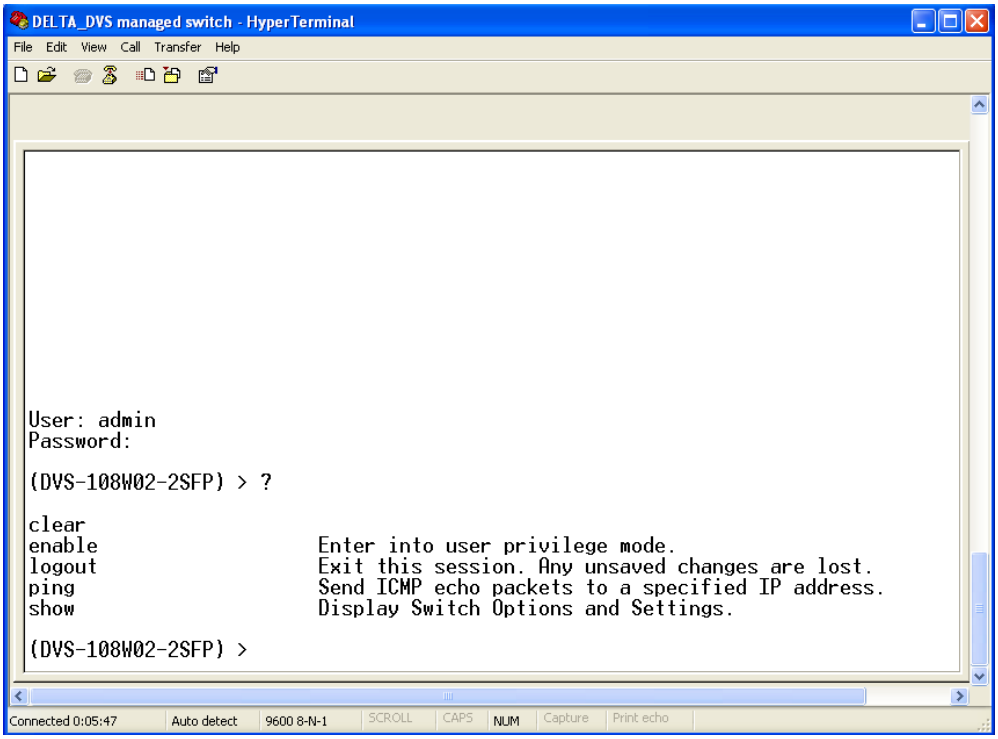
Note:
The Windows 7 system does not support Hyper Terminal. If you need it, you can download the terminal software to use it.



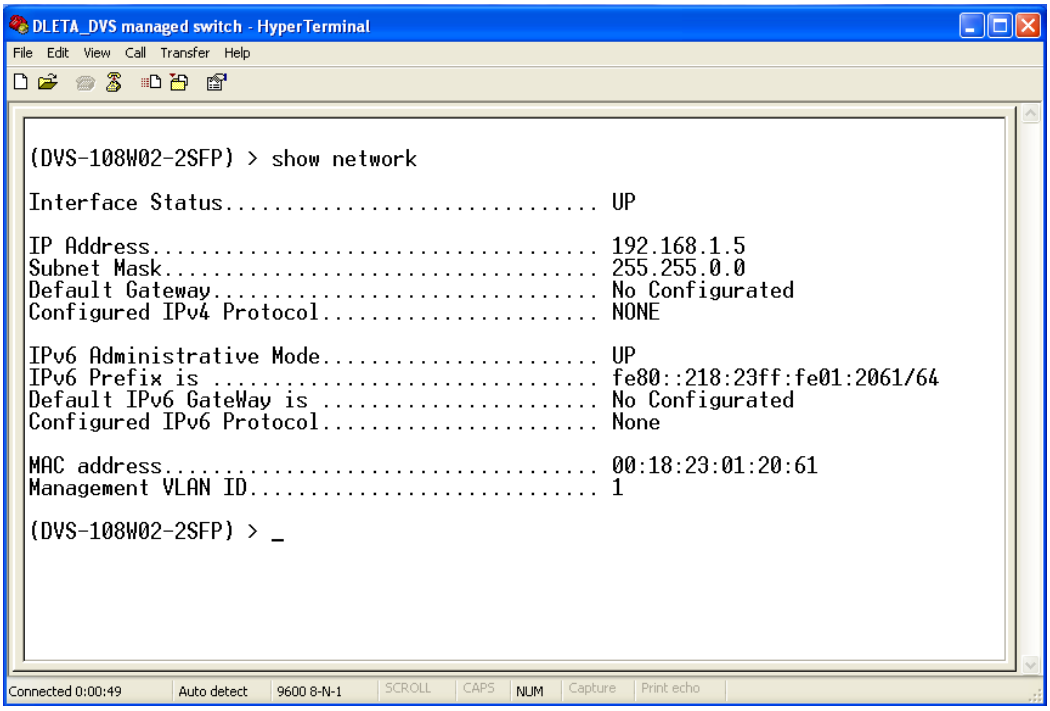
2. The user name and the password are the same as Web Browser. The default user name is “admin”, and the password is blank.



You can use “?” to list the commands.



Example 1:
There is a DHCP server in your environment, and the Delta switch can get an IP address from the DHCP server. If you don't want to check the IP address from the DHCP server, then you can use the USB console cable to login to the Delta switch. Using the "show network" command can display the IP address information of the Delta switch.



Example 2:
If you want to change the network configuration protocol from DHCP mode to static mode, using CLI commands to change the protocol and setting a static IP address and a subnet mask.

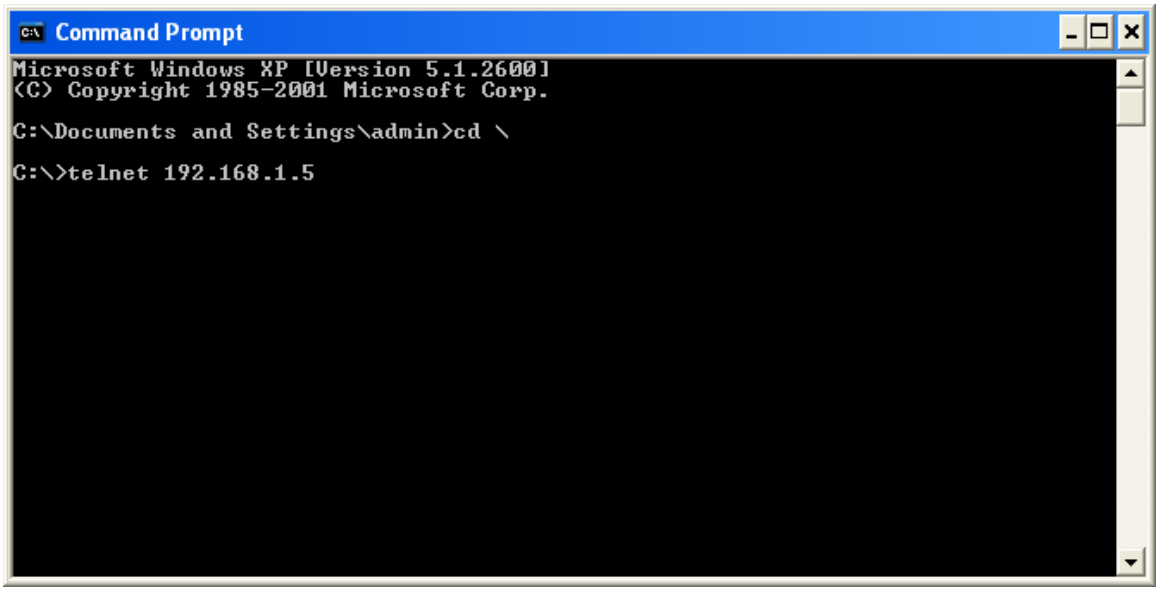
```
(DVS-108W02-2SFP) > enable
(DVS-108W02-2SFP) # configure terminal
(DVS-108W02-2SFP) (config)# interface vlanmgmt
(DVS-108W02-2SFP) (config-if)# no ip address
(DVS-108W02-2SFP) (config-if)# ip address 10.10.10.1 255.255.255.0
(DVS-108W02-2SFP) (config-if)# exit
(DVS-108W02-2SFP) (config)# exit
(DVS-108W02-2SFP) # save
Building configuration ...
[OK]
(DVS-108W02-2SFP) #
```

Note:
Before you use the USB console configuration, please make sure that you have installed the USB driver. You can find the driver in the CD package.

2.2 Telnet Console Configuration

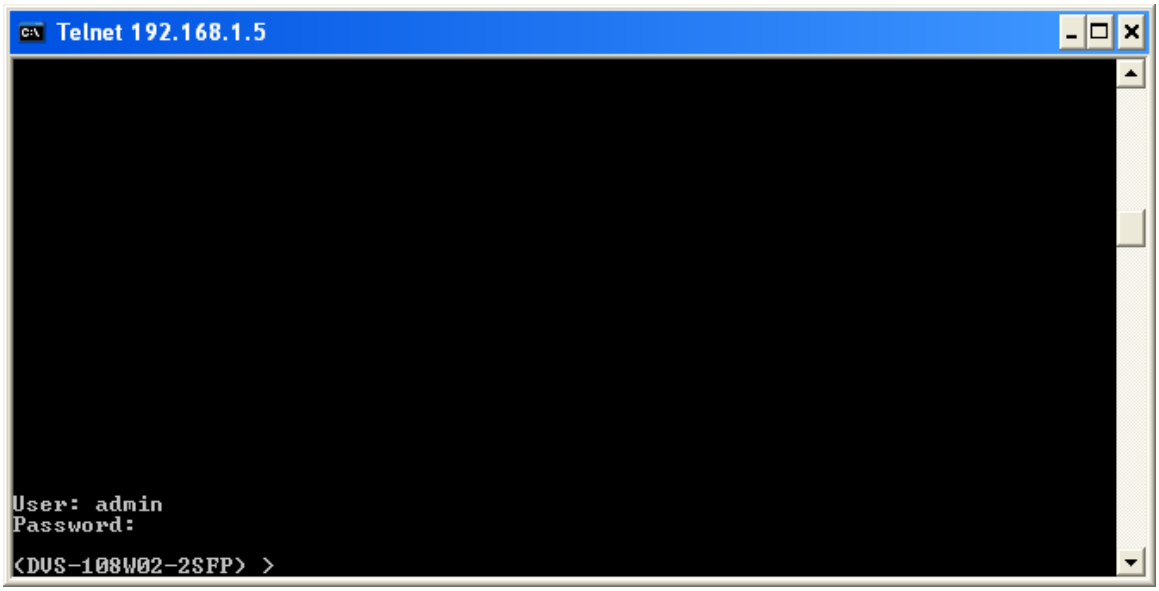
A Delta switch supports the telnet server function; it can be globally enabled or disabled. The user can use all CLI commands over a telnet session. The maximum number of inbound telnet sessions allowed on the switch can be configured to 0-5. The inactivity timeout value for the incoming Telnet sessions for the switch can be configured to 1-160 minutes. The login authentication supports the local user method or the remote user method which is configured. When the login authentication is the remote user method, it supports RADIUS and TACACS+.

1. Open a Command Prompt window and input “telnet 192.168.1.5” to login to a Delta switch.



2. After entering a user name and a password, you can use the CLI command to control the switch.

Note:
The default user name is “admin” and the password is blank.

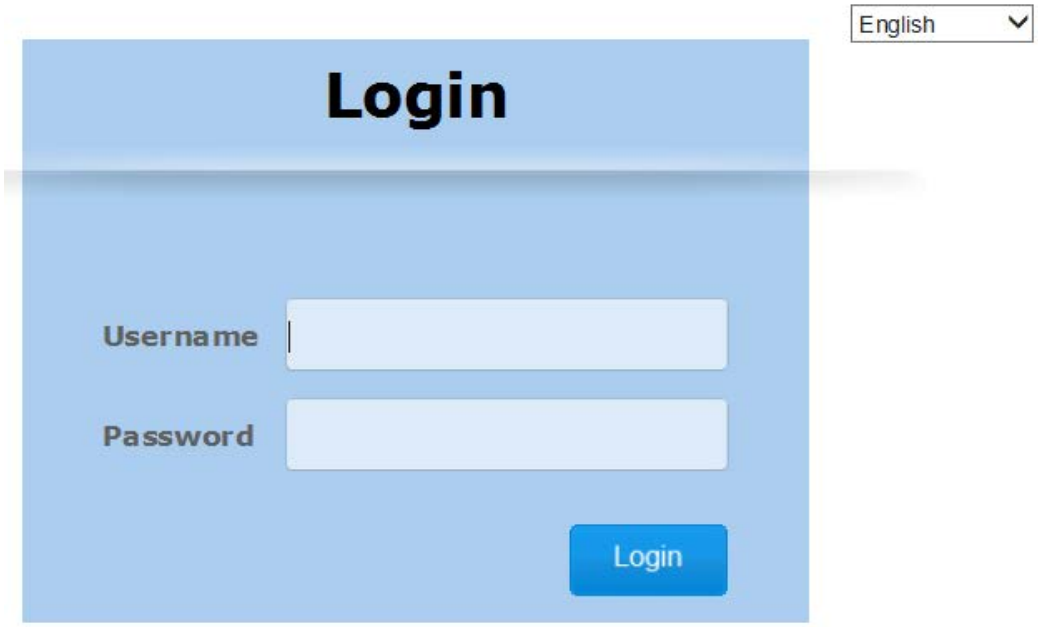


2.3 Web Browser Configuration

The Delta switch supports a friendly GUI for administrators to configure the switch. Admin user can monitor the port status of a Delta switch, and configure the settings of each function via the web interface.
The switch provides an admin user of high access level to create lower access level of a normal user

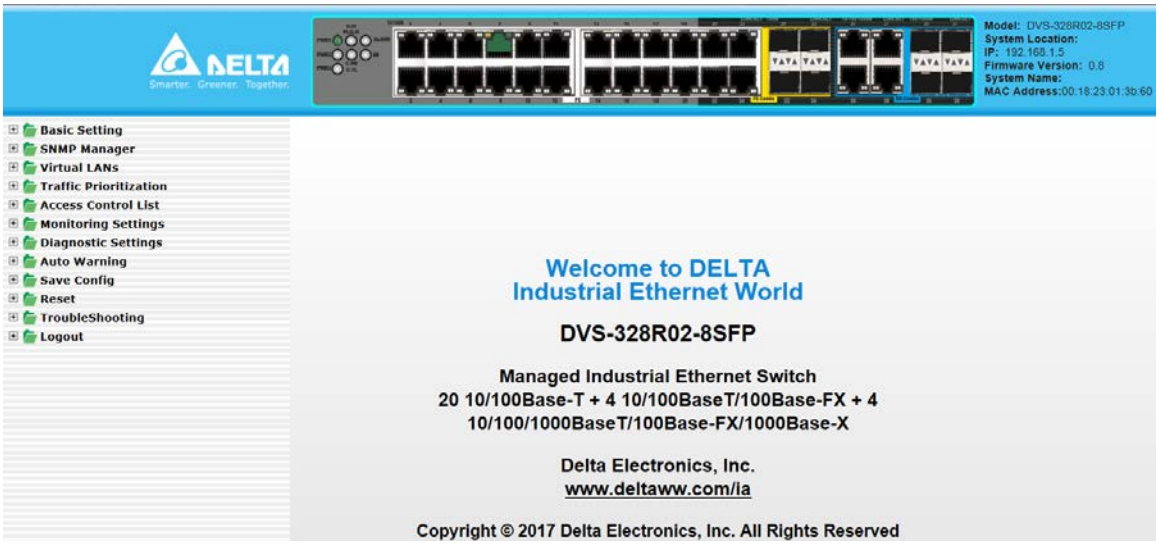
1. Open a web browser and connect to the default IP address 192.168.1.5. Enter a user name and a password. (The default user name is “admin” and the password is blank.)
   You can also change the language into English or Simplified Chinese via the drop-down list on the upper right.

   Note: The default user name “admin” is in the lowercase not uppercase.

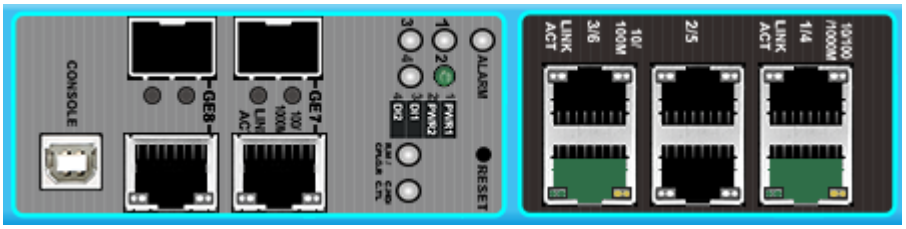


2. When an admin user logging in, the menu tree will show up the complete functions.You can see as below:

When a normal user loggin in, the menu tree will show up the part of functions.You can see as below:



3. The port status and the LED status on the switch can be monitored in the top frame. The status of the Delta switch in the top frame displays the real status with the physical switch synchronously.



MEMO

Chapter 3 Featured Functions

Table of Contents

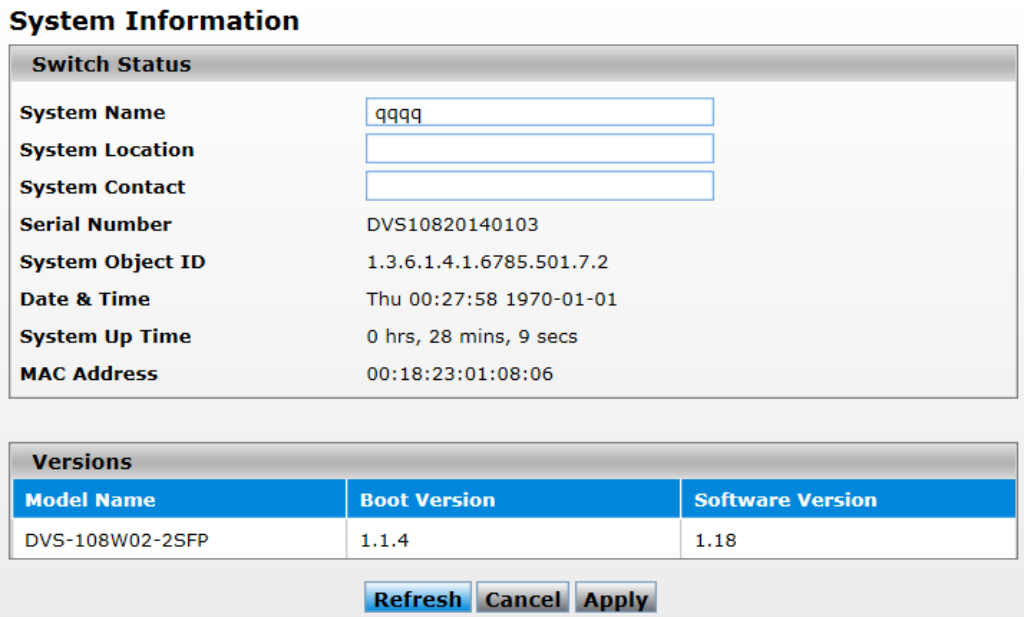
3.1 Basic Setting

The basic setting group includes the most common settings, and an administrator can maintain the control of the Delta switch in this group.

> **IMPORTANT:**
> **Make sure that you save the configuration in the Save Configuration page after you have applied the configuration changes. (Save Config→Save Configuration) If you do not save the configuration, then the configuration will be cleared after the switch is rebooted.**

3.1.1 System Information

System Information includes the basic switch status items and the version .It also displayed in the banner of the GUI. These informations can help the administrator identify the switch in the network.



Switch Status

Description	Factory default
System Name	
Input the system name of the switch.	None
System Location	
Input the system location of the switch.	None
System Contact	
Input the system contact of the switch.	None
Serial Number	
The serial number of the switch.	Fixed
System Object ID	
The based object ID for the Management Information Base (MIB) of the switch.	Fixed
Date & Time	
The current date and time.	None
System Up Time	
The time of hours, minutes, and seconds since the switch was last started.	None
MAC Address	
The MAC address of the switch.	Fixed

Versions

Description	Factory default
Model Name	
The model name of the switch.	Model Name
Boot Version	
The boot version of the switch.	Boot Version
Software Version	
The software version of the switch.	Software Version

3.1.2 Network Interface

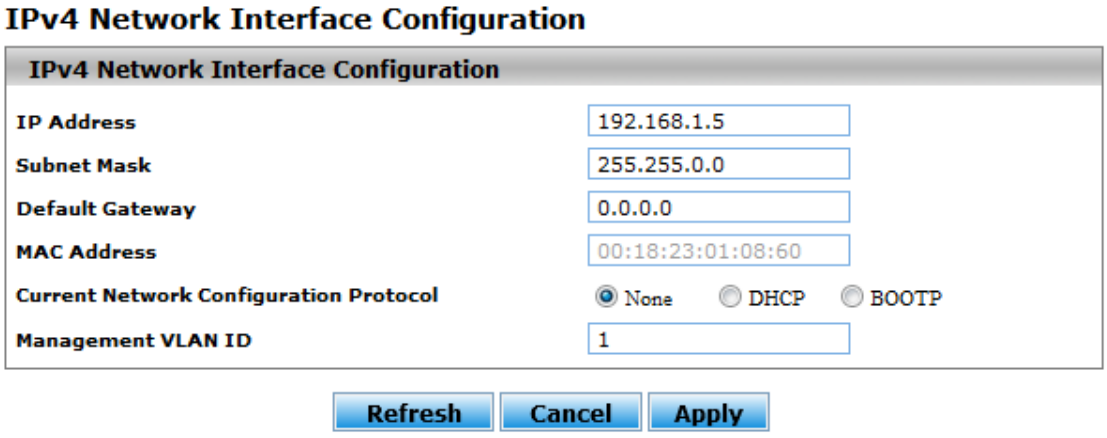
The network interface on the network device is a logical interface. Each network device must have one or more interfaces to connect with other network devices. But the configuration of the network interface does not affect the traffic which is forwarded.

3

3.1.2.1 IPv4 Network Configuration

You can configure a static IP address, a subnet mask and a default gateway for the switch. Or you can enable DHCP mode or BOOTP mode for receiving a dynamic IP address, a subnet mask and a default gateway. If you enable DHCP mode or BOOTP mode, but there is no DHCP or BOOTP server in the network, the default link local IP address will be **169.254.100.100**.

Note:
The default Current Network Configuration Protocol is None. And the default IP address is **192.168.1.5**.

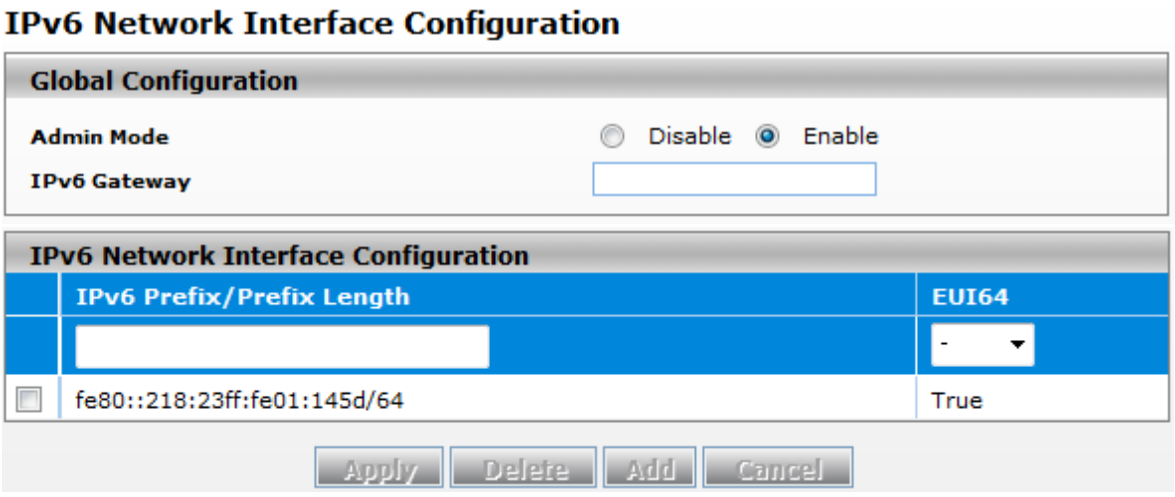


IPv4 Network Interface Configuration

Description	Factory default
IP Address	
Input the IP address of the IPv4 network interface. **Note:** After you change the IP address and clicking Apply, we suggest you to login again, and making sure the URL is the latest IP address.	192.168.1.5
Subnet Mask	
Input the IP subnet mask of the IPv4 network interface.	255.255.0..
Default Gateway	
Input the default gateway of the IPv4 network interface.	0.0.0.0.
MAC Address	
This field displays the MAC address of the switch.	MAC address
Current Network Configuration Protocol	
Select one item to specify how the switch gets its IP information: • **None**: Specify the static IP address information. • **DHCP**: The IP information of the switch is assigned by a Dynamic Host Configuration Protocol (DHCP) server on the network. • **BOOTP**: The IP information of the switch is assigned by a Bootstrap Protocol (BOOTP) server on the network.	None
Management VLAN ID	
Input the management VLAN ID in the range from 1 to 4094.	1

3.1.2.2 IPv6 Network Configuration

If you need to configure a global IPv6 address, please follow the standard format: “IPv6 Prefix/Prefix Length”. Example: “1001:2002:3003::7007:8008/64”



Global Configuration

Description	Factory default
Admin Mode	
Specify the IPv6 administrative status of the network interface by selecting one item: • **Disable**: IPv4 only mode. Only support IPv4, not support IPv6. • **Enable**: IPv4 / IPv6 mode. Support both IPv4 and IPv6.	Enable
IPv6 Gateway	
Input the IPv6 address of the IPv6 gateway.	None

IPv6 Network Interface Configuration

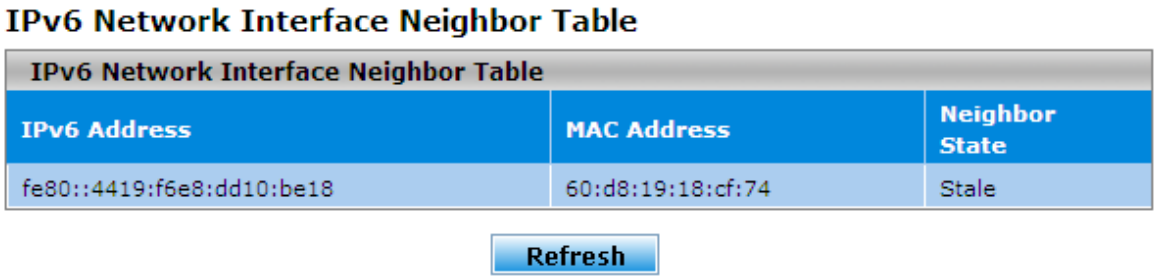
Description	Factory default
IPv6 Prefix / Prefix Length	
Enter the IPv6 address followed by a slash and then the prefix length of the network interface.	IPv6 address
EUI64	
Specify whether the IPv6 address is in the 64-bit extended unique identifier (EUI-64) format: • **True**: The IPv6 address is in the EUI-64 format. • **False**: The IPv6 address is not in the EUI-64 format.	None

3

Note:
An IPv6 address in the EUI-64 format is an automatically self-assigned unique 64-bit IPv6 interface identifier. You do not need to manually configure such an IPv6 address, and it is not assigned by a DHCP server.

3.1.2.3 IPv6 Network Neighbor

The IPv6 network interface neighbor table can display the neighbor IPv6 address.



IPv6 Network Interface Neighbor Table

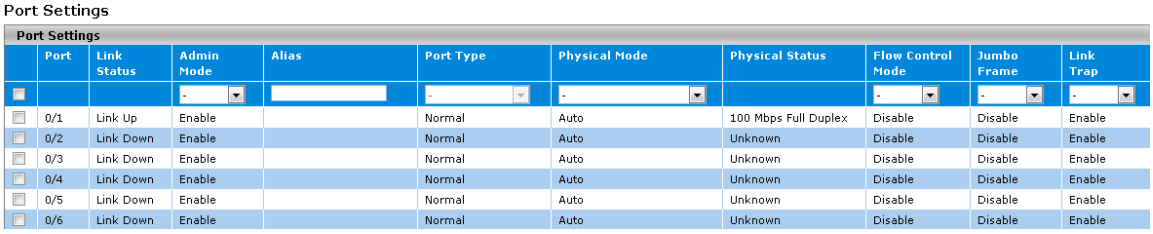
Description	Factory default
IPv6 Address	
The IPv6 address of the neighbor.	None
MAC Address	
The MAC address of the neighbor.	None
Neighbor State	
The status of the neighbor: • **Static:** The neighbor has a static IP address. • **Reachable:** The neighbor was reached very recently (that is, within a period of tens of seconds). • **Incomplete:** The address resolution for the neighbor is in progress, but the link-layer address of the neighbor has not yet been determined. • **Stale:** The neighbor can no longer be reached. Until the traffic is sent to the neighbor, no attempt is made to verify it if it can be reached again. • **Delay:** The neighbor can no longer be reached. The traffic was recently sent to the neighbor, but neighbor solicitation probes are delayed because the confirmation that the neighbor can be reached might be received. • **Probe:** The neighbor can no longer be reached. Unicast neighbor solicitation probes are sent to verify whether the neighbor can be reached again. • **Unknown:** The status of the neighbor is unknown.	None

3.1.3 Port Settings

You can configure the basic port settings and LAG settings of the Delta switch in the Port Settings group.

3.1.3.1 Port Settings

You can configure and monitor the port status on this page.


Port Settings

Port Settings

	Port	Link Status	Admin Mode	Alias	Port Type	Physical Mode	Physical Status	Flow Control Mode	Jumbo Frame	Link Trap
			-		-	-		-	-	-
	0/1	Link Up	Enable		Normal	Auto	100 Mbps Full Duplex	Disable	Disable	Enable
	0/2	Link Down	Enable		Normal	Auto	Unknown	Disable	Disable	Enable
	0/3	Link Down	Enable		Normal	Auto	Unknown	Disable	Disable	Enable
	0/4	Link Down	Enable		Normal	Auto	Unknown	Disable	Disable	Enable
	0/5	Link Down	Enable		Normal	Auto	Unknown	Disable	Disable	Enable
	0/6	Link Down	Enable		Normal	Auto	Unknown	Disable	Disable	Enable

Port Settings

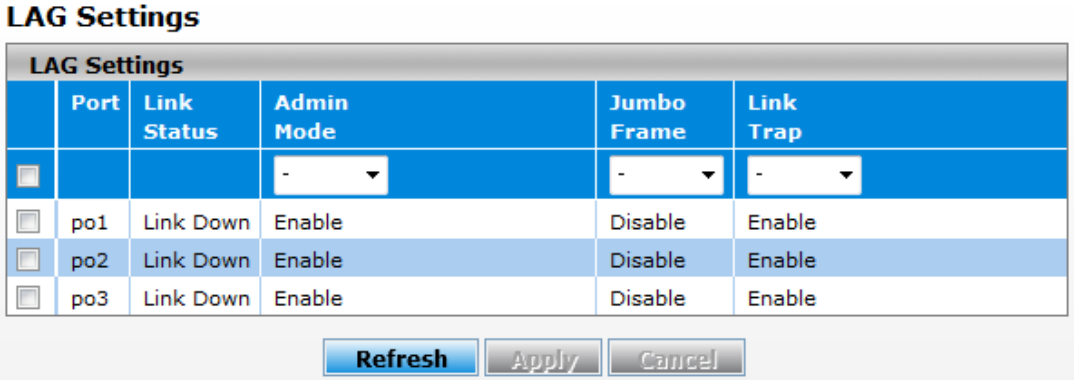
Description	Factory default
Port	
This field displays the interface number.	*interface number*
Link Status	
This field displays the connection of the interface. • **Link Up**: There is a network device connecting to the interface. • **Link Down**: No network device is connecting to the interface.	Link down
Admin Mode	
The administrative state of the interface: • **Enable**: The interface is switched on and the network device can connect to the interface. • **Disable**: The interface is switched off and the network device can not connect to the interface.	Enable
Alias	
Specify an alias for the port to help administrators differentiate between different ports. For example: Head port.	*None*
Port Type	
This field displays whether the interface is a member of a port channel: • **Trunk Member**: The interface is a member of a link aggregation group. • **Normal**: The interface is not a member of a link aggregation group (port channel). **Note:** If you add ports in the lag, the port type will show “Trunk Member”. The LAG configuration could be configured in Port Trunk.	Normal
Physical Mode	
Specify the speed capability of each interface: • **Auto**: The duplex mode and the speed of the interface are set by the auto-negotiation process. The interface can support the maximum capability: Full duplex and 1 Gbps or 100Mbps. • **10 Mbps Half Duplex**: Indicates that the interface works at 10 Mbps in the half duplex mode. • **10 Mbps Full Duplex**: Indicates that the interface works at 10 Mbps in the full duplex mode. • **100 Mbps Half Duplex**: Indicates that the interface works at 100 Mbps in the half duplex mode. • **100 Mbps Full Duplex**: Indicates that the interface works at 100 Mbps in the full duplex mode.	Auto
Physical Status	
This field displays the actual port speed and the duplex mode.	None
Flow Control Mode	

Description	Factory default
This field displays whether the flow control is enabled for the port: • **Enable**: The flow control is enabled. If the port buffers become full, the switch sends pause packets. • **Disable**: The flow control is disabled. If the port buffers become full, the switch does not send pause packets.	Disable
Jumbo Frame	
The field displays whether the jumbo frame is enabled for the port. • **Enable**: The jumbo frame is enabled. The switch supports a fixed jumbo frame size - 9000 bytes payload (9218 bytes frame) size. • **Disable**: The jumbo frame is disabled.	Disable
Link Trap	
Specify whether to send a trap when the interface link status changes: • **Enable**: When the link status changes, the switch sends a trap. This is the default setting. • **Disable**: When the link status changes, the switch does not send a trap.	Enable

3

3.1.3.2 LAG Settings

You can configure the LAG settings and monitor the LAG status on this page.



LAG Settings

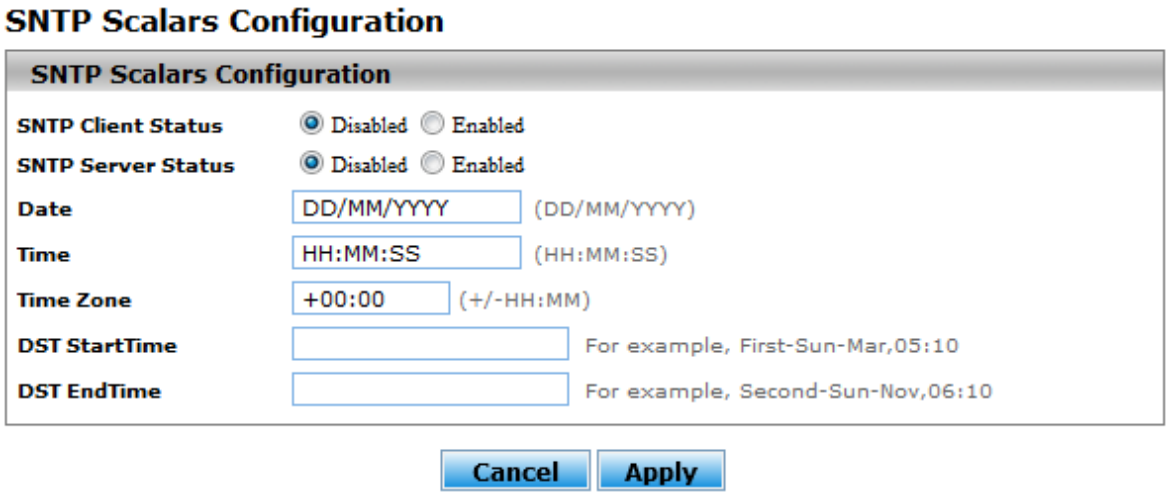
Description	Factory default
Port	
This field shows the interface number.	*interface number*
Link Status	
This filed shows the connection of the interface. • **Link Up:** The interface is connected to another device. • **Link Down:** The interface is not connected to another device.	Link Down
Admin Mode	
Specify the administrative state of the interface: • **Enable:** The interface is switched on and can be connected to another device. • **Disable:** The interface is switched off and can not be connected to another device.	Enable
Jumbo Frame	
The filed displays whether the jumbo frame is enabled for the port. • **Enable:** The jumbo frame is enabled. The switch supports a fixed jumbo frame size - 9000 byte payload (9018 byte frame) size. • **Disable:** The jumbo frame is disabled.	Disable
Link Trap	
Specify whether the switch sends a trap when the interface link status changes: • **Enable:** When the link status changes, the switch sends a trap. This is the default setting. • **Disable:** When the link status changes, the switch does not send a trap.	Enable

3.1.4 Time

The Delta managed switch supports SNTP (Simple Network Time Protocol). It can work as an SNTP client to get time from an SNTP or NTP server, and it also can work as an SNTP server to provide time service and send a time reply to a client.

3.1.4.1 SNTP Scalars Configuration

SNTP Scalars Configuration lets a user configure the time of the switch which can be gotten from the SNTP server. And it also can be configured manually.



SNTP Scalars Configuration

Description	Factory default
SNTP Client Status	
Specify whether the switch works as an SNTP client, and the switch will send an NTP request to the server which the user specify on the SNTP Unicast Server Configuration page. • **Enable**: The switch works as an SNTP client. • **Disable**: The switch does not work as an SNTP client.	Disable
SNTP Server Status	
Specify whether the switch works as an SNTP server. • **Enable**: The switch works as an SNTP server. • **Disable**: The switch does not work as an SNTP server.	Disable
Date	
The date parameter format is DD/MM/YYYY. When an SNTP client is disabled, you can manually set the date. When an SNTP client is enabled, the field is grayed out.	DD/MM/YYYY
Time	
The time parameter format is HH:MM:SS. When an SNTP client is disabled, you can mpinganually set the time. When an SNTP client is enabled, the field is grayed out.	HH:MM:SS
Time Zone	
The time zone setting format HH:MM is preceded by a plus (+) or minus (-). For example, for Taipei, enter +08:00. And it allows the conversion from GMT (Greenwich Mean Time) to the local time.	+00:00
DST StarTime	
Enter the daylight saving time (DST) start time. Specify the date and time in the following format: Week of the month-day of the week-month-HH:MM. For example, if DST starts on the first Saturday in May at 03:00 AM, enter the following	None

Description	Factory default
format: First-Sat-May-03:00.	
DST EndTime	
Enter the daylight saving time (DST) end time. Specify the date and time in the following format: Week of the month-day of the week-month-HH:MM. For example, if DST ends on the second Monday in December at 04:00 AM, enter the following format: Second-Mon-Dec-04:00.	None

Note:

1. After you have clicked Apply, the date and time are applied and the fields revert to their default setting of DD/MM/YYYY and HH:MM:SS.
2. The manual date and time setting will be lost after the switch is rebooted, even if you have saved the changes

3

3.1.4.2 SNTP Unicast Server Configuration

If you want to specify a known SNTP server, you can enter the IP address or DNS on this page.

SNTP Unicast Server Configuration

Description	Factory default
Forward Address Type	
Specify a type of SNTP server IP address: • **IPv4**: Use an IPv4 address to recognize an SNTP server. This is the default setting. • **IPv6**: Use an IPv6 address to recognize an SNTP server. • **DNS**: Use FQDN to recognize an SNTP server.	IPv4
Unicast Server IP Address	
Enter the server IPv4, IPv6 address or host name (FQDN). (Depend on the type you select in the Forward Address Type field.)	None
Unicast Server Type	
Specify a type of server by selecting Primary or Secondary from the drop-down list.	None
Last Updated	
This field displays the last time the SNTP unicast server updated its time information.	None
Tx Requests	
This field displays the number of SNTP transmit requests made by the switch since it was last rebooted.	None

Note:
We recommend that you add the SNTP unicast server for the Delta switch to synchronize the time. It can make sure that the time on the Delta switch is accurate.

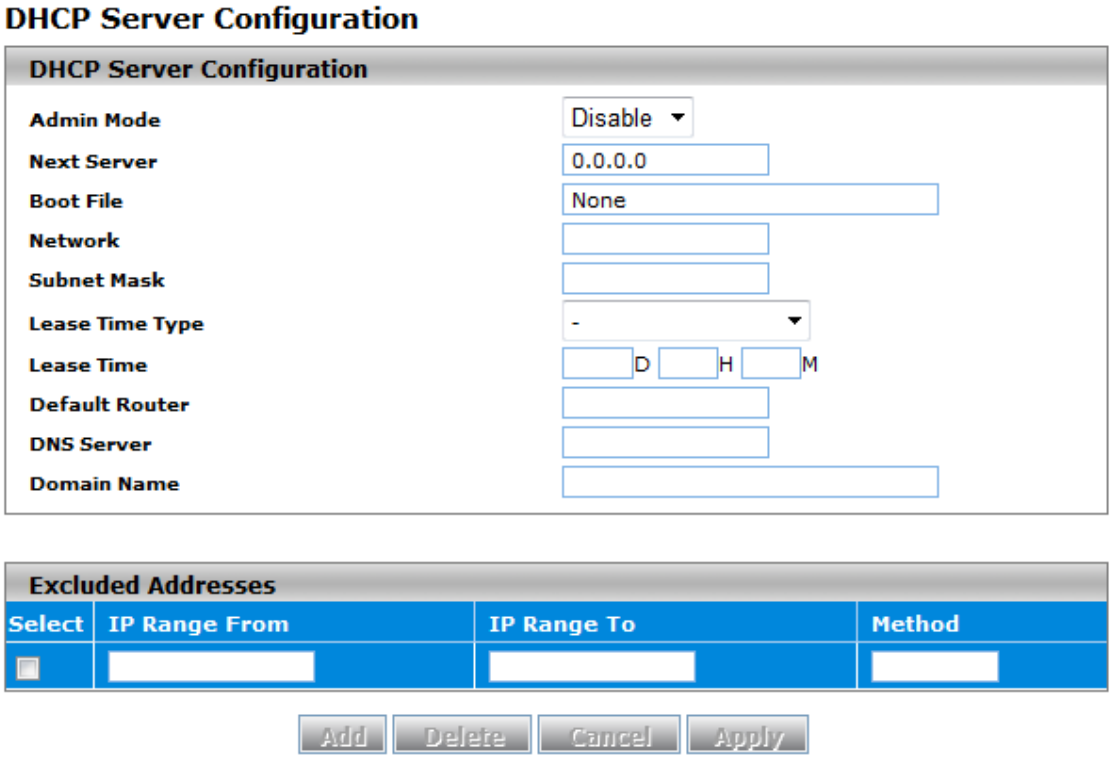
3.1.5 DHCP/BOOTP Settings

The Delta switch can function as a DHCP server, DHCP relay and DHCP L2 relay. If there is no DHCP server in your network, then you can enable a DHCP server function on the Delta switch. If there is a DHCP server in your network, then you can configure the Delta switch as a DHCP relay. If there is already a DHCP server and a DHCP relay in your network, or there are L2 devices between DHCP clients and relay agents, then you can configure the Delta switch as a DHCP L2 relay in this network.

3.1.5.1 DHCP Server

If the DHCP server is enabled on the switch, it can assign an IP address which is in the same network as the switch to the client.The Delta switch also supports the MAC Based DHCP Configuration and the Port Based DHCP Configuration.

- DHCP Server Configuration
  You can enable or disable the DHCP server function and configure the DHCP configuration on this page.



DHCP Server Configuration

Description	Factory default
Admin Mode	
Specify the status of the DHCP server on the switch: • **Disable**: The DHCP server is disabled. When you want to enable the DHCP relay function, please select this setting. • **Enable**: The DHCP server is enabled.	Disable
Next Server	
Specify the boot server host name.	0.0.0.0
Boot File	
Specify the boot file name.	None
Network	
Enter the network for the DHCP pool.	None
Subnet Mask	
Enter the IP subnet mask for the DHCP pool.	None

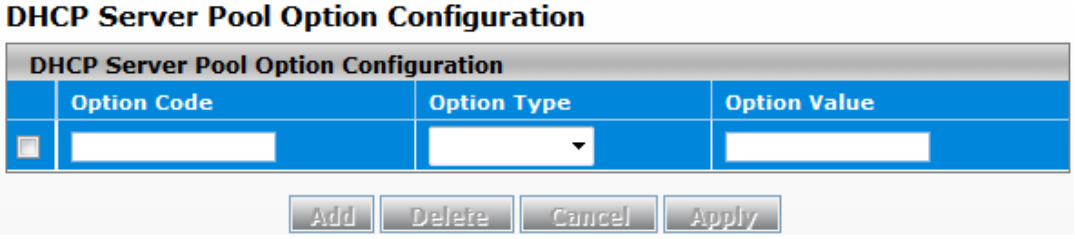
Description	Factory default
Lease Time Type	
Specify a type of lease time: • **Specified Duration**: The leased IP address has a specific duration. You need to specify the duration in the Lease Time fields. • **Infinite**: The leased IP address does not expire.	None
Lease Time	
If you select Specified Duration from the Lease Time Type in the drop-down list, specify the duration by entering the days, hours, and minutes in the Lease Time fields.	None
Default Router	
Specify the default gateway IP address. The information will be included in the DHCP offer packet.	None
DNS Server	
Specify the DNS server IP address. The information will be included in the DHCP offer packet.	None
Domain Name	
Specify the domain name. The information will be included in the DHCP offer packet.	None

Excluded Addresses

Description	Factory default
IP Range From	
Enter the start IP address of the exclusion IP range which you created in the DHCP server pool.	None
IP Range To	
Enter the end IP address of the exclusion IP range which you created in the DHCP server pool.	None
Method	None
It indicates that the excluded address is created by a DHCP server or a user. There are two values: • **Auto**: The entry is created by a DHCP server. • **Manual:** The entry is created by a user.	None

- DHCP Server Pool Option Configuration

DHCP messages contain many option fields. These options have much control information and many configuration parameters.



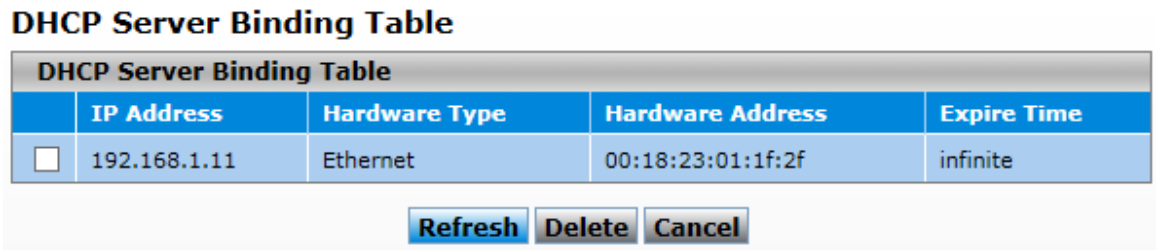
DHCP Server Pool Option Configuration

Description	Factory default
Option Code	
Enter the option code. For example, the option code 3 is a router, 6 is a domain name server. (If you need more information, please refer to RFC2132, DHCP Options and BOOTP Vendor Extensions.)	None
Option Type	
Specify the option type: • **ASCII:** Enter an ASCII value in the Option Value field. • **Hex:** Enter a hexadecimal value in the Option Value field. • **IP Address**: Enter an IP address or a subnet mask in the Option Value field.	None

Description	Factory default
Option Value	
Enter the value that corresponds to the option type you select.	None

- DHCP Server Binding Table

  If the DHCP server function is activated, you can see the DHCP client's information which is get the IP address from the DHCP server on this page.



DHCP Server Binding Table

Description	Factory default
IP Address	
The IP address of the DHCP client.	None
Hardware Type	
This field displays a type of hardware address of the client. • **Client ID**: If the client uses DHCP option 61 to specify itself, the hardware type is the client ID, and the hardware address is the string identifier. • **Ethernet**: The hardware type is Ethernet, and the hardware address is an MAC address.	None
Hardware Address	
This field displays the MAC address or the string identifier of the DHCP client.	None
Expire Time	
The expiration time of the DHCP client.	None

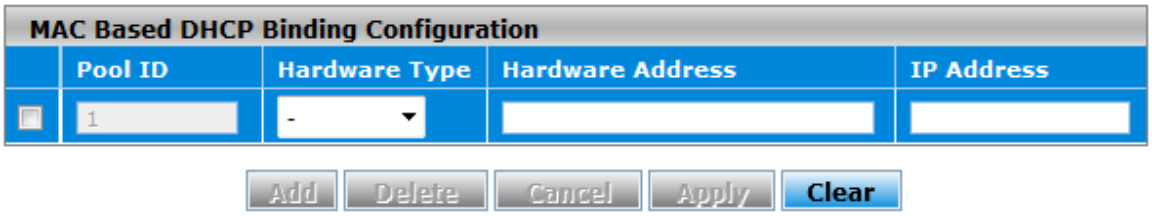
- MAC Based DHCP Configuration

  MAC Based DHCP Configuration supports the administrator assigned the specific IP address to the MAC address in the list.

Note:
MAC Based DHCP Mode and Port Based DHCP Mode can't enable and work at the same time.

MAC Based DHCP Mode

Description	Factory default
Admin Mode	
Specify the status of the MAC Based DHCP on the switch. • **Disable**: The MAC Based DHCP Configuration is disabled. • **Enable**: The MAC Based DHCP Configuration is enabled. **Note:** If you need to enable the admin mode of MAC Based DHCP Mode, it must be enabled the DHCP server mode first.	Disable



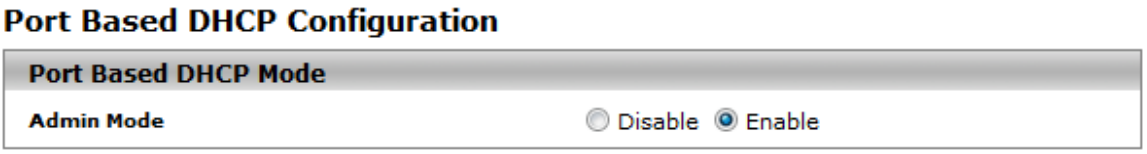
MAC Based DHCP Binding Configuration

Description	Factory default
Pool ID	
It's the DHCP Pool number.	fixed
Hardware Type	
This field displays a type of hardware address of the client. • **Client ID**: The type of the HW address.If the client uses DHCP option 61 to specify itself, the hardware type is the client ID, and the hardware address is the string identifier. **Ethernet**: The type of the HW address, and the hardware address is an MAC address.	None
Hardware Address	
This field displays the MAC address or the string identifier.	None
IP Address	
It's the static IP address which assigned to the specified HW Address.And it should be included in the Excluded Address of DHCP Server Configuration.	None

- Port Based DHCP Configuration

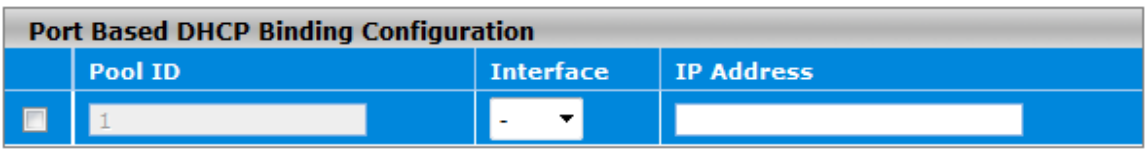
  Port Based DHCP Configuration supports the administrator assigned the specific IP address for the port number in the list.

Note:
MAC Based DHCP Mode and Port Based DHCP Mode can't enable and work at the same time.



Port Based DHCP Mode

Description	Factory default
Admin Mode	
Specify the status of the Port Based DHCP on the switch. • **Disable**: The Port Based DHCP Mode is disabled. • **Enable**: The Port Based DHCP Mode is enabled. **Note:** If you need to enable the admin mode of MAC Based DHCP Mode, it must be enabled the DHCP server mode first.	Disable



Port Based DHCP Binding Configuration

Description	Factory default
Pool ID	
It's the DHCP Pool number.	1
Interface	
The interface number.You can specify the interface which will assign the specific IP address when the DHCP client is connect to the specific interface.	None
IP Address	
The static IP address which assigned to the specified interface.And it should be included in the Excluded Address of DHCP Server Configuration.	None

- RARP Bindings Configuration
  The RARP Bindings Configuration supports to use RARP to acquire IP for device without DHCP client function.

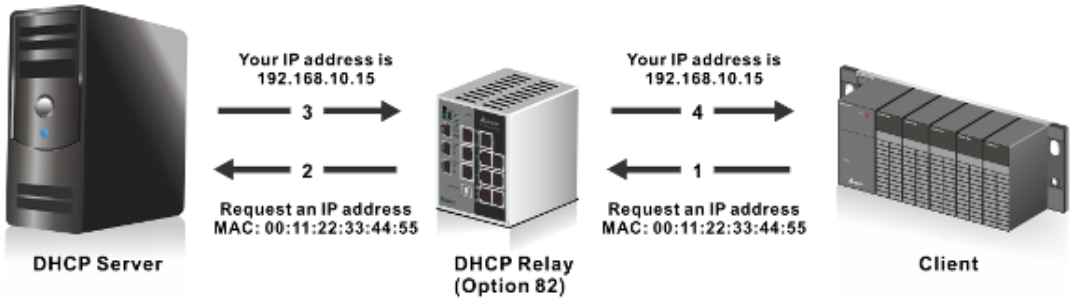
Note:
Please remember to enable the MAC Based DHCP Binding Configuration or Port Based Binding Configuration before you use this function, otherwise the RARP will not use the static binding to assign IP address to the client.

RARP Binding Configuration

Description	Factory default
IP Address	
It's the static IP which acquired from the MAC Based DHCP Binding Configuration or Port Based Binding Configuration.	None
Hardware Type	
This field displays a type of hardware address of the client. • **Client ID**: The type of the HW address.If the client uses DHCP option 61 to specify itself, the hardware type is the client ID, and the hardware address is the string identifier. • **Ethernet**: The type of the HW address, and the hardware address is an MAC address.	None
Hardware Address	
This field displays the MAC address or the string identifier.	None

3.1.5.2 DHCP Relay

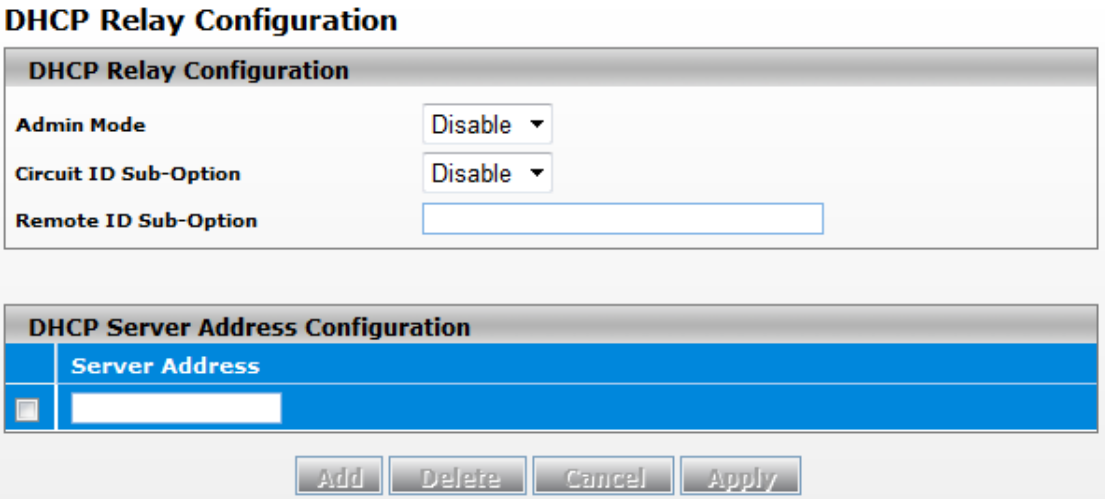
A DHCP Relay can make broadcast messages to be sent over routers. And a DHCP relay can receive a DHCP broadcast request packet and forward it to a specified server. The operating theory is shown in the figure below.



Notice:
When a DHCP request packet comes, the DHCP relay receives it and then sends it to all VLANs. But according to RFC 2131, when a unicast DHCP request packet renews, it will be sent to a DHCP server directly without passing a DHCP relay, so it is recommended to make sure that the DHCP client can ping the server after getting an IP address.

- DHCP Relay Configuration
  The DHCP relay sends a unicast DHCP packet to the specified server(s). The maximum number of specified servers is 5. You can enable or disable a DHCP relay function, and configure the parameters of the circuit ID sub-option (the interface ID on the switch which connects to the host) and the remote ID sub-option (the MAC address of the host which sends DHCP request) on this page.

3



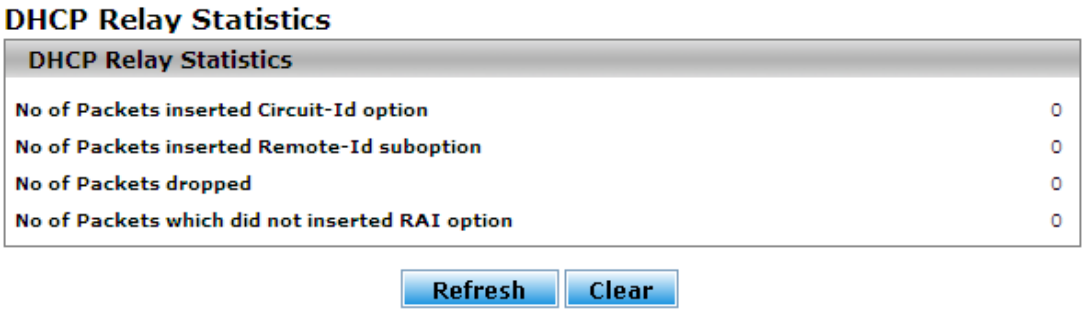
DHCP Relay Configuration

Description	Factory default
Admin Mode	
Specify the status of the DHCP relay on the switch: • **Disable**: The DHCP relay is disabled. This is the default setting. • **Enable**: The DHCP relay is enabled. **Notice:** Before you enabled Admin Mode, please create at least one server IP in DHCP Server Address Configuration.	Disable
Circuit ID sub-option	
Specify whether the circuit ID sub-option (the interface ID of the switch) is enabled. • **Disable**: The circuit ID can not be added to a DHCP packet. This is the default setting. • **Enable**: The circuit ID can be added to a DHCP packet.	Disable
Remote ID Sub-Option	
Enter a remote ID string (the MAC address of the host which sends the DHCP request) for the circuit ID mode. This is a local identifier of the circuit from which a DHCP client-to-server packet is received. It ensures that the DHCP relay sends DHCP server responses back to the correct circuit.	None

DHCP Server Address Configuration

Description	Factory default
Server Address	
The IP address of the DHCP server IP.	None

- **DHCP Relay Statistics**

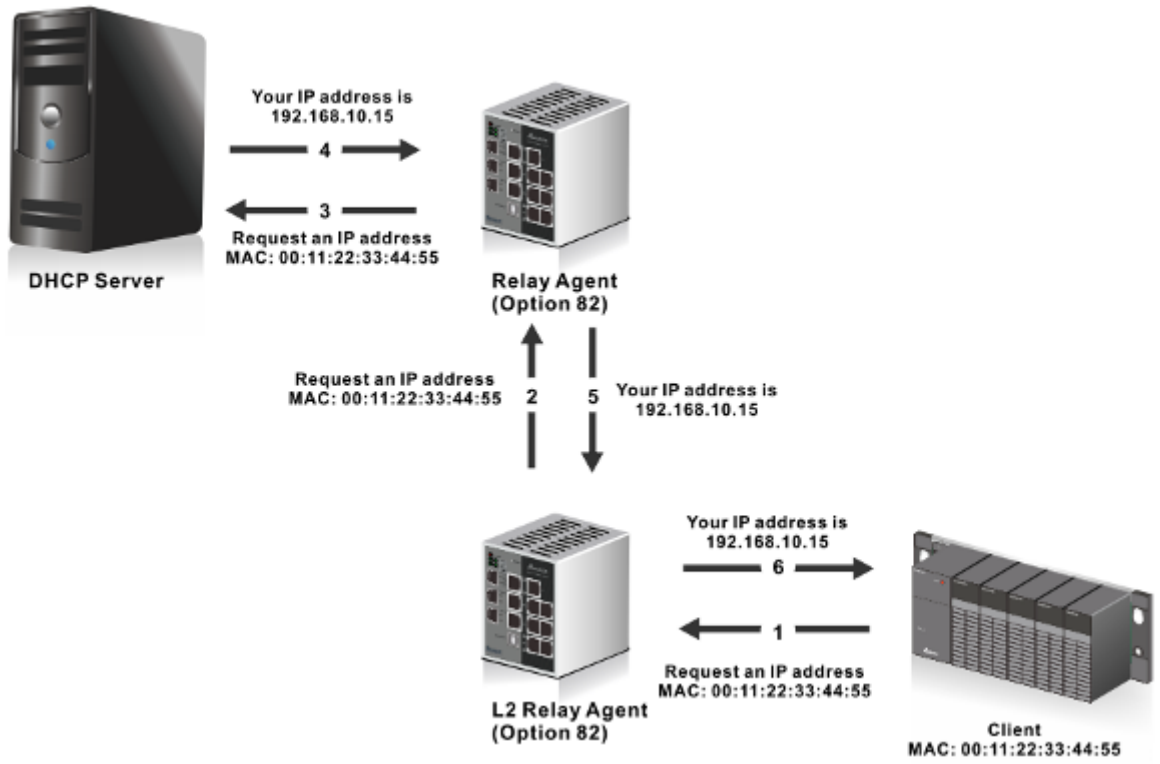


DHCP Relay Statistics

Item	Description
No of Packets inserted Circuit-Id option	The number of packets which inserted the circuit-Id option.
No of Packets inserted Remote-Id suboption	The number of packets which inserted the remote-Id suboption.
No of Packets dropped	The number of packets which dropped.
No of Packets which did not inserted RAI option	The number of packets which did not insert the RAI (Relay Agent Information) option.

3.1.5.3 DHCP L2 Relay

In some networks, DHCP servers rely on the Relay Agent Information option appended by Relay Agents for the IP address and other parameter assignment policies. This works fine when end hosts are directly connected to Relay Agents. In some network configurations, one or more Layer 2 devices may reside between DHCP clients and a Relay agent. In these network scenarios, it is difficult to use the Relay Agent Information option for an IP address and other parameter assignment policies effectively. So there is a requirement for the device that is closest to the end hosts to append a Relay Agent Information option in DHCP messages. These devices are typically known as Layer 2 Relay Agents. The operating theory is shown in the figure below.

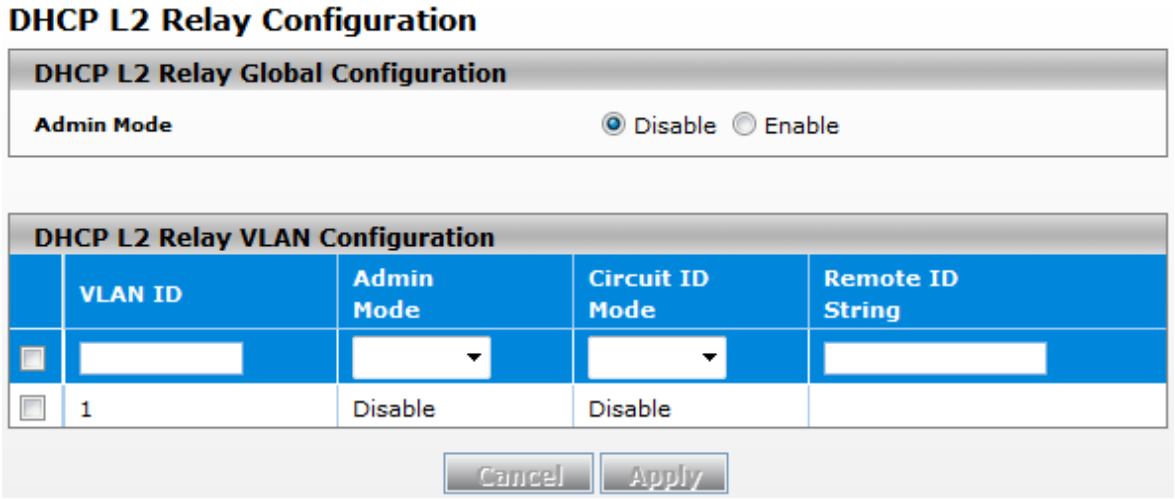


DHCP snooping steps:

1. A DHCP client sends a DHCP request via the broadcast.
2. When a switch (relay agent) receives the DHCP request, it will add DHCP option-82 to the packet. DHCP option-82 includes the MAC address of the host which sends a DHCP request (remote-ID sub-option) and the interface ID on the switch which connects to the host (circuit-ID sub-option).
3. If the switch has configured an IP address, the IP address will be added to the DHCP packet.
4. If a DHCP server supports option-82, after the DHCP server receives the DHCP request, it will allocate the IP address numbers according to the remote-ID sub-option or circuit ID sub-option.
5. A DHCP server responds to the switch via the unicast. And the switch checks whether the remote-ID or the circuit-ID in option-82 matches the value of the DHCP request, and makes sure it sends from the certificated DHCP server. Then it removes the information of option-82, and sends back to the interface on the switch which sends the DHCP request.

- DHCP L2 Relay Global Configuration

  You can enable or disable a DHCP relay function, and configure the parameters of the circuit ID sub-option (the interface ID on the switch which connects to the host) and the remote ID sub-option (the MAC address of the host which sends DHCP request) on this page.



DHCP L2 Relay Global Configuration

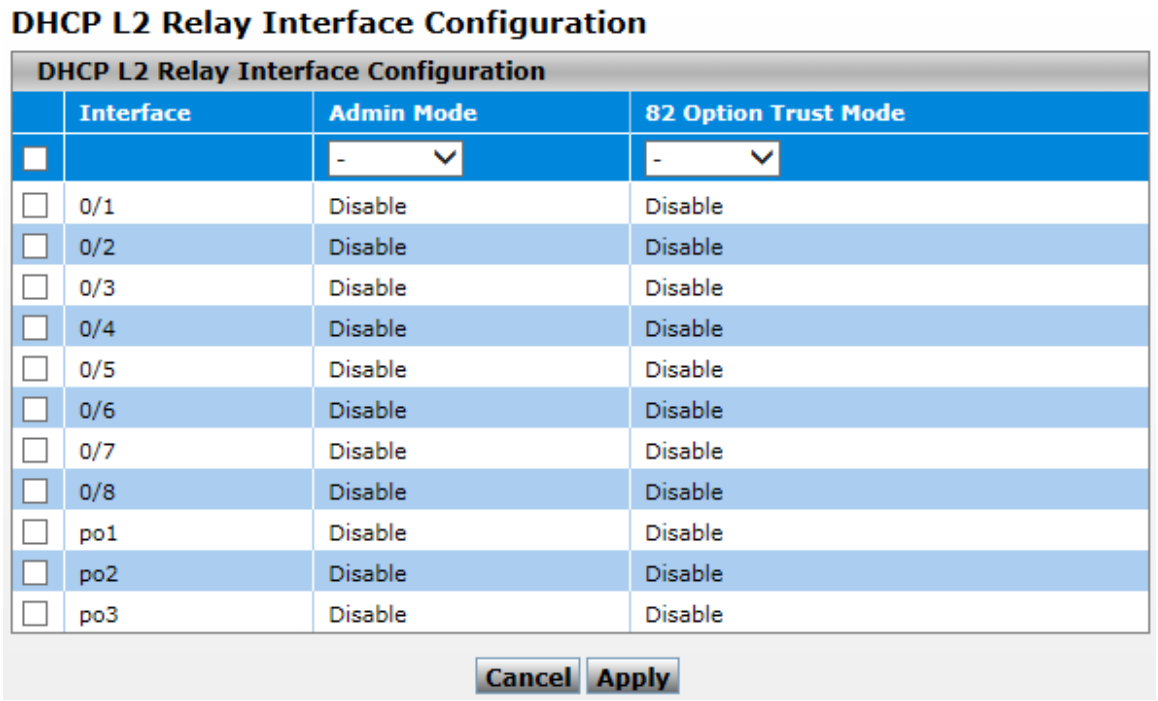
Description	Factory default
Admin Mode	
Specify whether the global status of the DHCP relay is enabled. • **Enable**: The DHCP relay function is enabled. • **Disable**: The DHCP relay function is disabled. This is the default setting.	Disable

DHCP L2 Relay VLAN Configuration

Description	Factory default
VLAN ID	
If you have added VLANs on the VLAN Configuration page, the VLANs can be shown in the VLAN ID column, and you can configure the DHCP L2 relay setting of each VLAN.	1
Admin Mode	
Specify whether the status of the DHCP relay is enabled on the VLAN: • **Enable**: Enable the DHCP relay on the VLAN. You can configure the VLAN DHCP relay settings if the DHCP relay is globally disabled. But the settings do not take effect even if you have applied it. • **Disable**: Disable the DHCP relay on the VLAN.	Disable
Circuit ID	
Specify whether the DHCP relay agent information option (DHCP option 82) is enabled: • **Enable**: Enable the relay agent information option.	Disable

Description	Factory default
• **Disable**: Disable the relay agent information option. This is the default setting for the default VLANs 1, 2, and 3.	
Remote ID String	
Enter the remote ID string for the circuit ID mode. This is a local identifier of the circuit from which a DHCP client-to-server packet is received. It can make sure that the DHCP relay responds to packets from the DHCP server to the correct circuit.	None

- DHCP L2 Relay Interface Configuration
  The interface which is connected to a DHCP server is a trusty interface; the interface which is connected to a DHCP client is an untrustful interface.
  - ◆ Trusted port:
    (a) When a DHCP request packet with opt82 is received, it will be forwarded.
    (b) When a DHCP reply packet with opt82 is received, if the remote ID is same as the switch's ID, opt82 will be stripped and forwarded; if the remote ID is not same as the switch's ID, it will be forwarded directly.
    (c) When a DHCP packet without opt82 is received, it will be dropped.
  - ◆ Un-trusted Port:
    (a) When a DHCP packet with opt82 is received, it will be dropped.
    (b) When a DHCP packet without opt82 is received, opt82 will be inserted and the packet will be forwarded.



DHCP L2 Relay Interface Configuration

Description	Factory default
Interface	
The interface number.	*interface number*
Admin Mode	
Specify whether the DHCP relay is enabled on the interface: • **Enable**: Enable the DHCP relay on the interface. If the DHCP relay is globally disabled on the switch, you can still configure the interface DHCP relay settings, but the settings do not take effect even if you have applied it. • **Disable**: Disable the DHCP relay on the interface.	Disable
82 Option Trust Mode	
As a security consideration, specify whether the interface is trusted when the DHCP relay agent information (DHCP option 82) is received on the interface: • **Enable**: The relay agent information that is received on the interface can be trusted. • **Disable**: The relay agent information that is received on the interface can not be trusted and should be ignored.	Disable

- DHCP L2 Relay Statistics
  You can see the statistics of DHCP L2 relay messages on this page.

DHCP L2 Relay Interface Statistics

DHCP L2 Relay Interface Statistics

Interface	Untrusted Server Messages With Opt82	Untrusted Client Messages With Opt82	Trusted Server Messages Without Opt82	Trusted Client Messages Without Opt82
0/1	0	0	0	0
0/2	0	0	0	0
0/3	0	0	0	0
0/4	0	0	0	0
0/5	0	0	0	0
0/6	0	0	0	0
0/7	0	0	0	0
0/8	0	0	0	0
po1	0	0	0	0
po2	0	0	0	0
po3	0	0	0	0

Clear Refresh

DHCP L2 Relay Interface Statistics

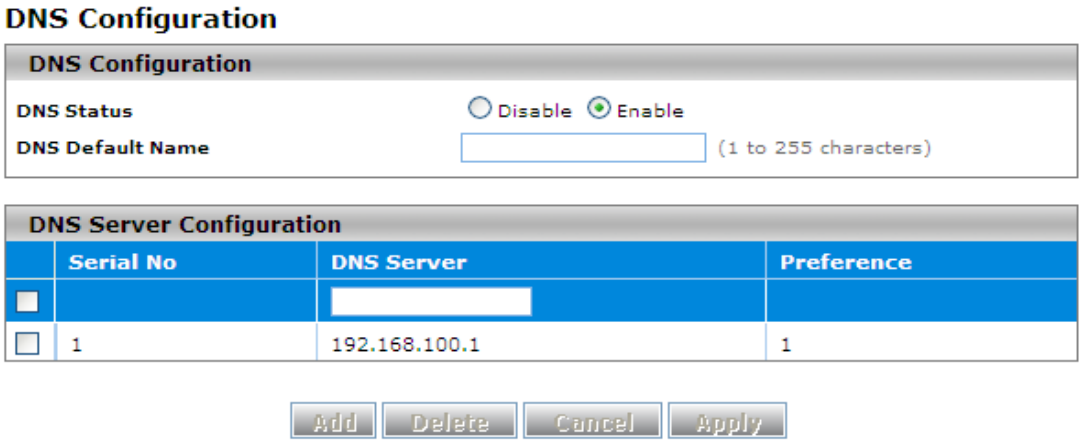
Item	Description
Interface	The interface number.
Untrusted Server Messages With Opt82	The number of DHCP packets with option 82 that were received from an untrusted server.
Untrusted Client Messages With Opt82	The number of DHCP packets with option 82 that were received from an untrusted client.
Trusted Server Messages Without Opt82	The number of DHCP packets without option 82 that were received from a trusted server.
Trusted Client Messages Without Opt82	The number of DHCP packets without option 82 that were received from a trusted client.

3.1.6 DNS

The Delta switch can function as a DNS client and forward the DNS queries to a DNS server. You can configure DNS servers manually or add them via a DHCP server.

3.1.6.1 DNS Configuration

You can configure the global DNS settings and add a DNS server manually on this page.



DNS Configuration

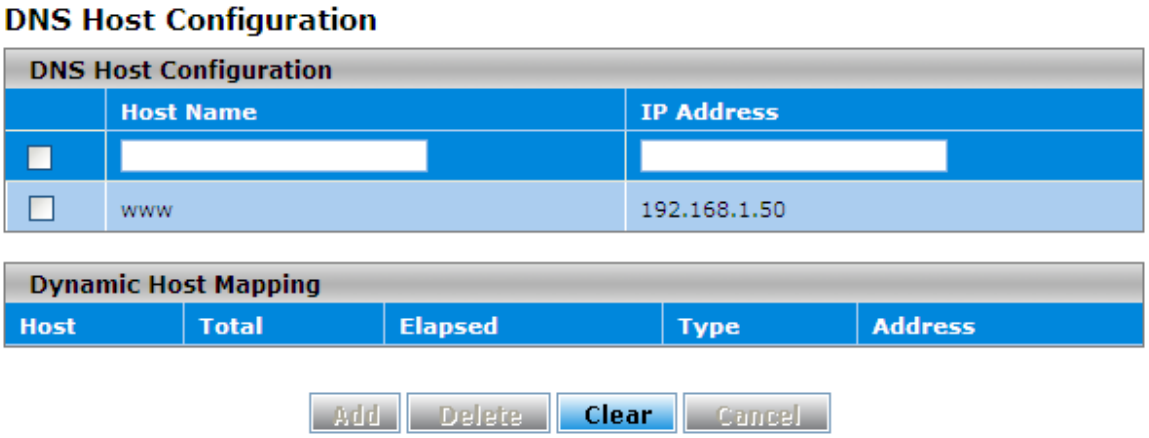
Description	Factory default
DNS Status	
Specify whether the switch functions as a DNS client: • **Disabled**: The switch does not function as a DNS client and does not send DNS queries. The settings do not take effect even if you configure a DNS server. • **Enabled**: The switch functions as a DNS client and can send DNS queries to a DNS server.	Enable
DNS Default Name	
Enter the DNS default domain name to be included in DNS queries. When the switch performs a lookup for an unqualified host name, the DNS default domain name is provided as the domain name. For example, if the DNS default domain name is delta.com and you enter "dvs" for a DNS query, then "dvs" is changed to "dvs.delta.com" to resolve the name. The length of the name can not be longer than 255 characters.	None

DNS Server Configuration

Description	Factory default
Serial No	
The sequence number of the DNS server in the table. If the IP address of the DNS server was dynamically added through DHCP, the number is followed by an asterisk (*).	None
DNS Server	
The DNS server can be added manually or added dynamically through DHCP. The Delta switch can support 8 DNS servers.	None
Preference	
The preference of the DNS server. The preference is determined by the order in which the IP address was added to the table. So preference number 1 is the first IP address that was added to the table.	None

3.1.6.2 Host Configuration

You can map a DNS host name to an IP address on this page.



DNS Host Configuration

Description	Factory default
Host Name	
Specify the static host name. The maximum number of characters is 255.	None
IP Address	
Specify the IP address of the host name.	None

Dynamic Host Mapping

Description	Factory default
Host	
The host name was added dynamically.	None
Total	
The total time to live (TTL) for the dynamic entry.	None
Elapsed	
The elapsed time since the dynamic entry was added to the table.	None
Type	
The dynamic entry types: • IPv4 • IPv6 • Canonical name	None
Address	
The IP address of the host name.	None

3.1.7 System File Update

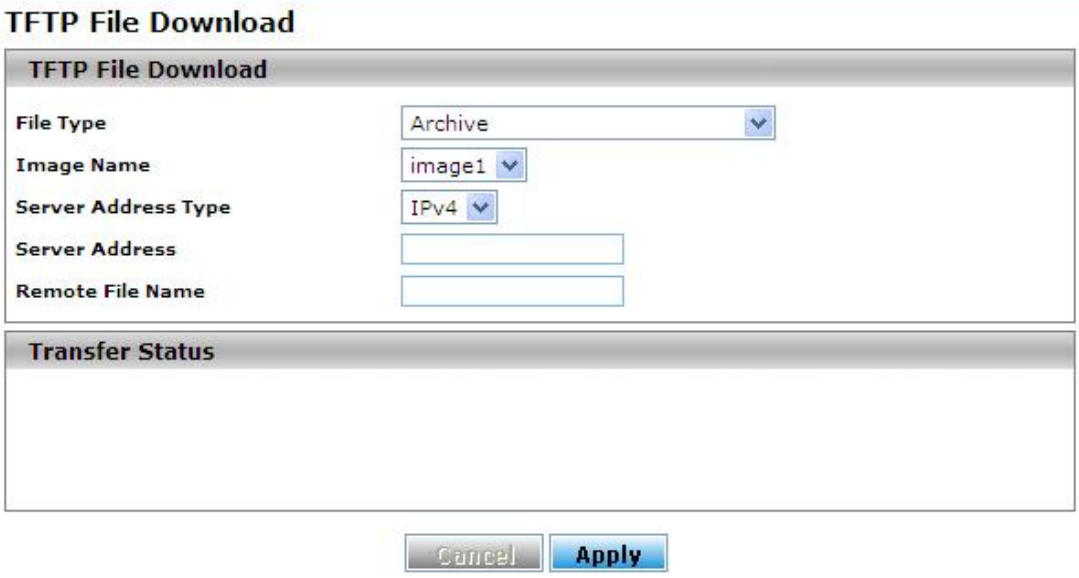
The Delta switch supports downloading the firmware, configuration, or log file from a TFTP server or local host. And it also supports uploading the files to a TFTP server or local host.

3.1.7.1 Download File

The Delta switch supports 2 ways for users to download files. If there is no TFTP server in your network environment, you can choose the HTTP way to download files from the local host.

Notice:
If the file version is that you update is older than the current version, the curret configuration will be lost when you finish the update process, and it will restore the factory default configuration.

- TFTP Download

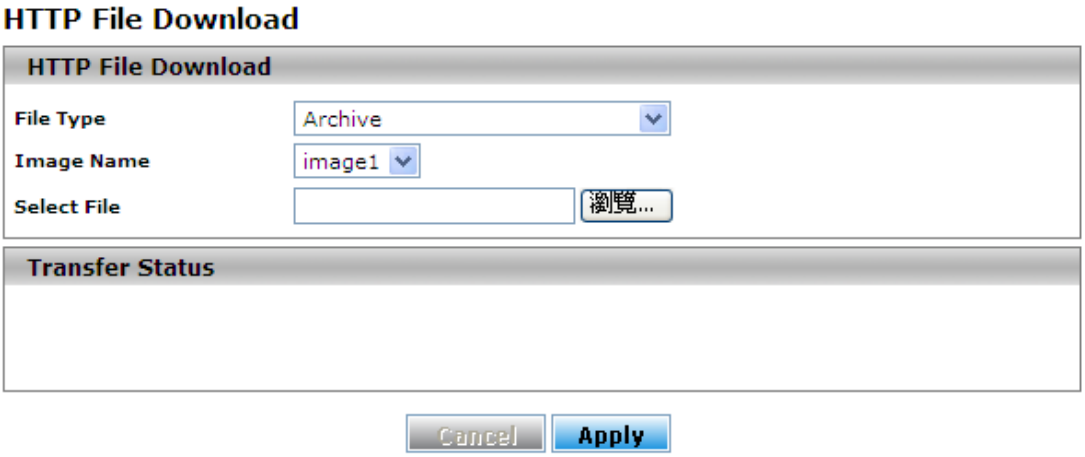


TFTP File Download

Description	Factory default
File Type	
Specify a type of file in the drop-down list that you want to download: • **Archive**: When you select Archive, the Image Name drop-down list is displayed. • **Startup Configuration**: When the switch boots up, Startup Configuration will be applied. • **SSL Server Certificate PEM File**: For more information about the SSL server certificate PEM file, please see the Certificate Information page. • **Script File**: This file is used to configure the switch by the CLI script.	None
Image Name	
Only when you select Archive from the File Type drop-down list is the Image Name drop-down list displayed. Specify the image: • **image1**: The downloaded image firmware as image1. • **image2**: The downloaded image firmware as image2.	image1
Server Address Type	
Specify a type of server address and enter the IP address or host name in the Server Address field: • **IPv4**: The IPv4 address of a TFTP server. • **DNS**: The DNS host name of a TFTP server.	IPv4
Server Address	
Enter an IPv4 address or a DNS host name of the TFTP server.	None
Remote File Name	
Enter the name of the file that you want to download to the switch. You can enter up to 32 characters.	None

If you select Archive in the File Type drop-down list, the image name item will show up. After selecting File Type, setting up Server Address and specifying Remote File Name, click **Apply** to start the downloading.

- **HTTP Download**



HTTP Download

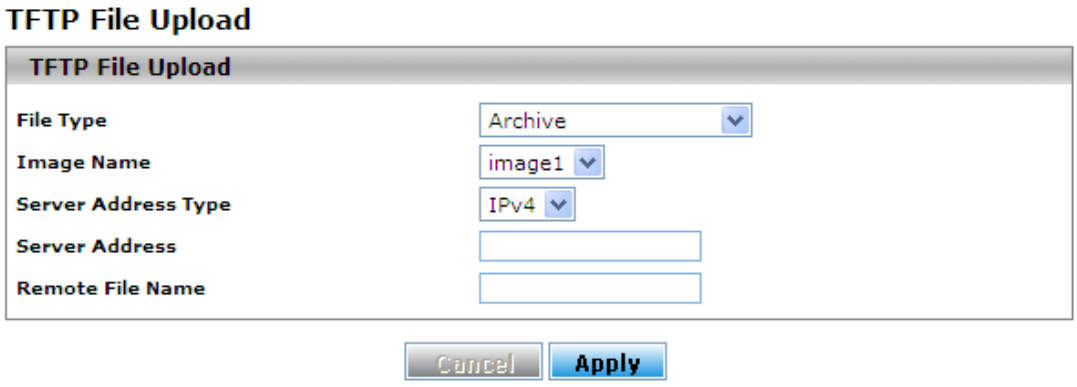
Description	Factory default
File Type	
Specify a type of file in the drop-down list that you want to download: • **Archive**: When you select Archive, the Image Name drop-down list is displayed. • **Startup Configuration**: When the switch boots up, Startup Configuration will be applied. • **SSL Server Certificate PEM File**: For more information about the SSL server certificate PEM file, please see the Certificate Information page. • **Script File**: This file is used to configure the switch by the CLI script.	None
Image Name	
Only when you select Archive from the File Type drop-down list is the Image Name drop-down list displayed. Specify the image: • **image1**: The downloaded image firmware as image1. • **image2**: The downloaded image firmware as image2.	image1
Select File	
Specify the file that you want to download.	None

If you select Archive in the File Type drop-down list, the image name item will show up. After selecting File Type and the path of the file on your PC, click **Apply** to start the downloading.

3.1.7.2 Upload File

The Delta switch supports 2 ways for user to upload files. If there is no TFTP server in your network environment, you can choose HTTP way to upload files.

- TFTP Upload

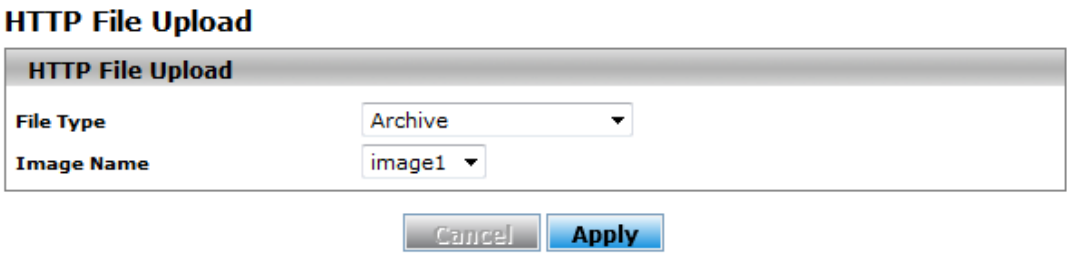


TFTP Upload

Description	Factory default
File Type	
Specify a type of file in the drop-down list that you want to upload: • **Archive**: When you select Archive, the Image Name drop-down list is displayed. • **Startup Configuration**: When the switch boots up, Startup Configuration will be applied. • **Backup Configuration**: It is used to backup the Startup Configuration file. • **Log:** This file records the log information of the switch. • **Script File**: This file is used to configure the switch by the CLI script.	None
Image Name	
Only when you select Archive from the File Type drop-down list is the Image Name drop-down list displayed. Specify the image: • **image1**: The uploaded image firmware as image1. • **image2**: The uploaded image firmware as image2.	image1
Server Address Type	
Specify a type of server address and enter the IP address or host name in the Server Address field: • **IPv4**: The IPv4 address of a TFTP server. • **DNS**: The DNS host name of a TFTP server.	IPv4
Server Address	
Enter an IPv4 address or a DNS host name of the TFTP server.	None
Remote File Name	
Enter the name of the file that you want to upload to the switch. You can enter up to 32 characters.	None

If you select Archive in the File Type drop-down list, the image name item will show up. After selecting File Type, you have to set up Server Address, specify Remote File Name, and click **Apply** to start uploading.

- HTTP Upload



HTTP Upload

Description	Factory default
File Type	
Specify a type of file in the drop-down list that you want to upload: • **Archive**: When you select Archive, the Image Name drop-down list is displayed. • **Startup Configuration**: When the switch boots up, Startup Configuration will be applied. • **Backup Configuration**: It is used to backup the Startup Configuration file. • **Log**: This file records the log information of the switch. • **Script File**: This file is used to configure the switch by the CLI script. **Notice:** The Backup Configuration file is for user to back up the Startup Configuration file, but it must use CLI to back up the file. You can use the command: "**copy nvram:startup-config nvram:backup-config**" to back up the Startup Configuration file by Hyper Terminal or Telnet.	None

Description	Factory default
Image Name	
Only when you select Archive from the File Type drop-down list is the Image Name drop-down list displayed. Specify the image: • **image1**: The uploaded image firmware as image1. • **image2**: The uploaded image firmware as image2.	image1

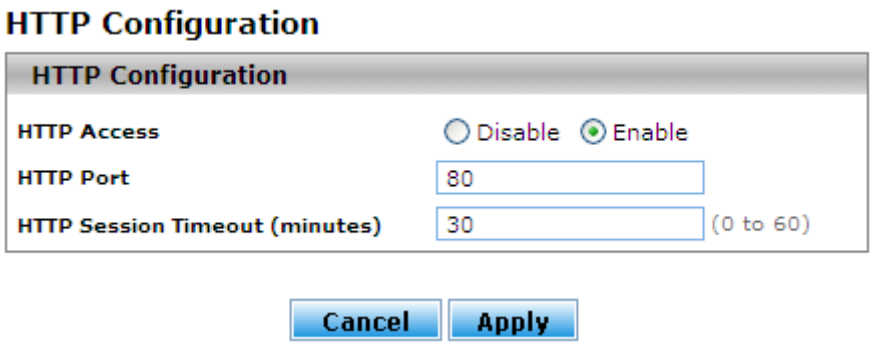
If you select Archive in File Type drop-down list, the image name item will show up. After selecting File Type, you have to click **Apply** and specify a path to start uploading.

3.1.8 Management Access

The Delta switch supports not only one way to access the web management interface. You can configure HTTP or secure HTTP (HTTPS), and you also can configure Secure Shell (SSH), Telnet and the console port access.

3

3.1.8.1 HTTP Configuration



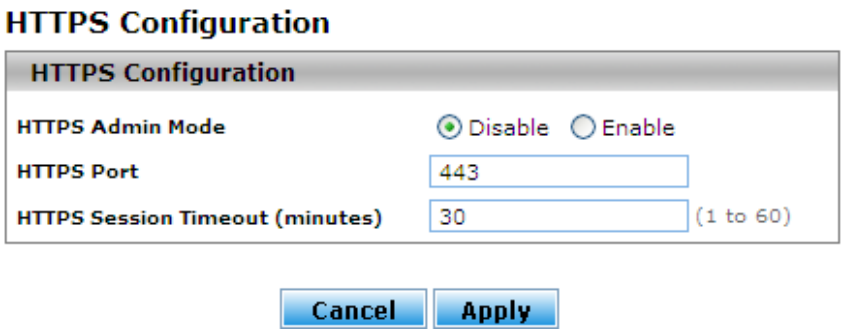
HTTP Configuration

Description	Factory default
HTTP Access	
Specify whether the web management interface can be accessed from a web browser over an HTTP connection. • **Disable**: The web management interface can not be accessed over an HTTP connection. You need to use a Telnet, SSH, or console connection to access the switch. • **Enable**: The web management interface can be accessed over an HTTP connection.	Enable
HTTP Port	
The HTTP port number. The number must be in the range of 1 to 65535. The default setting is port number 80.	80
HTTP Session Timeout (minutes)	
The HTTP session timeout period in minutes. The HTTP session will be closed when there is no activity and the timeout period is reached. Enter a period in the range of 0 to 60 minutes. Entering 0 disables the timeout.	30

3.1.8.2 HTTPS

Hypertext Transfer Protocol Secure (HTTPS) is a protocol for secure communication. It enables the transmission of HTTP over an encrypted Secure Sockets Layer (SSL) or Transport Layer Security (TLS) connection. So HTTPS can help protect the communication between a computer and a switch from eavesdroppers and man-in-the-middle (MITM) attacks.
If you want to configure the switch to access an HTTPS connection from a computer, the switch needs a public key certificate. You can configure the switch to generate a key or download it to the switch.

- HTTPS Configuration



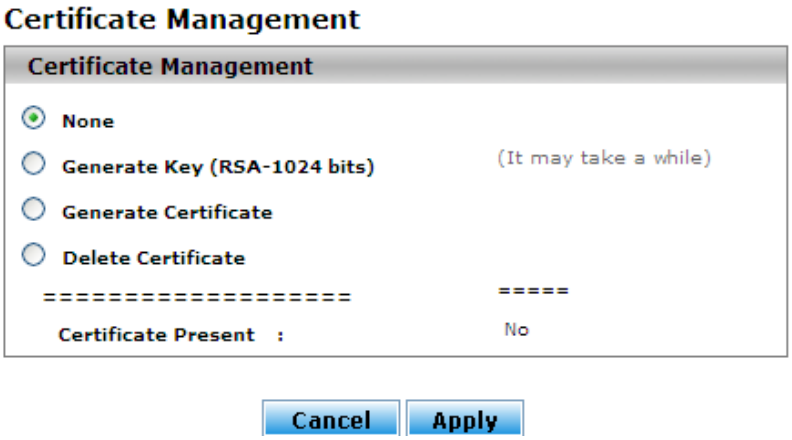
HTTPS Configuration

Description	Factory default
HTTPS Admin Mode	
Specify whether the web management interface can be accessed from a web browser over an HTTPS connection. • **Disable**: The web management interface can not be accessed over an HTTPS connection. You need to use a Telnet, SSH, or console connection to access the switch. • **Enable**: The web management interface can be accessed over an HTTPS connection. **Notice:** If you want to enable the HTTPS Admin mode, you need to use Generate Key, then apply Generate Certificate, please refer to **Certificate Management**.	Disable
HTTPS Port	
The HTTP port number. The number must be in the range of 1 to 65535.	443
HTTPS Session Timeout (minutes)	
The HTTPS session timeout period in minutes. When there is no activity and the timeout period is reached, the HTTP session will be closed. The time period must be in the range of 1 to 60 minutes.	30

After you enable the HTTPS connection, you can type **https://Delta switch's IP address** into the web browser to establish an HTTPS connection.
For example, if a switch's IP address is 192.168.1.5, the complete address is https://192.168.1.5.

- Certificate Management

You can use the function on this page to generate a self-signed certificate for an HTTPS connection.



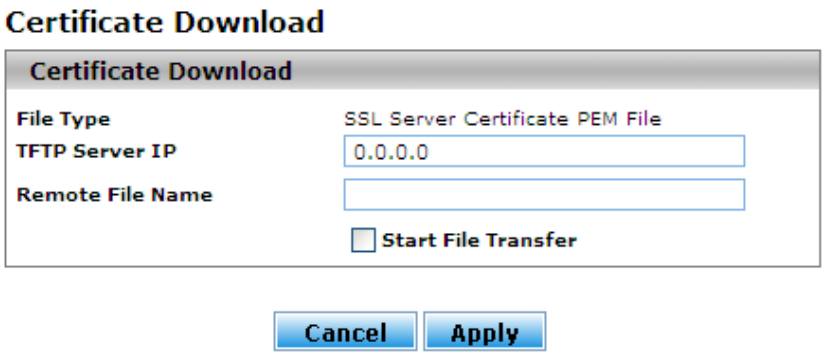
Certificate Management

Description	Factory default
None	
No certificate is to be generated.	None
Generate Key (RSA-1024 bits)	
Generate a 1024-bit RSA key. After the key has been generated, the page reverts to its default setting and the None item will be selected.	None
Generate Certificate	
Generate a certificate. After the key has been generated, the page reverts to its default setting and the None item will be selected.	None
Delete Certificate	
Delete the certificate on the switch.	None
Certificate Present	
Displays the present certificate on the switch.	None

- Certificate Download

Make sure of the conditions before you download a certificate to the switch:

- The file which is ready to be downloaded from the TFTP server is on the server and in the appropriate directory.
- The file's format is in PEM.
- The switch has a path to the TFTP server.

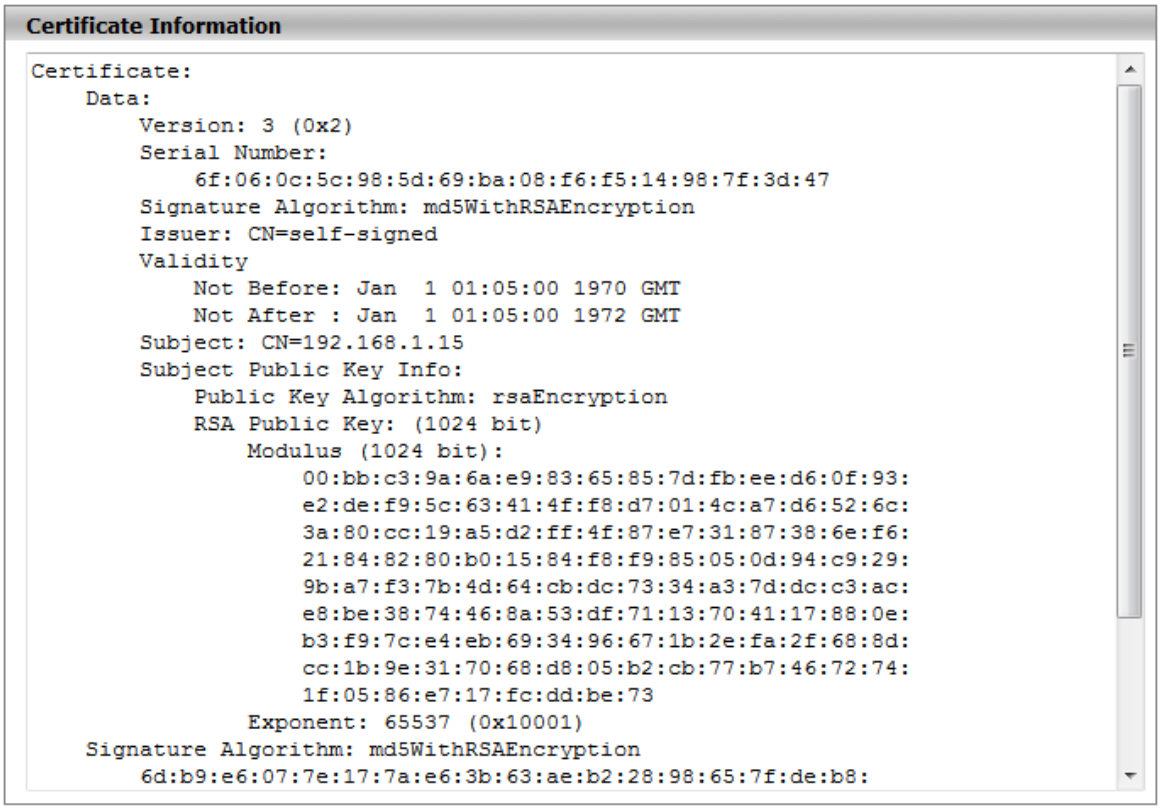


Certificate Download

Description	Factory default
TFTP server IP	
Specify a TFTP server IP address.	0.0.0.0
Remote File Name	
Specify a certificate file name which can be downloaded.	None

- Certificate Information

Certificate Information



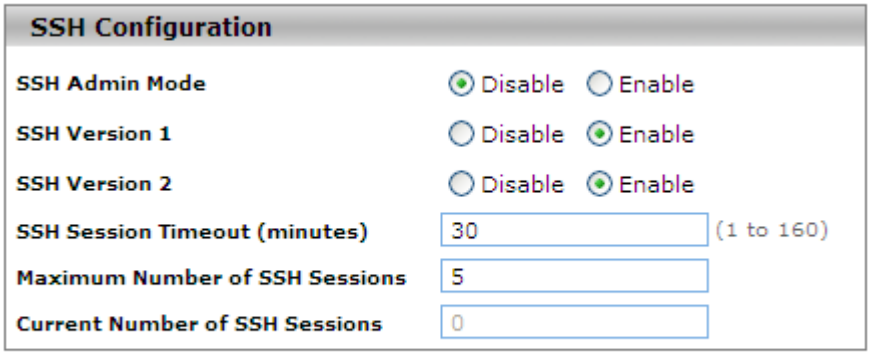
Refresh

Click **Refresh** for updating the information of the certificate.

3.1.8.3 SSH Configuration

You can configure an SSH configuration on this page.

SSH Configuration



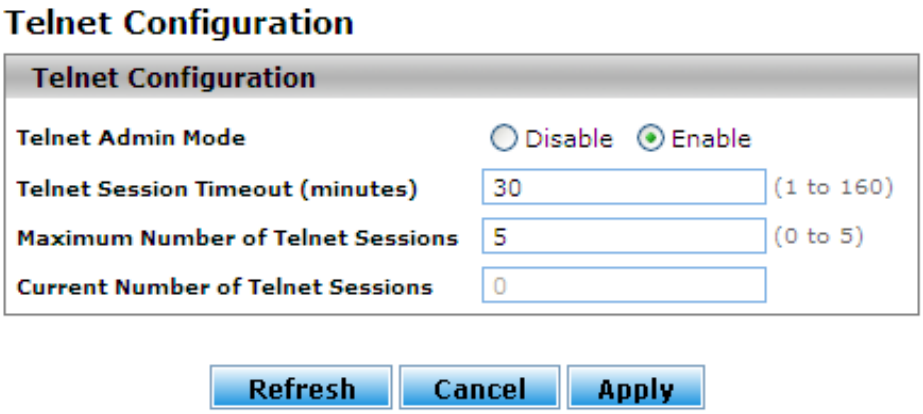
Refresh Cancel Apply

SSH Configuration

Description	Factory default
SSH Admin Mode	
Specify the status of SSH. • **Disable**: SSH is disabled. This is the default setting. • **Enable**: SSH is enabled.	Disable
SSH Version 1	
Specify whether SSH version 1 is supported. • **Disable**: SSH version 1 is not supported. • **Enable**: SSH version 1 is supported. Both version 1 and version 2 can be supported on the switch.	Enable
SSH Version 2	
Specify whether SSH version 2 is supported. • **Disable**: SSH version 2 is not supported. • **Enable**: SSH version 2 is supported. Both version 1 and version 2 can be supported on the switch.	Enable
SSH Session Timeout (minutes)	
The SSH session timeout period in minutes. When there is no activity and the timeout period is reached, the SSH session will be closed. Enter a period in the range of 1 to 160 minutes.	30
Maximum Number of SSH Sessions	
The maximum number of inbound SSH sessions. The number must be in the range of 0 to 5.	5
Current Number of SSH Sessions	
This field displays the number of simultaneous SSH sessions.	0

3.1.8.4 Telnet Configuration

You can configure the Telnet configuration on this page.

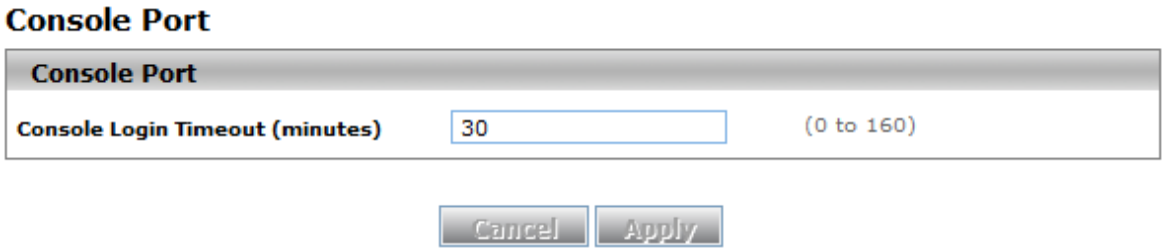


Telnet Configuration

Description	Factory default
Telnet Admin Mode	
Specify the status of Telnet. • **Disable**: Telnet is disabled. • **Enable**: Telnet is enabled.	Enable
Telnet Session Timeout (minutes)	
The Telnet session timeout period in minutes. When there is no activity and the timeout period is reached, the Telnet session will be closed. The period must be in the range of 1 to 160 minutes.	30
Maximum Number of Telnet Sessions	
The maximum number of inbound Telnet sessions that are allowed on the switch. The number must be in the range of 0 to 5.	5
Current Number of Telnet Sessions	
This field displays the number of simultaneous Telnet sessions.	0

3.1.8.5 Console Port

You can configure the console port configuration on this page.



Console Port

Description	Factory default
Console Login Timeout (minutes)	
The console port session timeout period in minutes. When there is no activity and the timeout period is reached, the console port session is closed. The period must be in the range of 0 to 160 minutes. Entering 0 disables the timeout.	30

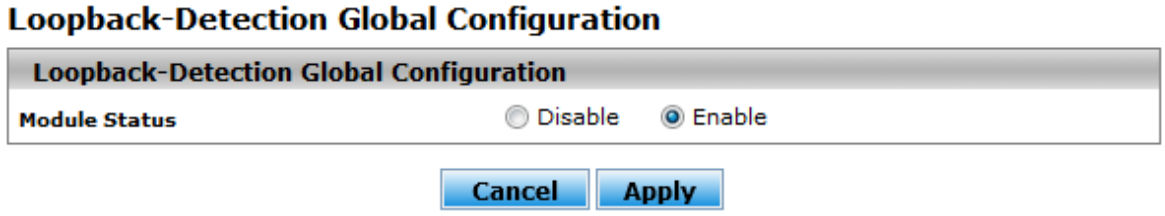
3.1.9 Loopback-Detection

A loopback error occurs when the keep-alive packet is looped back to the port that sent the keep-alive packet.The Delta managed switch provide the Loopback-Detection function to detecting the error in the network environment.

Notice:
We suggest that the Loopback-Detection function and redundancy protocol should not enable in the same time because the operating theory of these two functions are conflict.

3.1.9.1 Global Configuration

The module status of Loopback- Detection Global Configuration is used to enable/disable the Loopback-Detection feature.



Loopback-Detection Global Configuration

Description	Factory default
Module Status	
Specify whether the status in global configuration is activated or not.	Enable

3.1.9.2 Port Configuration

The parameters of Loopback-Detection should be set for each port.

Notice:
If you need to configure Loopback-Detection Port Configuration, you must enable the Loopback-Detection Global mode.

3

Loopback-Detection Port Configuration

Loopback-Detection Port Configuration

	Interface	Port Control	Recovery Mode	Recovery Interval
☐		-	-	
☐	0/1	Disable	Manual	300
☐	0/2	Disable	Manual	300
☐	0/3	Disable	Manual	300
☐	0/4	Disable	Manual	300
☐	0/5	Disable	Manual	300
☐	0/6	Disable	Manual	300
☐	0/7	Disable	Manual	300
☐	0/8	Disable	Manual	300
☐	po1	Disable	Manual	300
☐	po2	Disable	Manual	300
☐	po3	Disable	Manual	300

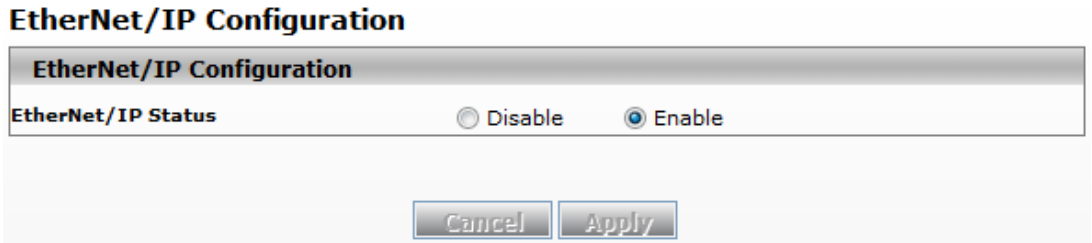
Apply Refresh

Loopback-Detection Port Configuration

Description	Factory default
Interface	
The interface number.	*interface number*
Port Control	
Enable/Disable the Loopback-Detection feature on the port.	Disable
Recovery Mode	
There are two recovery modes for recovering the blocking port. Loops occur as the reason for blocking the port. • **Auto Mode**: After the port is blocked, the port will be automatically linked up after a recovery interval. • **Manual Mode**: After the port is blocked, we have to manually enable the port. Follow Basic Setting > Port Setting > Port Settings (Admin Mode) to enable the blocking port.	Manual
Recovery Interval	
In Auto Mode, the blocking port will be linked up after a recovery interval. The unit is a second and the range is between 30 and 38400.	**300**

3.1.10 EtherNet/IP

The module status of EtherNet/IP is used to enable/disable the EtherNet/IP feature. If you need to set parameters, please refer to Appendix C EtherNet/IP.



Click Apply to cause the changes and occurring on the switch.

3.2 SNMP Manager

Simple Network Management Protocol (SNMP) is an application protocol used for exchanging management information between network devices. SNMP is a member of the TCP/IP protocol suite. SNMP v1, v2c and v3 are supported on the Delta switch, and it is enabled by default.
The Delta switch supports standard public MIBs for standard functionality and private MIBs that provide additional functionality. You can use SNMP to enable or disable authentication traps, cold-start and warm-start functionality traps, link up and link down traps, Spanning Tree Protocol (STP) traps, SFP traps, and password and IP address change traps.

> **IMPORTANT:**
> **Make sure that you save the configuration in the Save Configuration page after you have applied the configuration changes. (Save Config→Save Configuration) If you do not save the configuration, then the configuration will be cleared after the switch is rebooted.**

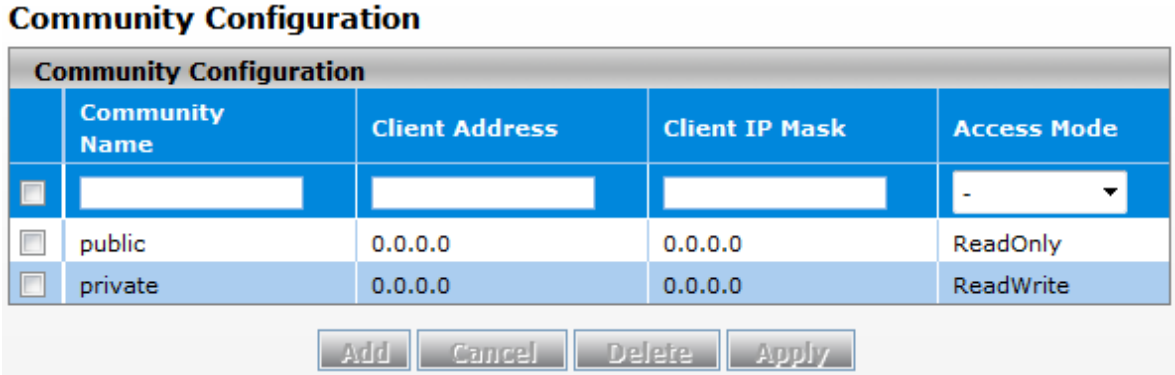
3.2.1 SNMP v1/v2c

SNMP version 1 (SNMP v1) is the initial implementation of the SNMP protocol. The authentication of clients is performed by a "community string", like a type of password, which is transmitted in clear text.
SNMP v2c revises version 1 and includes improvements of performance, security, confidentiality, and manager-to-manager communications. It adds a GetBulkRequest command; it sends iterative GetNextRequests for retrieving large amounts of management data in a single request.

3.2.1.1 Community Configuration

There are two default communities preconfigured for SNMP v1 and SNMP v2c:

- **public:** All IP addresses can be accessed with a read-only permission.
- **private:** All IP addresses can be accessed with a read/write permission.



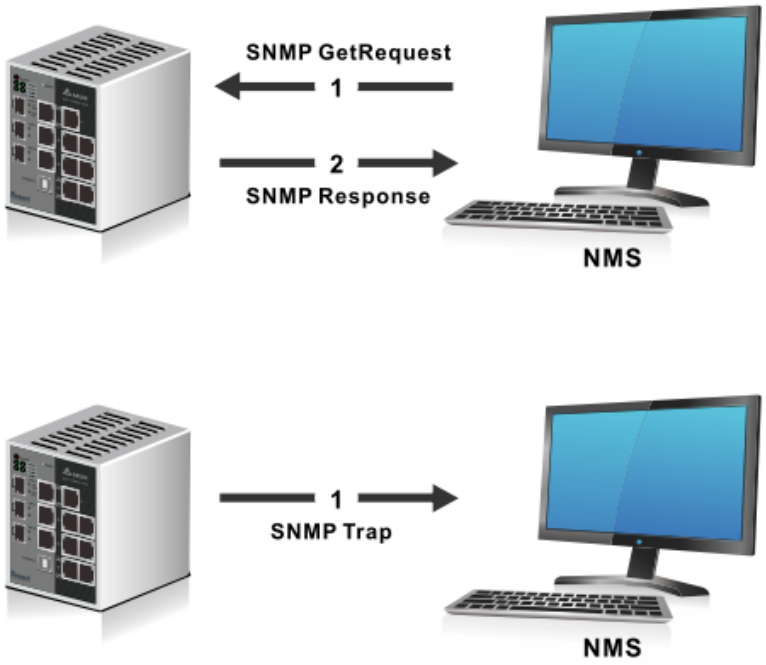
Community Configuration

Description	Factory default
Community Name	
Enter a case-sensitive string. The maximum length is 16 characters. The maximum community is 10.	None
Client Address	
Enter the client's IP address. Any IP address can be accessed if the IP address is 0.0.0.0.	0.0.0.0
Client IP Mask	
Enter the client's IP mask. All addresses allow accesses that are associated with a single client's IP address. For example, the client's IP address is 192.168.1.X, and its subnet mask is 255.255.255.0. If the client's IP address is between 192.168.1.0 and 192.168.1.255, it is allowed to be accessed. If the client's IP address is 192.168.1.15, and its subnet mask is 255.255.255.255, only this client allows to be accessed.	0.0.0.0
Access Mode	
Specify the access mode: • **ReadOnly**: Only allow the client to read information. • **ReadWrite**: Only allow the client to read information and modify configuration.	None

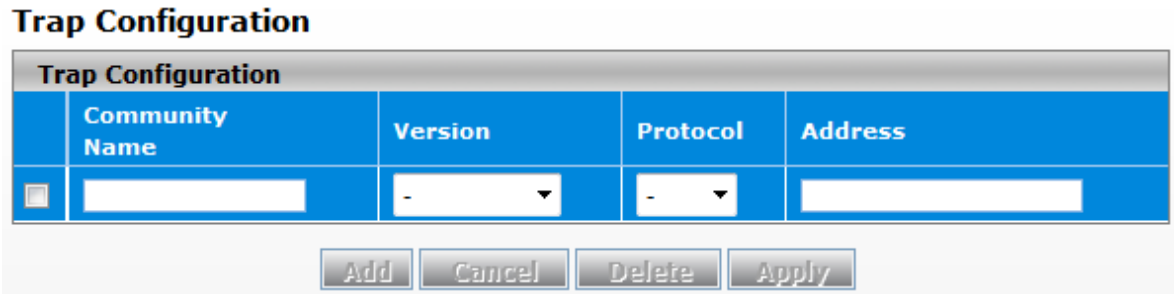
Notice:
The client address and client IP mask denote a range of IP addresses from which the SNMP clients can access the community on the switch.

3.2.1.2 Trap Configuration

If network engineers need to get information from an SNMP agent (network device), they usually use the SNMP software to poll information and get a response from an agent. But the SNMP Trap is the unsolicited trap which sends from the agent to the NMS (Network Management System).The operating theory is shown in the figure below.



An SNMP agent sends SNMP trap messages to the trap community (trap receiver). It monitors the switch for particular events or conditions, and generates trap messages based on these events or conditions.

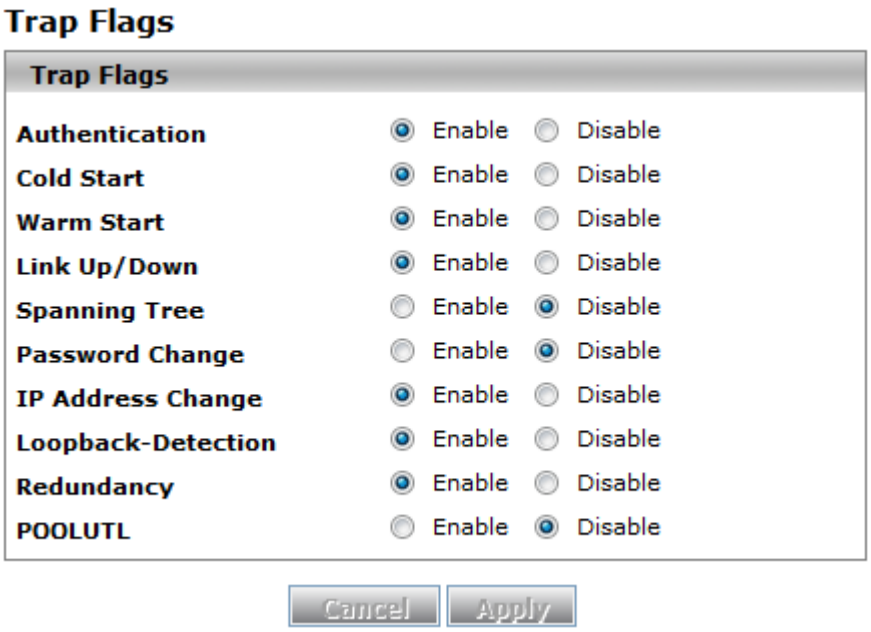


Trap Configuration

Description	Factory default
Community Name	
Enter a case-sensitive string. The maximum length is 16 characters. The maximum trap is 10.	None
Version	
Specify the SNMP version that is used for the trap community: • **SNMP v1**: Uses SNMP v1 to send traps to the trap community. • **SNMP v2c**: Uses SNMP v2c to send traps to the trap community.	None
Protocol	
Specify the IP version that is used for the trap community: • **IPv4**: Sends traps to an IPv4 address. Input an IPv4 address in the Address field. • **IPv6**: Sends traps to an IPv6 address. Input an IPv6 address in the Address field.	None
Address	
Enter an IPv4 or IPv6 address according to the selection in the Protocol drop-down list. For an IPv6 address, enter the address in the xxxx:xxxx:xxxx:xxxxx:xxxx:xxxx:xxxx:xxxx format.	None

3.2.1.3 Trap Flags

After you configure the trap communities, you also need to configure the SNMP traps which the switch can generate and send. When the switch detects the active trap which is an identified condition, a trap will be sent to the trap communities.



Trap Flags

Description	Factory default
Authentication	
Specify whether authentication traps are enabled. • **Enable**: Specify the switch which sends authentication trap messages. • **Disable**: Specify the switch which does not send authentication trap messages.	Enable
Cold Start	
Specify whether cold-start traps are enabled. • **Enable**: Specify the switch which sends cold-start trap messages. • **Disable**: Specify the switch which does not send cold-start trap messages.	Enable
Warm Start	
Specify whether warm-start traps are enabled. • **Enable**: Specify the switch which sends warm-start trap messages. • **Disable**: Specify the switch which does not send warm-start trap messages.	Enable
Link Up/Down	
Specify whether link status traps are enabled. • **Enable**: Specify the switch which sends link status trap messages when a link comes up or goes down. This is the default setting. • **Disable**: Specify the switch which does not send link status trap messages.	Enable
Spanning Tree	
Specify whether spanning tree traps are enabled. • **Enable**: Specify the switch which sends spanning tree trap messages. • **Disable**: Specify the switch which does not send spanning tree trap messages.	Disable
Password Change	
Specify whether Password Change traps are enabled. • **Enable**: Specify the switch which sends Password Change trap messages. • **Disable**: Specify the switch which does not send Password Change messages.	Disable
IP Address Change	
Specify whether IP Address Change traps are enabled. • **Enable**: Specify the switch which sends IP Address Change trap messages. • **Disable**: Specify the switch which does not send IP Address Change messages.	Enable
Loopback-Detection	Enable
Specify whether Loopback-Detection traps are enabled. • **Enable**: Specify the switch which sends Loopback-Detection trap messages. • **Disable**: Specify the switch which does not send Loopback-Detection messages	
Redundancy	Enable
Specify whether Redundancy traps are enabled. • **Enable**: Specify the switch which sends Redundancy trap messages. • **Disable**: Specify the switch which does not send Redundancy messages	
POOLUTL	Disable
Specify whether POOLUTL traps are enabled. • **Enable**: Specify the switch which sends POOLUTL trap messages. • **Disable**: Specify the switch which does not send POOLUTL messages	

3.2.2 SNMP v3

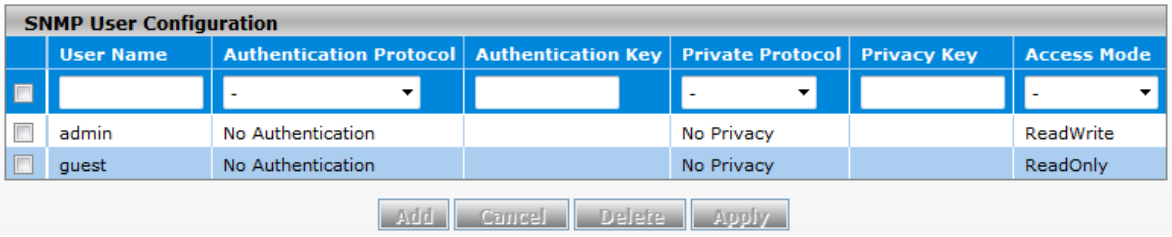
SNMP v3 primarily added security and remote configuration enhancements.The authentication in SNMP v1 and v2c uses a password (community string) sent in clear text between a manager and an agent. But the SNMP v3 message contains security parameters which are encoded as an octet string. You can choose the authentication protocol which you need for each user account.

3.2.2.1 User Configuration

The following default users are preconfigured for SNMP v3:

- **admin:** All admin users can access data with the read/write permission.
- **guest:** All IP guest users can access data with the read-only permission.

SNMP User Configuration



SNMP User Configuration

Description	Factory default
User Name	
Enter a case-sensitive string. The maximum length is 32 characters.	None
Authentication Protocol	
Specify the authentication protocol, if any, for the user: • **No Authentication**: Users can access data without authentication. If you select this item, the Authentication Key, Privacy Protocol, and Privacy Key fields are masked out and can not be configured. • **HMAC-MD5**: Users are authenticated by Hash-based Message Authentication Code (HMAC) with MD5. If you select this item, please enter a password in the Authentication Key field. • **HMAC-SHA**: Users are authenticated by HMAC with SHA-1. If you select this item, please enter a password in the Authentication Key field.	None
Authentication Key	
If the authentication protocol is HMAC-MD5 or HMAC-SHA, please enter a case-sensitive string for the password. The maximum length is 40 characters.	None
Private Protocol	
If the authentication protocol is HMAC-MD5 or HMAC-SHA, you can specify whether to use an SNMP v3 privacy protocol (encryption) for the user: • **No Privacy**: The users can access data without encryption. • **DES**: User communication is encrypted by Data Encryption Standard (DES). You need to enter a password in the Privacy Key field.	None
Privacy Key	
If the privacy protocol is DES, please enter a case-sensitive string for the password. The maximum length is 40 characters.	None
Access Mode	
Specify the access mode: • **ReadOnly**: The client can only have read permission to get information. • **ReadWrite**: The client can both have the read permission and the configuration permission to modify the information.	None

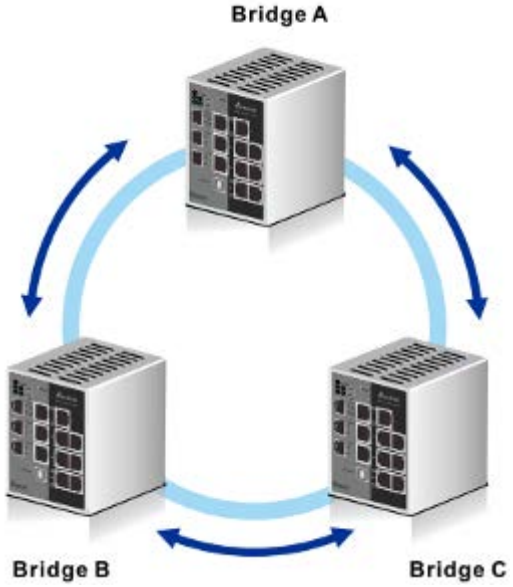
3.3 Network Redundancy

In some network environments, users need to set up redundant loops in the network to provide a backup path for disconnection or a network device breakdown. But if there are many network devices in the network, then each host needs to spend more time and cross many network devices to associate with each other. And sometimes the disconnection happens in a busy network, so the network must recover in a short time. Setting up redundancy on your network helps protect critical links against failure, protects against network loops, and keeps network downtime at a minimum. For example, if the Delta switch is used as a key communication component of a production line, several minutes of downtime may cause a big loss in production and revenue.

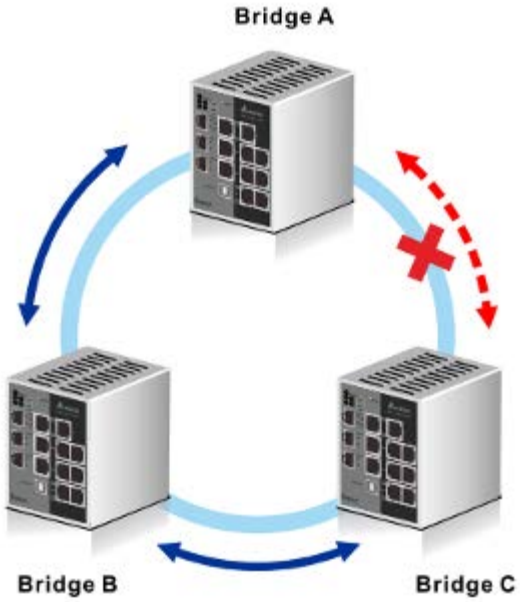
> **IMPORTANT:**
> **Make sure that you save the configuration in the Save Configuration page after you have applied the configuration changes. (Save Config→Save Configuration) If you do not save the configuration, then the configuration will be cleared after the switch is rebooted.**

3.3.1 STP

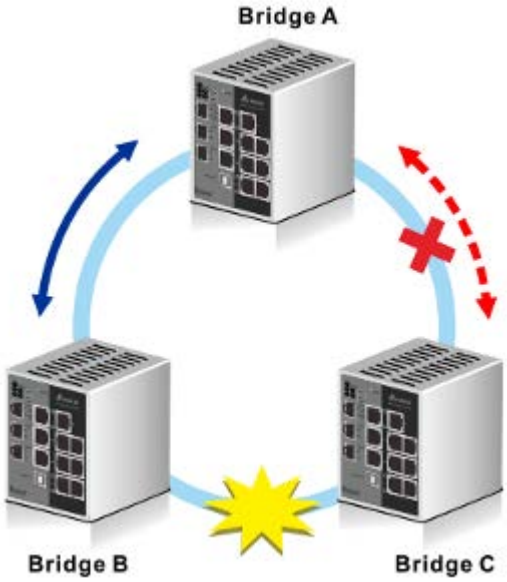
Spanning Tree Protocol (STP) provides a tree topology that helps reduce link failure in a network, find one path between end devices and protect loops in the network. Bridge Protocol Data Unit (BPDU) includes the calculation of information and it is used to negotiate between switches and establish STP. STP is a bridge based system and it defines 5 kinds of port statuses: blocking, listening, learning, forwarding and disabling. If the status of the blocking changes to forwarding, STP needs to spend more than 30 seconds.
Rapid Spanning Tree Protocol (RSTP) was defined by IEEE in 2001. RSTP provides faster tree convergence after a topology changes. Sometimes it only needs to spend a few hundred milliseconds. And RSTP can be backward compatible with standard STP.
The Delta switch supports different protocols to support communication redundancy. When configuring a redundant ring, all switches on the same ring must be configured to use the same redundant protocol. STP/RSTP can let you establish a redundant ring and protect the loop in a network, as shown in the figure below.



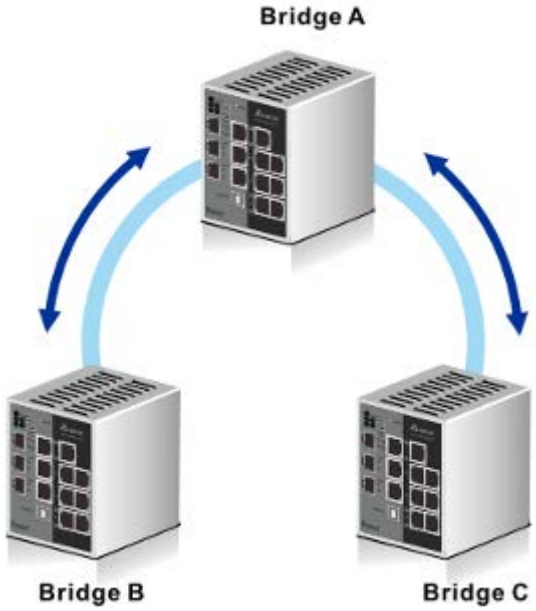
If STP/RSTP is enabled, it will detect duplicate paths, calculate the cost of each path and block the lowest cost path (ex. the path between A and C) from forwarding traffic. So bridges can communicate with each other without loops, as shown in the figure below.



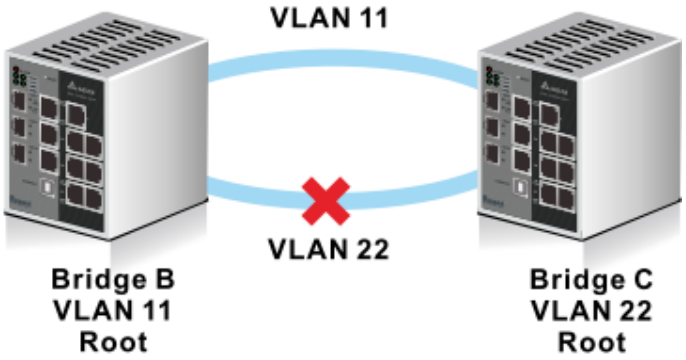
If the link failure is detected between bridge B and bridge C, STP/RSTP will start to reconfigure the network, as shown in the figure below.



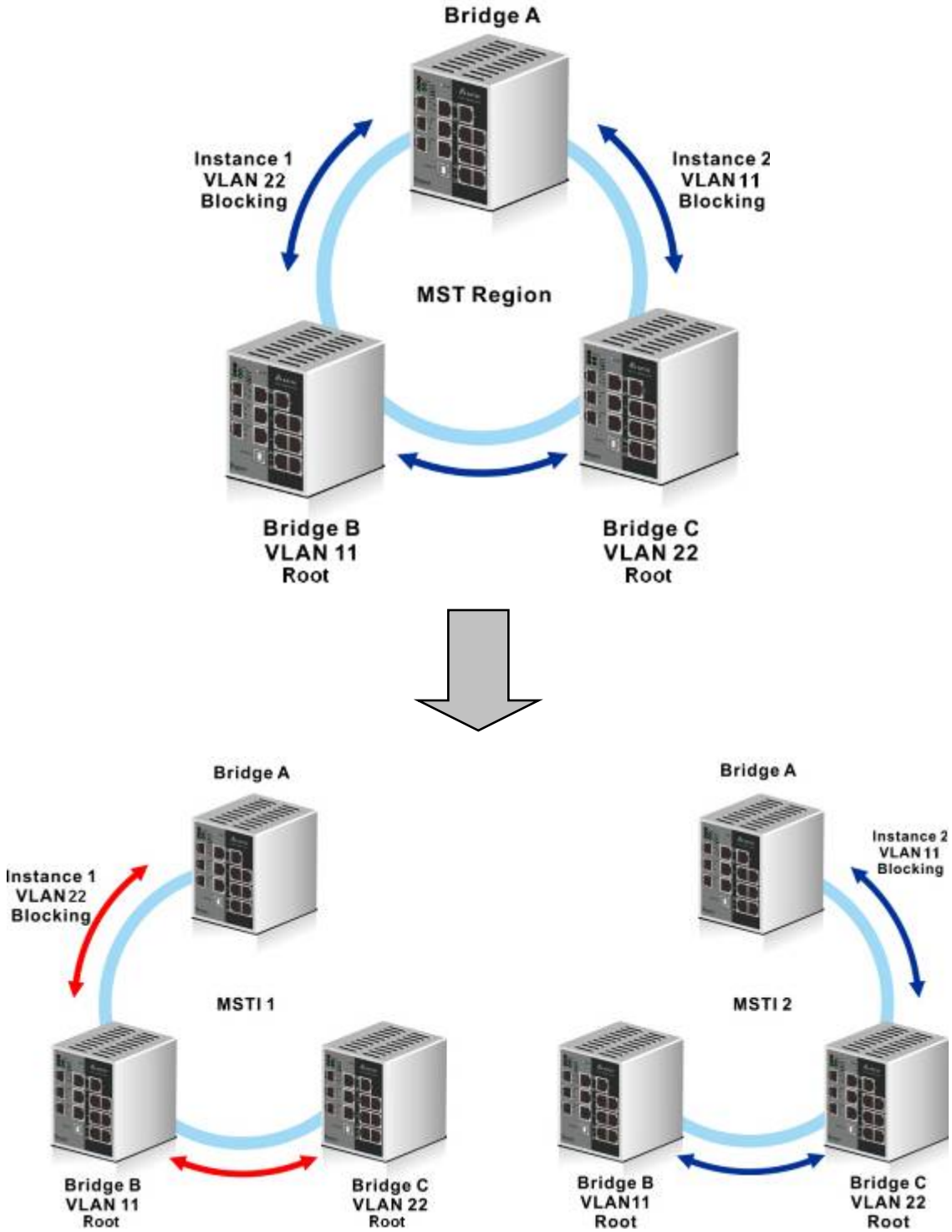
Then the traffic between bridge B and bridge C will flow through bridge A, as shown in the figure below.



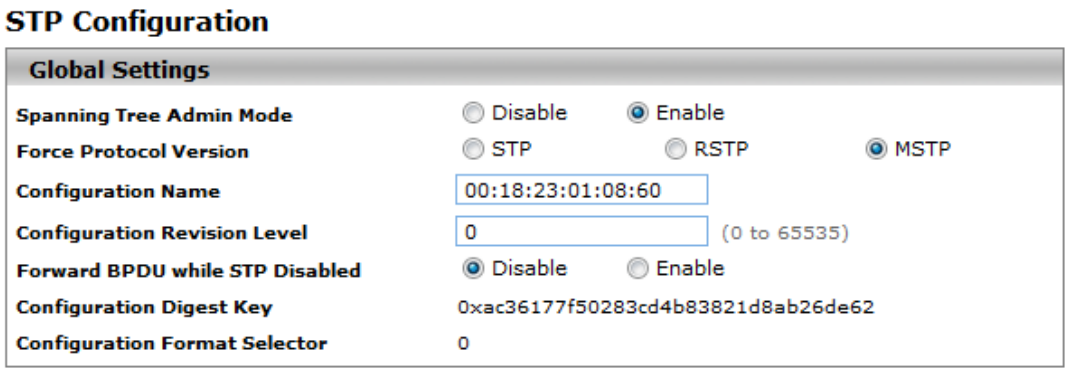
But STP/RSTP can not support more VLANs in your network topology. If there are 2 VLANs between 2 bridges, one path is blocked when STP/RSTP is enabled. So IEEE defined an extension to RSTP to further develop the usefulness of VLANs.



Multiple Spanning Tree Protocol (MSTP) is an extension protocol of RSTP. It can provide an independent spanning tree for different VLANs. MSTP builds a separate Multiple Spanning Tree (MST) for each instance. And MST Region may include multiple MSTP instances. The operating theory is shown in the figure below.

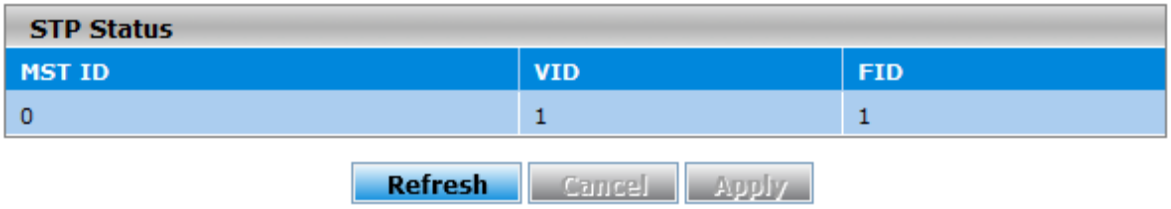

Bridge A
Instance 1
VLAN 22
Blocking
Instance 2
VLAN 11
Blocking
MST Region
Bridge B
VLAN 11
Root
Bridge C
VLAN 22
Root
Bridge A
Instance 1
VLAN 22
Blocking
MSTI 1
Bridge B
VLAN 11
Root
Bridge C
VLAN 22
Root
Bridge A
Instance 2
VLAN 11
Blocking
MSTI 2
Bridge B
VLAN 11
Root
Bridge C
VLAN 22
Root

3.3.1.1 STP Configuration



Global Settings Description

Description	Factory default
Spanning Tree Admin Mode	
Specify the admin mode of STP on the switch: • **Disable:** STP is disabled. The settings do not take effect after you have applied them, but you still can configure STP. • **Enable:** STP is enabled. The settings take effect after you have applied them.	Enable
Force Protocol Version	
Specify the version of the STP protocol: • **STP:** Spanning Tree Protocol. • **RSTP:** Rapid Spanning Tree Protocol. • **MSTP:** Multiple Spanning Tree Protocol.	MSTP
Configuration Name	
Enter the STP identifier for the switch. You can configure alphanumeric characters and special characters, and the maximum length is 32.	MAC address of the switch
Configuration Revision Level	
Enter an identifier that specifies the current configuration. The number must be in the range of 0 to 65535.	0
Forward BPDU while STP Disabled	
Specify whether spanning tree bridge protocol data units (BPDUs) are forwarded: • **Disable:** When STP is disabled, Spanning tree BPDUs are not forwarded. • **Enable:** When STP is disabled, Spanning tree BPDUs are forwarded.	Disable
Configuration Digest Key	
This field displays a calculated value from the MSTP configuration. The switches are qualified by the key and the function in the same region.	Fixed
Configuration Format Selector	
This field displays the configuration identifier format selector that is used.	0

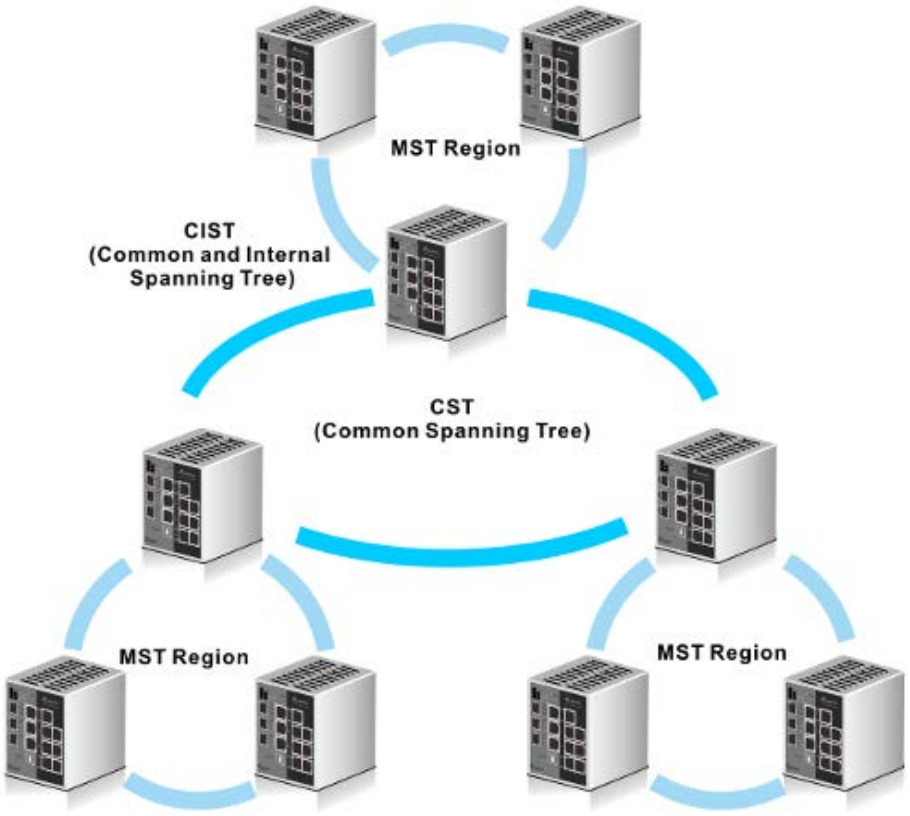


STP Status

Description	Factory default
MST ID	
The ID of the MST instance	0
VID	
The VLAN ID	1
FID	
The filtering ID (FID)	1

3.3.1.2 CST Configuration

Internal Spanning Tree (IST) is one of spanning trees in the MST region. Common Spanning Tree (CST) interconnects ISTs in the MST region. And Common and Internal Spanning Tree (CIST) consist of IST and CST. The operating theory is shown in the figure below.



CST Configuration

CST Configuration

Bridge Priority	32768	(0 to 61440)
Bridge Max Age (secs)	20	(6 to 40)
Bridge Hello Time (secs)	2	(1 to 2)
Bridge Forward Delay (secs)	15	(4 to 30)
Spanning Tree Maximum Hops	20	(6 to 40)
Dynamic Path Cost	◉ Disable	○ Enable
Extend System ID Status	◉ Disable	○ Enable

CST Status

Bridge Identifier	80:00:00:11:22:33:44:55
Time Since Topology Change	0 day 3 hr 49 min 48 sec
Topology Change Count	1
Designated Root	80:00:00:11:22:33:44:55
Root Path Cost	0
Root Port Identifier	00:00
Max Age (secs)	20
Forward Delay (secs)	15
Hold Time (secs)	1
CST Regional Root	80:00:00:11:22:33:44:55
CST Path Cost	0

Refresh | Cancel | Apply

CST Configuration

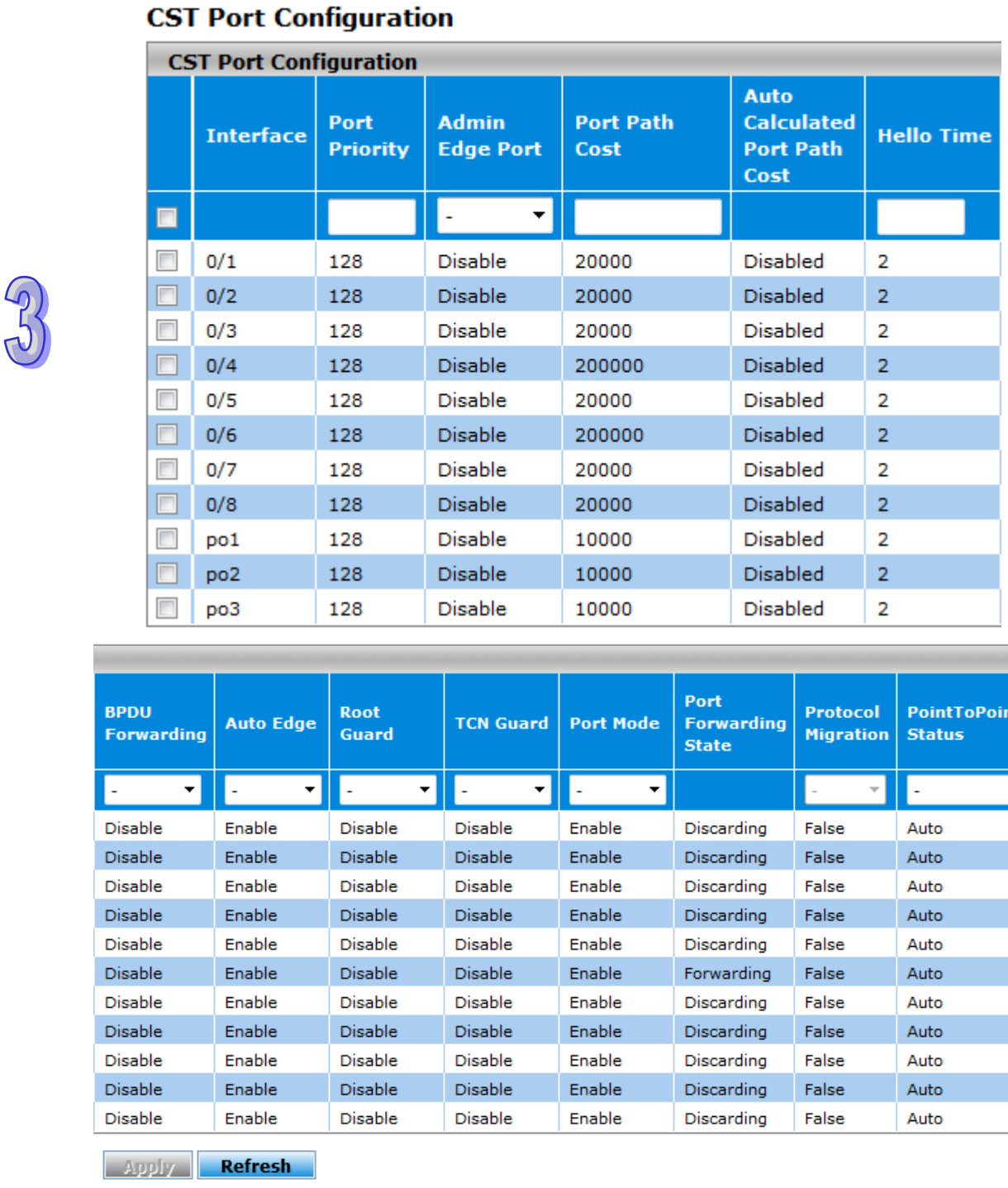
Description	Factory default
Bridge Priority	
Each switch or bridge is assigned a priority when they are running STP. After the devices exchange BPDUs, the lowest priority value becomes the root bridge. Enter the bridge priority value for the CIST. Enter a number that is a multiple of 4096 and it must be in the range of 0 to 61440.	32768
Bridge Max Age (secs)	
Enter the maximum age time for the CIST in seconds. This time is the period that a STP bridge or switch waits before implementing a topological change. The device will recognize itself as a root if it does not receive a hello message in the time of Bridge Max Age. Enter a number in the range of 6 to 40 seconds, considering that the period needs to be less than or equal to 2 *(Bridge Forward Delay–1) and greater than or equal to 2 * (Bridge Hello Time +1).	20
Bridge Hello Time (secs)	
The switch hello time for the CIST. This time is the period in seconds that a root bridge waits between configuration messages. The value is fixed at 2 seconds.	2
Bridge Forward Delay (secs)	
Enter the switch forward delay time, which is the period in seconds that a bridge remains in a listening and learning state before forwarding packets. Enter a number in the range of 4 to 30 seconds, considering that the period needs to be greater than or equal to (Bridge Max Age / 2) + 1.	15
Spanning Tree Maximum Hops	
Enter the maximum number of bridge hops; the information for a CST instance can	20

Description	Factory default
travel before being discarded. Enter a number in the range of 6 to 40.	
Dynamic Path Cost	
Specify whether the path cost is automatically calculated by selecting one of the following radio buttons: • **Disable:** The path cost is not automatically calculated. • **Enable:** The path cost is automatically calculated.	Disable
Extend System ID Status	
Specify whether the extended system identifier is added to the bridge priority by selecting one of the following radio buttons: • **Disable:** The extended system identifier is not added to the bridge priority. • **Enable:** The extended system identifier is added to the bridge priority. For example, bridge priority is 32768, for VLAN 1, the priority will be 32768+1; for VLAN 2, the priority will be 32768+2.	Disable

CTS Status

Description	Factory default
Bridge Identifier	
The STP bridge identifier for the Common Spanning Tree (CST) on the switch. The identifier consists of the bridge priority and the base (fixed) MAC address of the switch.	MAC address
Time Since Topology Change	
The time that has passed since the last change of the CST topology occurred. The time is displayed in the day-hour-minute-second format.	day-hour-minute-second
Topology Change Count	
The number of times the CST topology has changed.	0
Designated Root	
The STP bridge identifier of the root bridge. The identifier consists of the bridge priority and the base MAC address of the root bridge.	MAC address
Root Path Cost	
The path cost to the designated root for the CST.	0
Root Port Identifier	
The interface that provides access to the designated root for the CST.	00:00
Max Age (secs)	
The timer that controls the maximum time that passes before an STP bridge port saves its configuration BPDU.	20
Forward Delay (secs)	
The value that is derived from the bridge forward delay parameter of the STP root port.	15
Hold Time (secs)	
The minimum period between the transmissions of configuration BPDUs.	1
CST Regional Root	
The priority and the base MAC address of the CST regional root.	MAC address
CST Path Cost	
The path cost to the CST tree regional root.	0

3.3.1.3 CST Port Configuration



CST Port Configuration

CST Port Configuration

	Interface	Port Priority	Admin Edge Port	Port Path Cost	Auto Calculated Port Path Cost	Hello Time
			-			
	0/1	128	Disable	20000	Disabled	2
	0/2	128	Disable	20000	Disabled	2
	0/3	128	Disable	20000	Disabled	2
	0/4	128	Disable	200000	Disabled	2
	0/5	128	Disable	20000	Disabled	2
	0/6	128	Disable	200000	Disabled	2
	0/7	128	Disable	20000	Disabled	2
	0/8	128	Disable	20000	Disabled	2
	po1	128	Disable	10000	Disabled	2
	po2	128	Disable	10000	Disabled	2
	po3	128	Disable	10000	Disabled	2

BPDU Forwarding	Auto Edge	Root Guard	TCN Guard	Port Mode	Port Forwarding State	Protocol Migration	PointToPoint Status
-	-	-	-	-		-	-
Disable	Enable	Disable	Disable	Enable	Discarding	False	Auto
Disable	Enable	Disable	Disable	Enable	Discarding	False	Auto
Disable	Enable	Disable	Disable	Enable	Discarding	False	Auto
Disable	Enable	Disable	Disable	Enable	Discarding	False	Auto
Disable	Enable	Disable	Disable	Enable	Discarding	False	Auto
Disable	Enable	Disable	Disable	Enable	Forwarding	False	Auto
Disable	Enable	Disable	Disable	Enable	Discarding	False	Auto
Disable	Enable	Disable	Disable	Enable	Discarding	False	Auto
Disable	Enable	Disable	Disable	Enable	Discarding	False	Auto
Disable	Enable	Disable	Disable	Enable	Discarding	False	Auto
Disable	Enable	Disable	Disable	Enable	Discarding	False	Auto

Apply Refresh

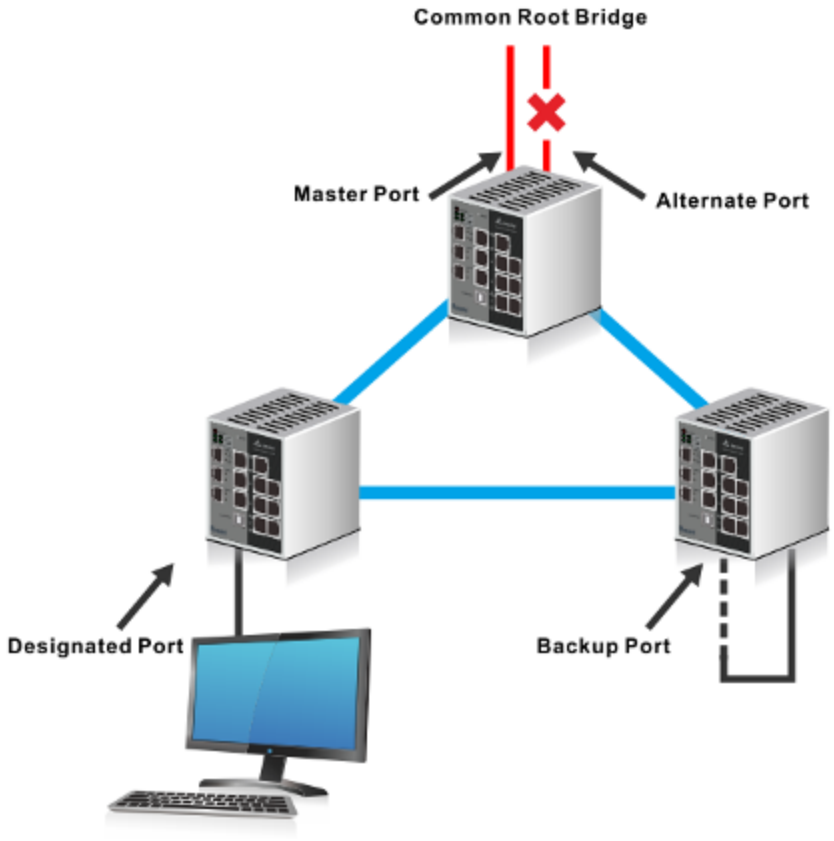
CST Port Configuration

Description	Factory default
Interface	
This field displays the interface number or port channel number.	*interface number*
Port Priority	
Enter the priority for the interface in the CIST. Enter a value between 0 and 240 that is a multiple of 16. The default priority is 128.	128
Admin Edge Port	
All ports directly connected to end stations can not create bridging loops in the network. Therefore, the edge port directly changes to the forwarding state, and skips the listening and learning stages. Specify whether the interface is an edge port in the CIST: • **Enable:** The interface is an edge port. • **Disable:** The interface is not an edge port.	Disable
Port Path Cost	
Leave the existing path cost, or enters a new path cost that is used for the interface in the CIST. Enter a number in the range of 1 to 200,000,000. Enter a blank (that is, remove the number and make sure that there is no space character in the field) to reset the path cost.	20000
Auto Calculated Port Path Cost	
This field shows whether you have globally enabled or disabled the dynamic path cost on the CST Configuration screen.	Disable
Hello Timer	
The hello time for the interface in the CIST. This time is the period in seconds that the interface waits between configuration messages. Enter 1 or 2 seconds. **Notice:** You can set the hello time only when the STP operation mode is MSTP.	2
BPDU Forwarding	
Specify whether the interface sets the mcheck flag to forward BPDUs: • **Enable:** Depending on the STP operation mode, RST or MST BPDUs are forwarded. • **Disable:** BPDUs are not forwarded.	Disable
Auto Edge	
Specify whether the interface automatically becomes an edge port if it does not process BPDUs for a while: • **Enable:** The interface becomes an edge port. • **Disable:** The interface does not become an edge port.	Enable
Root Guard	
Specify whether the root guard mode can cause the interface to discard any superior information received by the interface to prevent the root of the device from changing. When this situation occurs, the interface enters the discarding state and no longer forwards any packets: • **Enable:** The interface can enter the discarding state. • **Disable:** The interface can not enter discarding state.	Disable
TCN Guard	
Specify whether the topology change notification (TCN) guard restricts the interface from propagating the topology change information. This means that even if a port receives a BPDU with the topology change flag set to true, the port will not flush its MAC address table and send out a BPDU with a topology change flag set to true. • **Enable:** The interface can propagate the topology change information. • **Disable:** The interface can not propagate the topology change information.	Disable
Port Mode	
Specify the Spanning Tree Protocol (STP) administrative mode that is associated with the port or port channel:	Enable

Description	Factory default
• **Disable:** STP is disabled for the port or port channel. • **Enable:** STP is enabled for the port or port channel.	
Port Forwarding State	
This field displays whether the port is up and forwards traffic (Forwarding) or down and discards traffic (Discarding).	Discarding
Protocol Migration	
Force the specified port to set the mcheck flag to transmit RST or MST BPDUs: • **True:** The interface can receive the BPDU flood. • **False:** The interface can not receive the BPDU flood.	False
PointToPoint Status	
Specify the point-to-point status of the interface in the CIST: • **ForceTrue:** The interface has a point-to-point connection to a switch, bridge, or end node, irrespective of the actual connection. • **ForceFalse:** The interface does not have a point-to-point connection to a switch, bridge, or end node, irrespective of the actual connection. • **Auto:** The type of connection is automatically detected.	hAuto

3.3.1.4 CST Port Status

The port role types of the interface:



- **Root Port:** It is a concept of STP. Every non-root switch has one root port. The lowest cost of the path to the root switch will be the root port.
- **Master Port:** It is a concept of MSTP. It must meet two conditions: one is the root port in CIST; the other one is an edge port. The edge port is the port which connects two regions.
- **Designated Port:** The port responsible for forwarding data to the downstream network segment or device.
- **Alternate Port:** The standby port for the root port or master port. If a root port or master port is blocked, the alternate port becomes the new root port or master port.

- **Backup Port:** The backup port of designated ports. When a designated port is blocked, the backup port becomes a new designated port and starts to forward data without delay. When a loop occurs while two ports of the same MSTP device are interconnected, the device will block either of the two ports, and the backup port is the port to be blocked.

CST Port Status

CST Port Status

Interface	Port ID	Port Forwarding State	Port Role	Designated Root	Designated Cost	Root Priority	Designated Bridge
0/1	80:01	Discarding	Disabled	80:00:00:18:23:01:20:61	0	32768	80:00:00:18:23:01:20:61
0/2	80:02	Discarding	Disabled	80:00:00:18:23:01:20:61	0	32768	80:00:00:18:23:01:20:61
0/3	80:03	Discarding	Disabled	80:00:00:18:23:01:20:61	0	32768	80:00:00:18:23:01:20:61
0/4	80:04	Discarding	Disabled	80:00:00:18:23:01:20:58	0	32768	80:00:00:18:23:01:20:58
0/5	80:05	Discarding	Disabled	80:00:00:18:23:01:20:61	0	32768	80:00:00:18:23:01:20:61
0/6	80:06	Forwarding	Designated	80:00:00:18:23:01:20:61	0	32768	80:00:00:18:23:01:20:61
0/7	80:07	Discarding	Disabled	80:00:00:18:23:01:20:61	0	32768	80:00:00:18:23:01:20:61
0/8	80:08	Discarding	Disabled	80:00:00:18:23:01:20:61	0	32768	80:00:00:18:23:01:20:61
po1	80:09	Discarding	Disabled	80:00:00:18:23:01:20:61	0	32768	80:00:00:18:23:01:20:61
po2	80:0a	Discarding	Disabled	80:00:00:18:23:01:20:61	0	32768	80:00:00:18:23:01:20:61
po3	80:0b	Discarding	Disabled	80:00:00:18:23:01:20:61	0	32768	80:00:00:18:23:01:20:61

Refresh

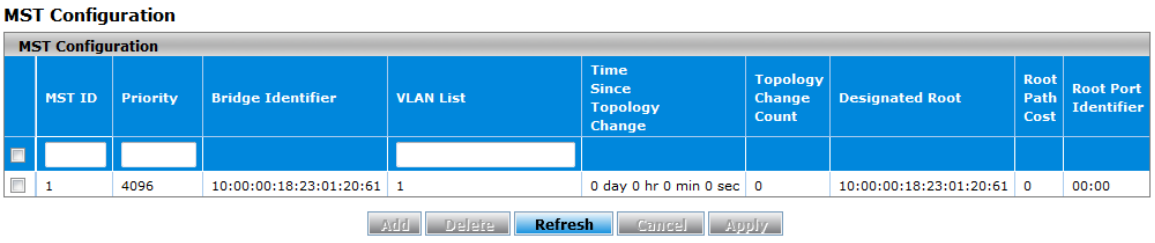
Designated Port	Edge Port	Point-to-Point MAC	CST Regional Root	Regional Root Priority	Regional Path Cost	CST Path Cost
80:01	Disabled	False	80:00:00:18:23:01:20:61	32768	0	20000
80:02	Disabled	False	80:00:00:18:23:01:20:61	32768	0	20000
80:03	Disabled	False	80:00:00:18:23:01:20:61	32768	0	20000
80:07	Disabled	True	80:00:00:18:23:01:20:61	32768	0	200000
80:05	Disabled	False	80:00:00:18:23:01:20:61	32768	0	20000
80:06	Enabled	True	80:00:00:18:23:01:20:61	32768	0	200000
80:07	Disabled	False	80:00:00:18:23:01:20:61	32768	0	20000
80:08	Disabled	False	80:00:00:18:23:01:20:61	32768	0	20000
80:09	Disabled	True	80:00:00:18:23:01:20:61	32768	0	10000
80:0a	Disabled	True	80:00:00:18:23:01:20:61	32768	0	10000
80:0b	Disabled	True	80:00:00:18:23:01:20:61	32768	0	10000

CST Port Status

Item	Description
Interface	The interface number or port channel number.
Port ID	The port identifier for the interface within the CST, which consists of the port priority and the interface number.
Port Forwarding State	The forwarding state of the interface. One of the following options is displayed: • **Discarding:** The interface is in the discarding mode; it can not forward traffic and can not learn new MAC addresses. • **Learning:** The interface is in the learning mode; it can not forward traffic, but it can learn new MAC addresses. • **Forwarding:** The interface is in the forwarding mode; it can forward traffic and learn new MAC addresses.

Item	Description
Port Role	The role type of the interface in the spanning tree: One of the following options is displayed: • Root • Master • Designated • Alternate • Backup • Disabled
Designated Root	The identifier of the root bridge of CIST. The identifier consists of the bridge priority and the base MAC address of the STP bridge.
Designated Cost	The path cost that is advertized by the designated port to the LAN. **Note:** Interfaces with a lower cost are less likely to be blocked if STP detects loops.
Root Priority	The priority of the CST root. The default root priority is 32768.
Designated Bridge	The identifier of the bridge with the designated port. The identifier consists of the bridge priority and the base MAC address of the STP bridge.
Designated Port	The port identifier on the designated bridge that offers the lowest cost to the LAN. The identifier consists of the port priority and the interface number. **Note:** If the port is the designated port, the identifiers in the Port ID and Designated Port fields are identical. If the port is not the designated port, that is, there is a root port and an alternate port, the identifiers in the Port ID and Designated Port fields are different.
Edge Port	The edge port status of the interface: • **Enabled:** The interface is an edge port. • **Disabled:** The interface is not an edge port.
Point-to-Point MAC	Connection types: • **True:** The connection is a point-to-point connection. • **False:** The connection is a shared LAN connection.
CST Regional Root	The identifier of the regional root bridge of CIST. The identifier consists of the bridge priority and the base MAC address of the STP bridge.
Regional Root Priority	The priority of the regional root. The default regional root priority is 32768.
Regional Path Cost	The path cost to the regional root.
CST Path Cost	The path cost to the CST tree regional root.

3.3.1.5 MST Configuration



MST Configuration settings

Description	Factory default
MST ID	
Enter an identifier for the MST instance. Enter a number in the range of 1 to 16.	None
Priority	
Enter the bridge priority. Enter a number between 0 and 61440 which is a multiple of 4096.	32768
VLAN List	
Enter the vlan id list. Enter a number in the range of 1 to 4096.	None

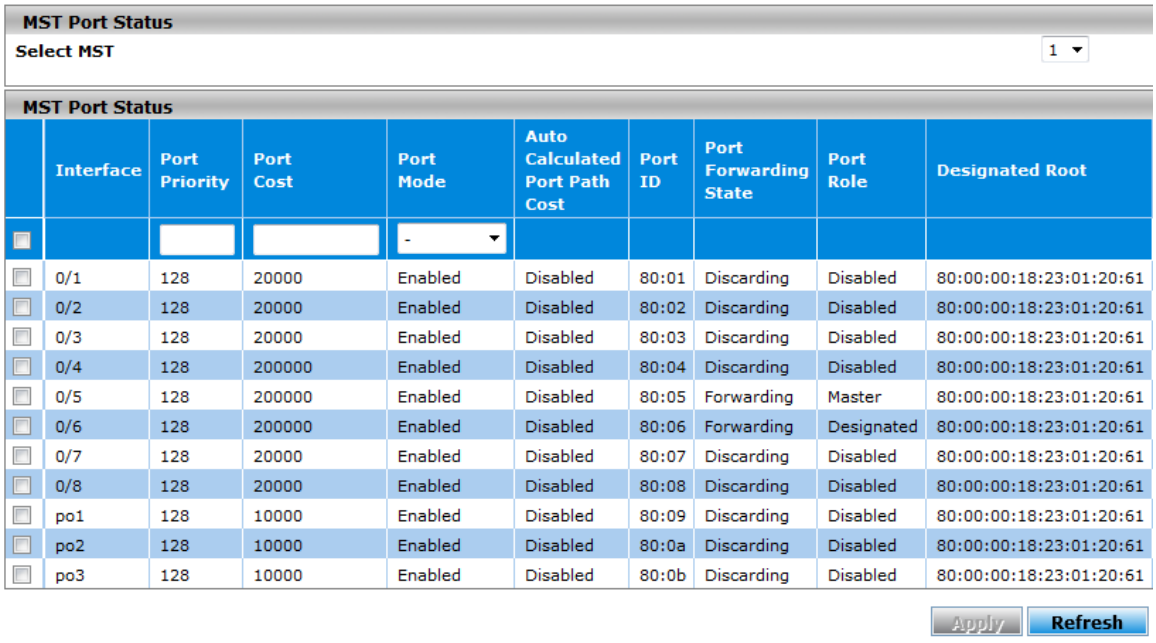
MST Configuration Table Information

Item	Description
MST ID	The identifier of the MST instance.
Priority	The bridge priority value for the MST instance.
Bridge Identifier	The bridge identifier for the MST instance. The bridge identifier is made up of the bridge priority and the base MAC address of the bridge.
VLAN List	The VLAN or VLANs to which the MST instance is mapped. You can enter a single VLAN ID or a number of VLAN IDs.
Time Since Topology Change	The time in seconds since the topology of the selected MST instance last changed.
Topology Change Count	The number of times the topology has changed the MST instance
Designated Root	The bridge identifier of the root bridge for the MST instance. The bridge identifier is made up of the bridge priority and the base MAC address of the root bridge.
Root Path Cost	The path cost to the designated root for the MST instance.
Root Port Identifier	The port identifier to access the designated root for the MST instance.

3.3.1.6 MST Port Status

The MST Port Status will show up after you finished the MST configuration settings.

MST Port Status



Designated Cost	Designated Bridge	Designated Port	Forward Transitions	Received BPDUs	Transmitted BPDUs	Invalid Received BPDUs
0	80:00:00:18:23:01:20:61	80:01	0	0	0	0
0	80:00:00:18:23:01:20:61	80:02	0	0	0	0
0	80:00:00:18:23:01:20:61	80:03	0	0	0	0
0	80:00:00:18:23:01:20:61	80:04	0	0	0	0
0	80:00:00:18:23:01:20:61	80:05	1	0	4	0
0	80:00:00:18:23:01:20:61	80:06	1	0	12	0
0	80:00:00:18:23:01:20:61	80:07	0	0	0	0
0	80:00:00:18:23:01:20:61	80:08	0	0	0	0
0	80:00:00:18:23:01:20:61	80:09	0	0	0	0
0	80:00:00:18:23:01:20:61	80:0a	0	0	0	0
0	80:00:00:18:23:01:20:61	80:0b	0	0	0	0

MST Port Status

Item	Description
Interface	This field shows the interface number or port channel number.
Port Priority	Enter the priority for the interface in the MST instance. Enter a value between 0 and 240 that is a multiple of 16. The default priority is 128.
Port Cost	Leave the default path cost, or entering a new path cost that is used for the interface in the MST instance. Enter a number in the range of 1 to 200,000,000. Enter zero (0) to reset the path cost. **Note:** The default path cost is 20,000 for a Gigabit Ethernet interface
Port Mode	Specify the administrative mode for the interface in the MST instance. • **Enable:** Enables STP for the interface. This is the default setting. • **Disable:** Disables STP for the interface.
Auto Calculated Port Path Cost	This field displays whether you have globally enabled or you can disable the dynamic path cost on the CST Configuration page.
Port Id	The port identifier, which consists of the port priority and the interface number
Port Forwarding State	The forwarding state of the interface in the MST instance. One of the following options is displayed: • **Discarding:** The interface is in the discarding mode; it can not forward traffic and can not learn new MAC addresses. • **Learning:** The interface is in the learning mode; it can not forward traffic, but it can learn new MAC addresses. • **Forwarding:** The interface is in the forwarding mode; it can forward traffic and learn new MAC addresses.
Port Role	The role types of the interface in the MST instance: One of the following options is displayed: • Root • Master • Designated • Alternate • Backup

Item	Description
	• Disabled
Designated Root	The identifier of the root bridge in the MST instance. The identifier consists of the bridge priority and the base MAC address of the MST root bridge.
Designated Cost	The path cost that is advertized by the designated port to the LAN. **Note:** Interfaces with a lower cost are less likely to be blocked if MST detects loops.
Designated Bridge	The identifier of the bridge with the designated port. The identifier consists of the bridge priority and the base MAC address of the MST bridge.
Designated Port	**Note:** The port identifier on the designated bridge that offers the lowest cost to the LAN. The identifier consists of the port priority and the interface number. **Note:** If the port is the designated port, the identifiers in the Port ID and Designated Port fields are identical. If the port is not the designated port, that is, there is a root port and an alternate port, the identifiers in the Port ID and Designated Port fields are different.
Forward Transitions	The number of forwarding transitions to other interfaces.
Received BPDUs	The number of BPDUs that were received on the interface for the MST instance.
Transmitted BPDUs	The number of BPDUs that were transmitted on the interface for the MST instance.
Invalid Received BPDUs	The number of invalid BPDUs that were received on the interface for the MST instance.

3.3.1.7 STP Statistics

STP Statistics

STP Statistics

Interface	Received MST BPDUs	Received RST BPDUs	Received Config BPDUs	Received TCN BPDUs	Transmitted MST BPDUs	Transmitted RST BPDUs	Transmitted Config BPDUs	Transmitted TCN BPDUs
0/1	0	0	0	0	0	0	0	0
0/2	0	0	0	0	0	0	0	0
0/3	604	0	0	0	3	0	0	0
0/4	0	0	0	0	5044	0	0	0
0/5	0	0	0	0	0	0	0	0
0/6	5886	0	0	0	11	0	0	0
0/7	0	0	0	0	0	0	0	0
0/8	0	0	0	0	0	0	0	0
po1	0	0	0	0	0	0	0	0
po2	0	0	0	0	0	0	0	0
po3	0	0	0	0	0	0	0	0

Refresh Clear

Received Invalid MST BPDUs	Received Invalid RST BPDUs	Received Invalid Config BPDUs	Received Invalid TCN BPDUs	Protocol Migration Count
0	0	0	0	0
0	0	0	0	0
0	0	0	0	0
0	0	0	0	0
0	0	0	0	0
0	0	0	0	0
0	0	0	0	0
0	0	0	0	0
0	0	0	0	0
0	0	0	0	0
0	0	0	0	0

STP Statistics

Item	Description
Interface	This field shows the interface number.
Received MST BPDUs	The number of MSTP BPDUs that were received on the interface.
Received RST BPDUs	The number of RSTP BPDUs that were received on the interface.
Received Config BPDUs	The number of configuration BPDUs that were received on the interface.
Received TCN BPDUs	The number of topology change notification (TCN) BPDUs that were received on the interface.
Transmitted MST BPDUs	The number of MSTP BPDUs that were transmitted on the interface.
Transmitted RST BPDUs	The number of RSTP BPDUs that were transmitted on the interface.
Transmitted Config BPDUs	The number of configuration BPDUs that were transmitted on the interface.
Transmitted TCN BPDUs	The number of TCN BPDUs that were transmitted on the interface.
Received Invalid MST BPDUs	The number of invalid MSTP BPDUs that were received on the interface.
Received Invalid RST BPDUs	The number of invalid RSTP BPDUs that were received on the interface.
Received Invalid Config BPDUs	The number of invalid configuration BPDUs that were received on the interface.
Received Invalid TCN BPDUs	The number of invalid TCN BPDUs that were received on the interface.
Protocol Migration Count	The number of times the interface received traffic from or transmitted traffic to a device that does not support RSTP or MSTP but STP only.

3.3.2 Redundancy

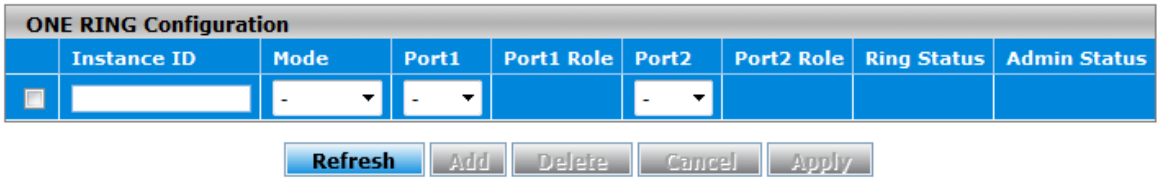
To keep the industrial network run non-stop, the Ethernet redundancy network is an essential feature in the industrial ethernet network. The Delta managed switch provides three topologies: ONE RING, ONE CHAIN and ONE COUPLING.
These redundancy topology operating theories look like STP, but when a connection failure was caused in the network, it can quickly recover the connection and work normally.

3.3.2.1 ONE RING Configuration

The ONE RING topology consists of nodes having two ports participating in ONE RING. There are two types of nodes, which namely master nodes and slave nodes. There can be only one master and up to 250 slave nodes.

Note:
The ports and LAGs which are the members of ONE RING should disable the STP mode and the Loopback-Detection mode.

ONE RING Configuration



ONE RING Configuration

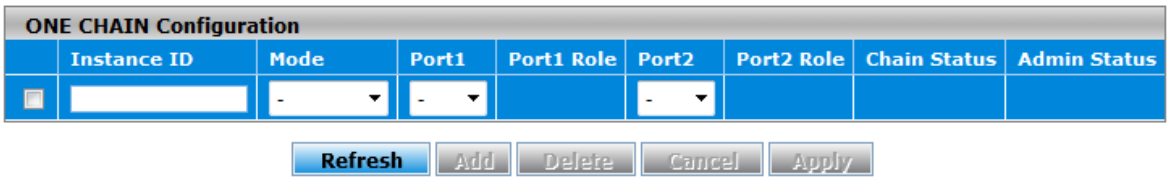
Item	Description
Instance ID	The ONE RING instance index. The range is 1 to 1000.
Mode	Defines the node role. The possible field values are: • **Master**: The master node manages the ring network, and there can only be one master node in a ring network. • **Slave:** The slave nodes forward the hello packets along the ring, and there are up to 250 slave nodes.
Port1	On the master node, it is the primary port. On the slave node, it is just one of the member ports.
Port2	On the master node, it is the backup port. On the slave node, it is just one of the member ports.
Ring Status	Defines the current ring status of the node. Master state: • **Discover**: The ring is not completed yet • **Monitor**: The ring is completed and healthy. • **Fault**: The ring failed. The backup path is activated. Slave State: • **Forwarding**: After the instance is created, it will stay at this state. • **Hold**: It is a middle state of the slave when 2 member ports are linked down->up.
Admin Status	The ONE RING instance entry status, including active, inactive, and etc.

3.3.2.2 ONE CHAIN Configuration

ONE CHAIN will connect a series of nodes to a LAN network.It consists of a head node, a tail node and a series of member nodes. The head node hosts the head port that is forwarded by default.The tail node hosts the tail port that is blocked by default. Any link failure caused in the ONE CHAIN will make the tail port as a forwarding port. The topology will be restored after the recovery from failure.

Note:
The ports and LAGs which are the members of ONE CHAIN should disable the STP mode and the Loopback-Detection mode.

ONE CHAIN Configuration



ONE CHAIN Configuration

Item	Description
Instance ID	The ONE CHAIN instance index. The range is 1 to 1000.
Mode	Defines the node role. The possible field values are: • **Head**: A Head node has one head port and one member port. • **Tail**: A Tail node has one tail port and one member port. The tail has two statuses: block and forwarding. • **Member**: A Member node has two member ports.
Port1	On the head node, it is the head port. On the member node, it is just one of the member ports. On the tail node, it is the tail port.
Port2	On the head node, it is the member port. On the member node, it is just one of the member ports. On the tail node, it is the member port.
Chain Status	Defines the current ring status of the node. On the Head node: • **Discover**: The chain is not completed yet. • **Monitor**: The chain is completed and healthy. The Head port is linked up, and no node is disconnected. • **Fault**: The chain is disconnected because the member node is linked down or the head port is linked down. • **Hold**: The Head port is linked down->up. On the Member node: • **Forwarding**: After the instance is created, it will stay at this state. • **Hold**: It is a middle state of the slave when 2 member ports are linked down->up. It changes to the Forwarding state when it receives the clear-FDB message or HOLD timer timeout. On the Tail node: • **Discover**: The chain is not completed yet. • **Monitor**: The chain is completed and healthy. • **Fault**: The chain failed. The backup path is activated.
Admin Status	The ONE CHAIN instance entry status, including active, inactive, and etc.

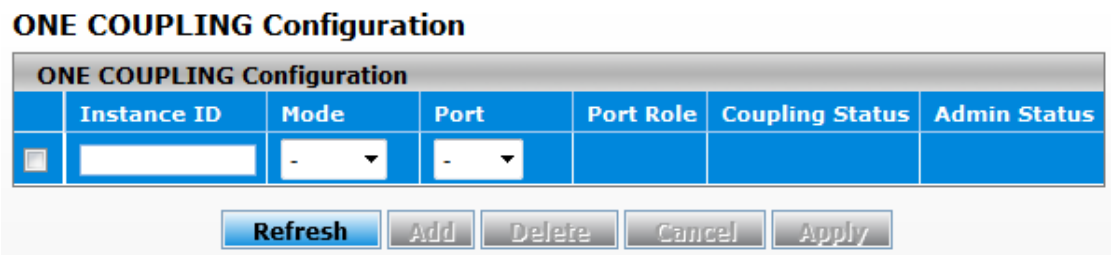
3.3.2.3 ONE COUPLING Configuration

ONE COUPLING is used to connect two redundant ring networks. There is a main path and a backup path, and two types of nodes which namely head nodes and tail nodes. The head node hosts the main path and the tail node hosts the backup path. The backup path will be blocked by default. When there is a failure in the main path, the backup path will get unblocked.

Only ONE RING will be configured with the head coupling node and the tail coupling node

Note:

The ports and LAGs which are the members of ONE COUPLING should disable the STP mode and the Loopback-Detection mode.



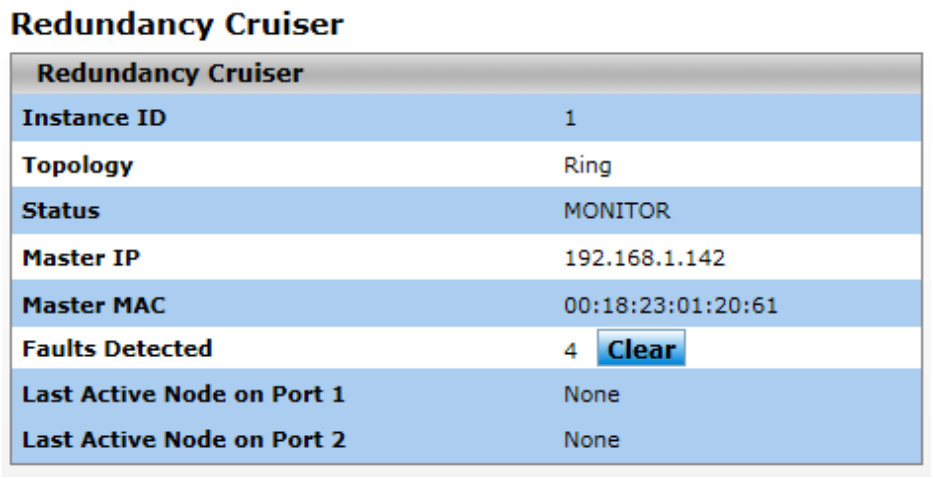
ONE COUPLING Configuration

Item	Description
Instance ID	The ONE COUPLING instance index. The range is 1 to 1000.
Mode	Defines the node role. The possible field values are: • **Head**: The Head node sends periodic status packets to the ring on both the ring ports. If the main path is disrupted, the head node will send a status message indicating the linking down. After the main path is restored, the main path ports will be initially set to the blocked state. • **Tail**: The tail node receives status messages from the head. The backup path is blocked by default. On detecting the main path failure, it will allow the forwarding in the backup path. On detecting the main path recovery, it will change the state of the backup path to the blocking.
Port	On the head node, it is the head port. On the tail node, it is tail port.
Coupling Status	Defines the current ring status of the node. Head state: • **Monitor**: The head port is linked up. • **Fault**: The head port is linked down. It will notify the tail node to activate the backup path. • **Link-Up**: The head port is linked up. If the head port is linked down at this state, it will change to Fault again. • **Hold**: After the Link-Up timer timeout occurs, the node will change to the HOLD state. Tail State: • **Discover**: The coupling is not completed yet. It waits for the head port link status message from the head node. • **Monitor**: The coupling is completed and healthy. • **Fault**: The coupling is disconnected.
Admin Status	The ONE COUPLING instance entry status, including active, inactive, and etc.

3.3.2.4 Redundancy Cruiser

Redundancy Cruiser is used to monitoring the ONE RING / ONE CHAIN / ONE COUPLING link status. The administrator can get the redundancy network information immediately if there is any link down or unknow situation happened.

Note:
This feature is only activated on the master node of ONE RING, the head node / tail node of ONE CHAIN, and the tail node of ONE COUPLING.



3

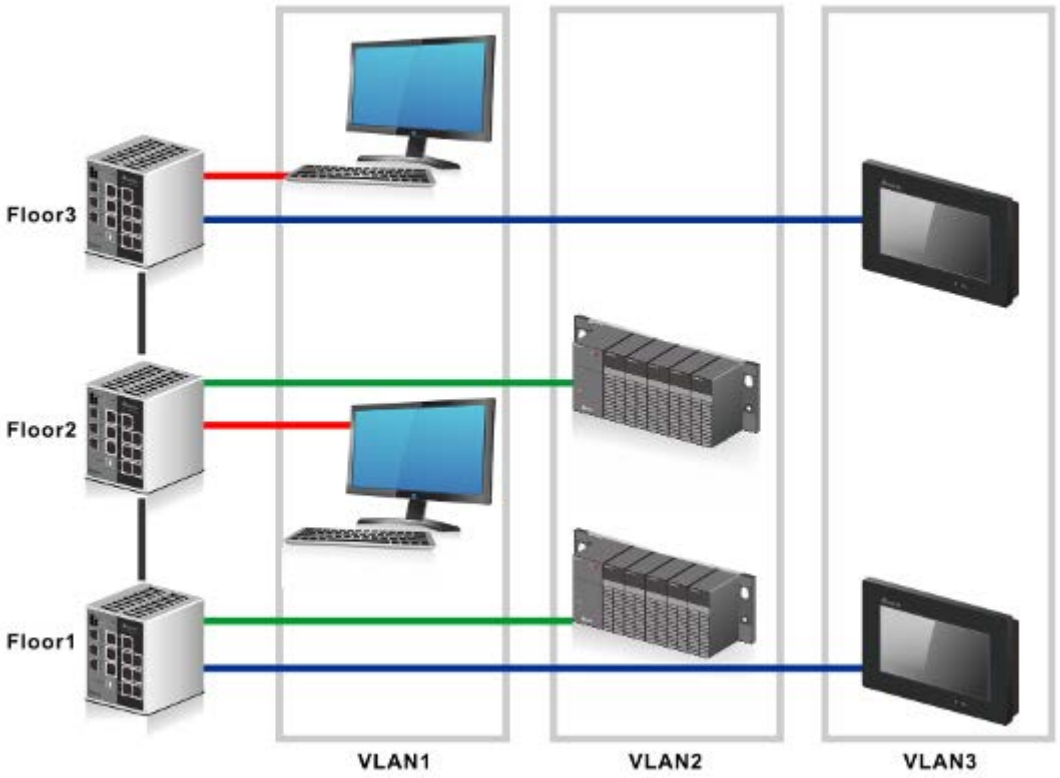
Redundancy Cruiser

Item	Description
Instance ID	The redundancy network instance index. The range is 1 to 1000.
Topology	This field shows the topology type which is monitoring. • Ring: It is cruising in ONE RING topology. • Chain: It is cruising in ONE CHAIN topology. • Coupling: It is cruising in ONE COUPLING topology.
Status	This field shows the network status which is under monitoring. • DISCOVER: The topology is not completed yet. • MONITOR: The topology is completed and healthy. • FAULT: The topology failed. The backup path is activated.
Master IP	This field shows the IP address of master node.
Master MAC	This field shows the MAC address of master node.
Faults Detected	This field shows the detection times which the status is change from DISCOVER state or FAULT state to MONITOR state.
Last Active Node on Port 1	This field shows the IP address and MAC address of the node which is on the path from the port1.
Last Active Node on Port 2	This field shows the IP address and MAC address of the node which is on the path from the port2.

3.4 Virtual LANs

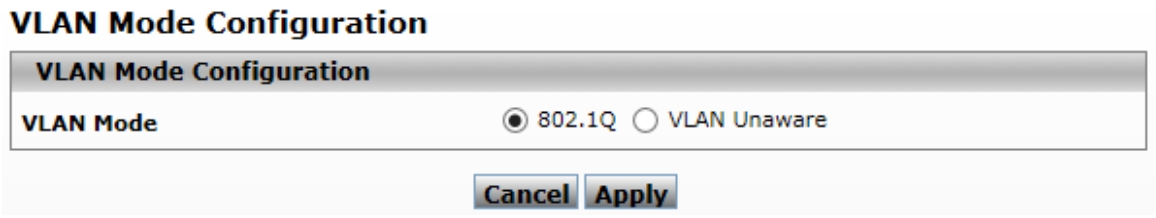
Virtual LAN (VLAN) is a logical group network. VLANs electronically separate interfaces on the same switch into different broadcast domains so that broadcast packets are not sent to all the interfaces on a single switch. VLAN allows the switch manager to isolate network traffic so that only members of the VLAN can receive traffic from the same VLAN members. VLAN also allows a user to access the network from a different place or switch. So VLAN provide security and flexibility.
For example: Configure department A, B, C to VLAN 1, 2, 3. Users can only access the resource which belongs to their department, so the resource in their department can be protected. And they can access the resource in a different floor, even though in a different place. So they do not need to stay in a fixed place to access the resource which belongs to their department.

IMPORTANT:
Make sure that you save the configuration in the Save Configuration page after you have applied the configuration changes. (Save Config→Save Configuration) If you do not save the configuration, then the configuration will be cleared after the switch is rebooted.



3.4.1 VLAN Mode Configuration

There are two VLAN modes can be chosen: 802.1Q and VLAN Unware.You can choose the properly VLAN mode on the Delta managed switch so that it can increase the efficiency of your network.



3

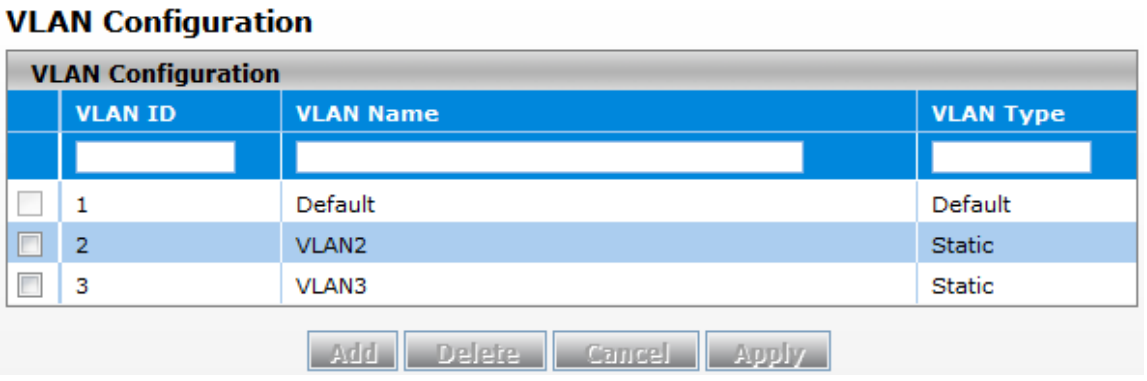
VLAN Mode Configuration

Status	Description
802.1Q	It logically segment the shared media LAN, forming virtual workgroup.They are redefine and optimize the basic Transparent Bridging functionalties like learning, forwarding, filtering and flooding, etc. The advantages of VLANs are: enhanced network security, controlled broadcast activity, members of the VLAN need not to be connected to the same LAN segment.
VLAN Unaware	It doesn't check the VLAN tags of input Ethernet frame.In other words,VLAN Unaware mode can pass all VLAN tags from one customer domain to another no matter it is VLAN tagged or VLAN untagged.

3.4.2 VLAN Configuration

VLAN Configuration is used to define VLAN groups and the VLAN information will be stored in the VLAN membership table. The Delta switch supports up to 256 VLANs. VLAN 1 is the default VLAN, and all interfaces are untagged members by the default setting.

Note:
The interfaces that you make members of link aggregation groups (that is, physical interfaces that function as trunk members) lose their membership of the default VLAN.



VLAN Configuration

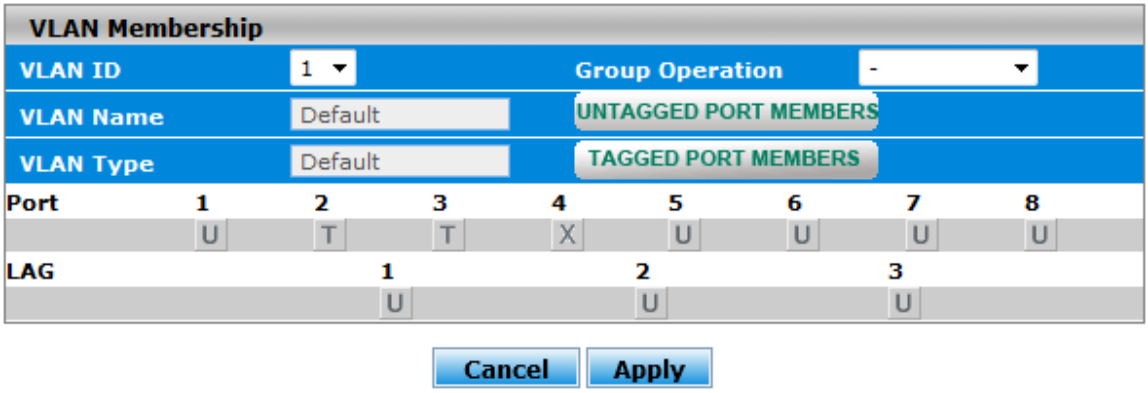
Description	Factory default
VLAN ID	
Enter the identifier for the new VLAN. The range can be set in the range of 1 to 4094.	None
VLAN Name	
Enter a name for the VLAN. The name can be up to 32 alphanumeric characters long, including blanks.	None
VLAN Type	
When you create VLAN, the VLAN type always displays Static.	Static

3.4.3 VLAN Membership

You cannot change the VLAN Type of VLAN 1, because VLAN 1 is the default VLAN and the type is always Default. When you create a VLAN on this page, its type will always be Static. An interface or LAG can be a tagged (T) or untagged (U) VLAN member.

Note:
If you need to access the switch via the port, we suggest that you make sure that the port you use is the untagged port of VLAN 1 (the default VLAN).

VLAN Membership



VLAN Square Status

Status	Description
blank square (Auto)	If the interface or LAG is not a member of VLAN, the square must keep blank. The port currently is not the static member of the VLAN, but it can be added dynamically by other protocols, for example by GVRP.
T (Tagged)	If the square status of the interface or LAG is T, frames transmitted from the interface or LAG are tagged with the port VLAN ID. Click **Tagged Port Members** to view the interfaces and LAGs which are tagged.
U (Untagged)	If the square status of the interface or LAG is U, frames transmitted from this interface or LAG is untagged. Each interface or LAG can be an untagged member of any VLAN. That is, an interface or LAG can be an untagged member of multiple VLANs. All interfaces and LAGs are untagged members of VLAN 1 by the default setting. Click **Untagged Port Members** to view the interfaces and LAGs which are untagged.
X (Forbidden)	This port can not be the member of this VLAN permanently. (It also can not be added dynamically by other protocols.)

Add and configure the interface or LAG:

- Click once to add the interface or LAG as a tagged member to the VLAN.
- Click twice to add the interface or LAG as an untagged member to the VLAN.
- Click three times to remove the interface or LAG from the VLAN.

Add and configure all interfaces:

- **Untag All:** Adds all interfaces or LAGs as untagged members to the VLAN.
- **Tag All:** Adds all interfaces or LAGs as tagged members to the VLAN.
- **Remove All:** Removes all interfaces or LAGs from the VLAN.

3.4.4 VLAN Status

You can click **Refresh** button to update the information.

VLAN Status

VLAN Status

VLAN ID	VLAN Name	VLAN Type	Member Ports	Untagged Ports
1	Default	Default	0/1-8,po1,po2,po3	0/1-8,po1,po2,po3
2	Test	Static	0/1-2,po1	0/1-2,po1
3	Test2	Static	0/4-6,po2	0/4-6,po2

Refresh

VLAN Status

Item	Description
VLAN ID	The identifier of VLAN.
VLAN Name	The name of VLAN.
VLAN Type	The type of VLAN (Default or Static).
Member Ports	The interfaces that are members of VLAN.
Untagged Ports	The interfaces that are untagged members of VLAN.

3.4.5 Port PVID Configuration

VID (VLAN ID) is the tag of VLAN. It defines the interface which can **receive** the packets of the VLAN; PVID (Port VLAN ID) defines the untagged port which can **forward** the VLAN's packets.
For example: If port 1 belongs to VLAN 1, 2, 3, and its PVID is 1, port 1 can receive the packets from VLAN 1, 2, 3, but it can only forward the packets to VLAN 1.
The default port VLAN ID (PVID) is assigned to 1 on all interfaces, because they are assigned to default VLAN 1. If there is no other values specified, the default VLAN PVID is used for untagged or priority-tagged frames.

Note:
If you want to change the default PVID of an interface, create VLAN and then includes the interface as a member.

Port PVID Configuration

Port PVID Configuration

	Port	PVID	Acceptable Frame Types	Ingress Filtering	Port Priority
☐			-	-	
☐	0/1	1	All	Disabled	0
☐	0/2	1	All	Disabled	0
☐	0/3	1	All	Disabled	0
☐	0/4	1	All	Disabled	0
☐	0/5	1	All	Disabled	0
☐	0/6	1	All	Disabled	0
☐	0/7	1	All	Disabled	0
☐	0/8	1	All	Disabled	0
☐	po1	1	All	Disabled	0
☐	po2	1	All	Disabled	0
☐	po3	1	All	Disabled	0

Apply

Port PVID Configuration

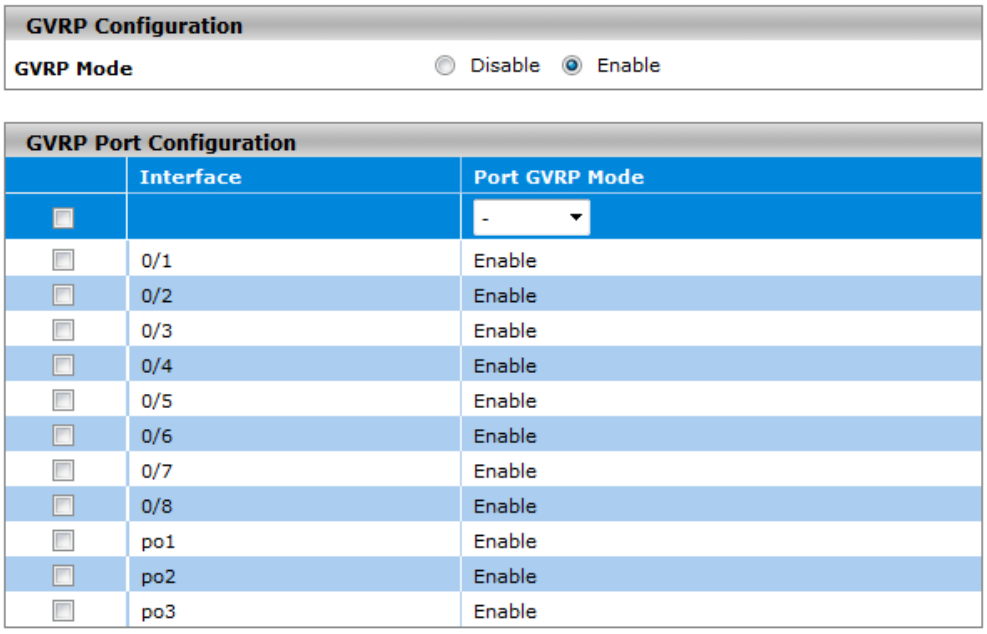
Description	Factory default
Port	
This field displays the interface number or port channel number.	*interface number*
PVID	
This field displays the current PVID.	1
Acceptable Frame Types	
Specify the types of frames that can be received on the interface: • **All:** Accept tagged, untagged, and priority-tagged frames. Untagged or priority-tagged frames are assigned the VLAN ID for this interface. VLAN-tagged frames are forwarded. • **Tagged:** Only forward VLAN-tagged frames, drop all other frames. • **UnTagged and Priority Tagged:** Forward untagged and priority-tagged frames, drop VLAN-tagged frames.	All
Ingress Filtering	
Specify whether the ingress filtering is applied: • **Enabled:** The ingress filtering is enabled for the interface. If the interface is not a member of VLAN with which the frame is associated, an incoming frame is dropped. In a tagged frame, VLAN is identified by the VLAN ID in the tag. In an untagged frame, VLAN is PVID. • **Disabled:** The ingress filtering is disabled for the interface. All frames are forwarded.	Disabled
Port Priority	
Enter the default priority that is assigned to incoming untagged packets. Enter a number between 0 and 7. And 7 is the highest priority.	0

3.4.6 GVRP Configuration

The GARP (Generic Attribute Registration Protocol) VLAN Registration Protocol defines a GARP application that provides the 802.1Q-compliant VLAN pruning and dynamic VLAN creation on 802.1Q trunk ports. With GVRP, the switch can exchange VLAN configuration information with other GVRP switches, prune unnecessary broadcast and unknown unicast traffic, and dynamically create and manage VLANs on switches connected through 802.1Q trunk ports.

Note:
If you need to configure Port Configuration, we suggest that you make sure that GVRP Configuration is enabled, or it can not work on Port Configuration.

GVRP Configuration



GVRP Configuration

Description	Factory default
GVRP Mode	
Specify whether the GVRP mode is enabled. • **Disable:** The GVRP mode is disabled. • **Enable:** The GVRP mode is enabled.	Enable

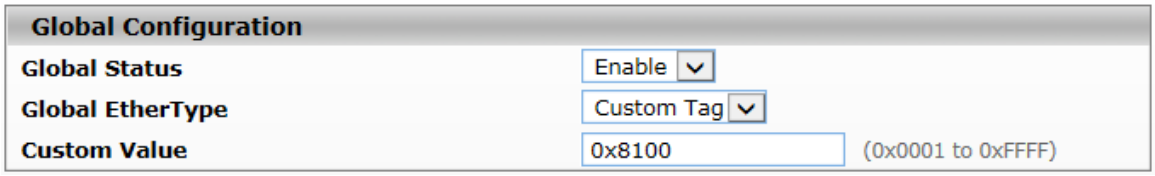
GVRP Port Configuration

Description	Factory default
Interface	
This field displays the interface number.	*interface number*
Port GVRP Mode	
Specify whether the GVRP mode is enabled on the interface.	Enable

3.4.7 Double VLAN Configuration

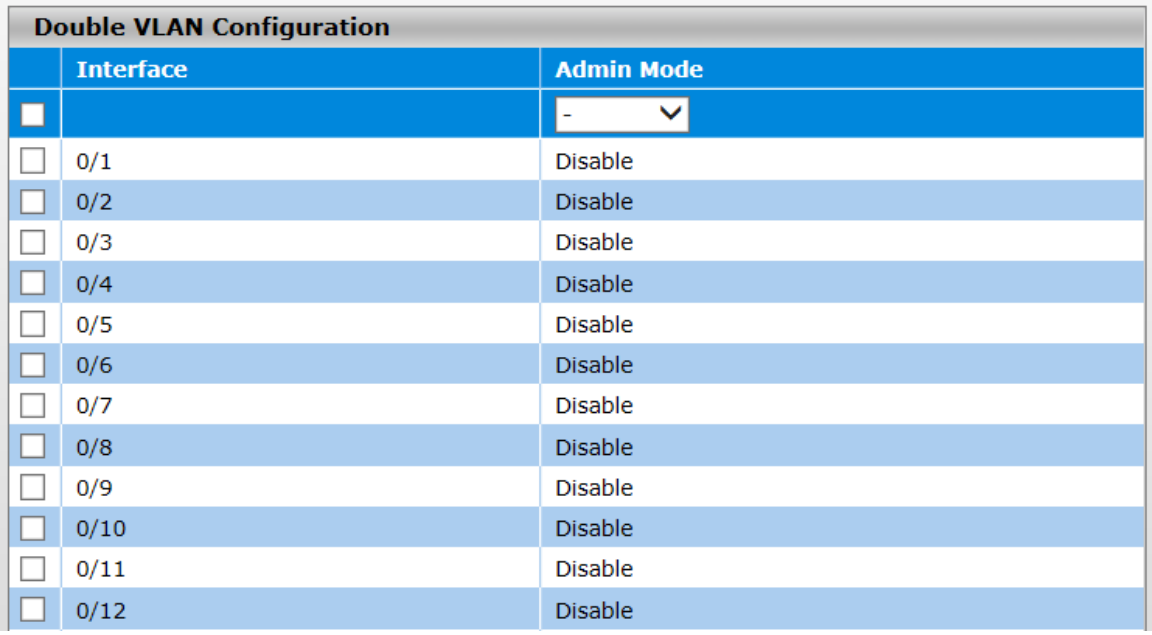
Double VLAN (Q-in-Q VLAN) is a way to pass VLAN traffic from one customer domain to another through a metro core.The function allows admin user to add an additional tag in one Ethernet frame.

Double VLAN Configuration



Global Configuration

Description	Factory default
Global Status	
Specify whether the status in global configuration is activated or not.	Disable
Global EtherType	
Specify which EtherType can be globally configured. • **802.1Q Tag**: Set EtherType as 802.1Q mode. • **vMAN Tag**: Set EtherType as vMAN mode. • **Custom Tag**: Set EtherType as Custom mdoe.You can define the TPID of the VLAN, and the range is 0x0001 to 0xFFFF.	802.1Q
Custom Value	
Specify the TPID when the Global EtherType is Custom Tag.The TPID will be effective on the provider port.The range is from 0x0001 to 0xFFFF	0x8100

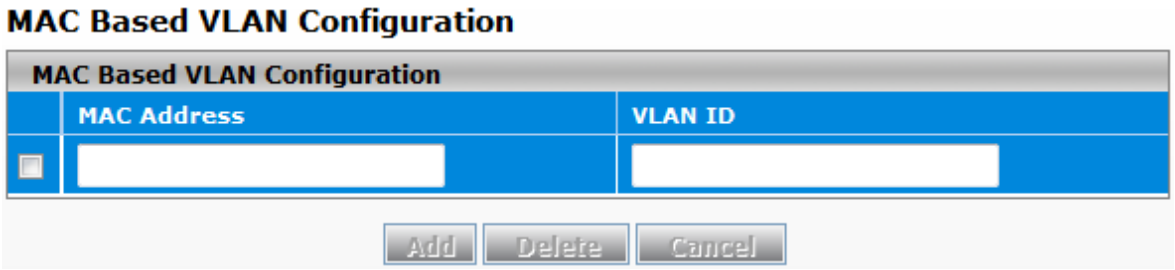


Double VLAN Configuration

Description	Factory default
Interface	
The interface number.	*interface number*
Admin Mode	
Enable/Disable the feature on the port. • **Enable**: Enable Double VLAN (Q-in-Q) function.The port will become provider port • **Disable**: Disable the Double VLAN (Q-in-Q) function, and the port becomes a customer port.	Disable

3.4.8 MAC Based VLAN

A MAC based VLAN feature allows incoming untagged and priority packets to be assigned to a VLAN, and thus classify the traffic based on the source MAC address. It can support 64 MAC based VLAN entries, and can be configured across all ports of the device.



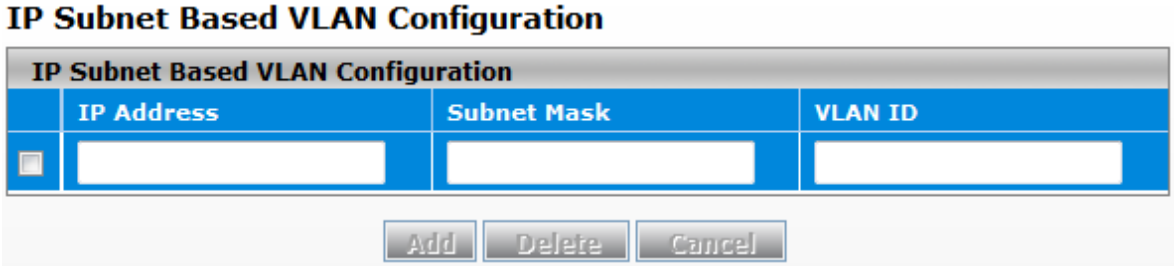
3

MAC Based VLAN

Description	Factory default
MAC Address	
Specify a unicast mac address.	None
VLAN ID	
Specify a vlan ID, and the range is 1 to 4094.	None

3.4.9 IP Subnet Based VLAN

An IP Subnet Based VLAN feature allows incoming untagged and priority packets to be assigned to a VLAN, and thus classify the traffic based on the IP subnet of the packet. It can support 16 IP Subnet Based VLAN entries, and can be configured across all ports of the device.



IP Subnet Based VLAN

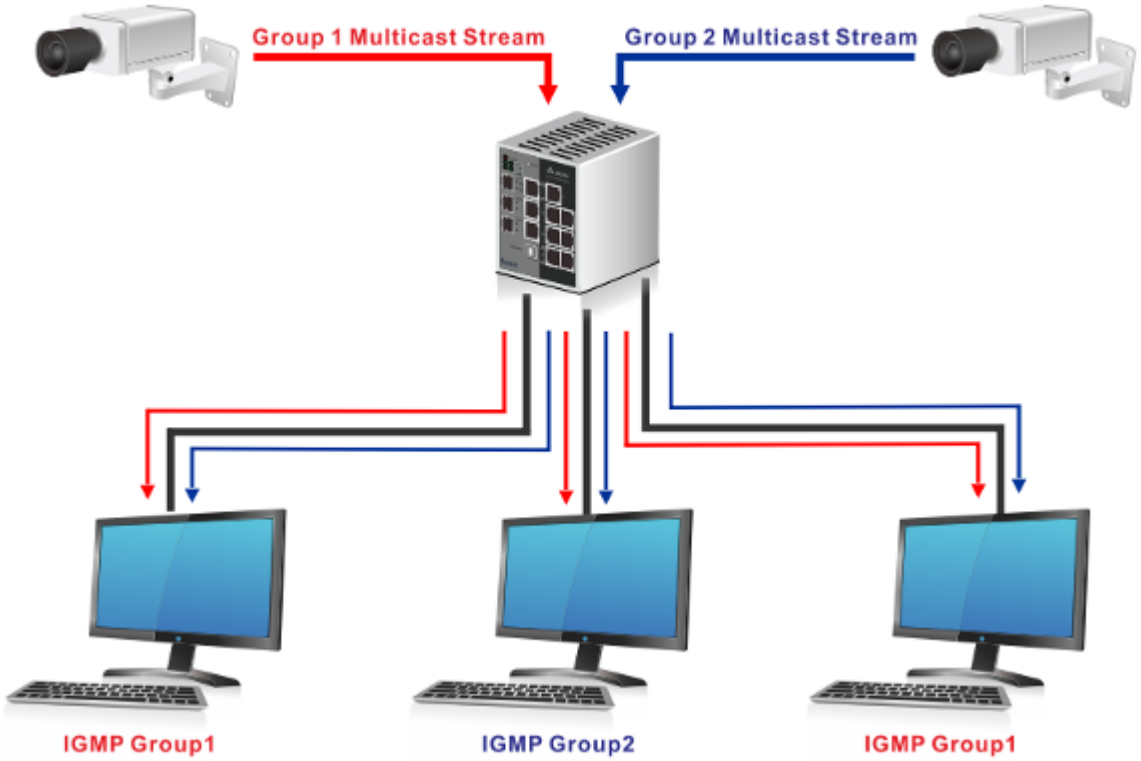
Description	Factory default
IP Address	
Specify an IP network address for the subnet.	None
Subnet Mask	
Specify a subnet mask for the IP subnet.	None
VLAN ID	
Specify a vlan ID and the range is 1 to 4094.	None

3.5 Multicast Filtering

Multicast IP traffic is traffic that is assigned to a host group. Host groups are identified by class D IP addresses, which range from 224.0.0.0 to 239.255.255.255. A multicast IP packet is only sent by one host to multiple hosts. Only those hosts that belong to a specific multicast group will receive the multicast. The Internet Group Management Protocol (IGMP) snooping enables the switch to forward multicast traffic intelligently to only the interface that requests the multicast traffic. So the network resource is not wasted too much.
If there is a network without the multicast filtering, and a host needs to send data to many hosts, then it needs to produce several copies in the network. It wastes too much network bandwidth. If there is a network with the multicast filtering, then it reduces the load of resources (ex. a server) and makes the network bandwidth efficient. The figures below show the difference between the network without Multicast Filtering and the network with Multicast Filtering.

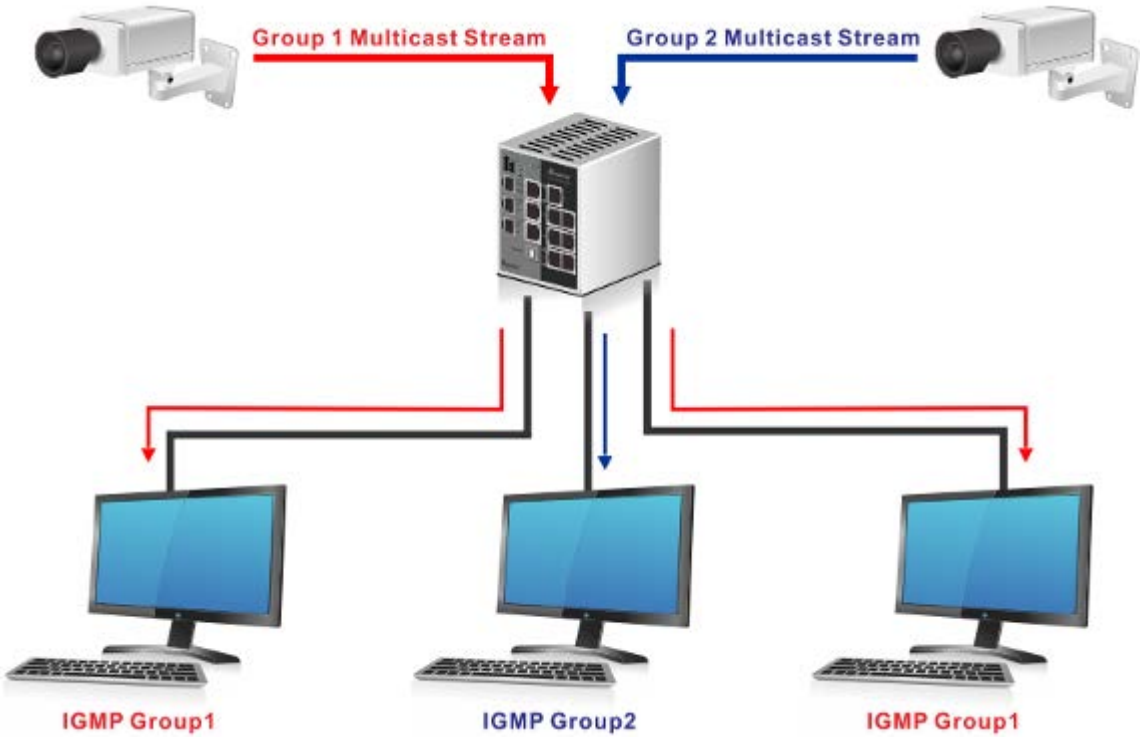
IMPORTANT:
Make sure that you save the configuration in the Save Configuration page after you have applied the configuration changes. (Save Config→Save Configuration) If you do not save the configuration, then the configuration will be cleared after the switch is rebooted.

Network without Multicast Filtering:



(All hosts receive the multicast traffic.)

Network with Multicast Filtering:



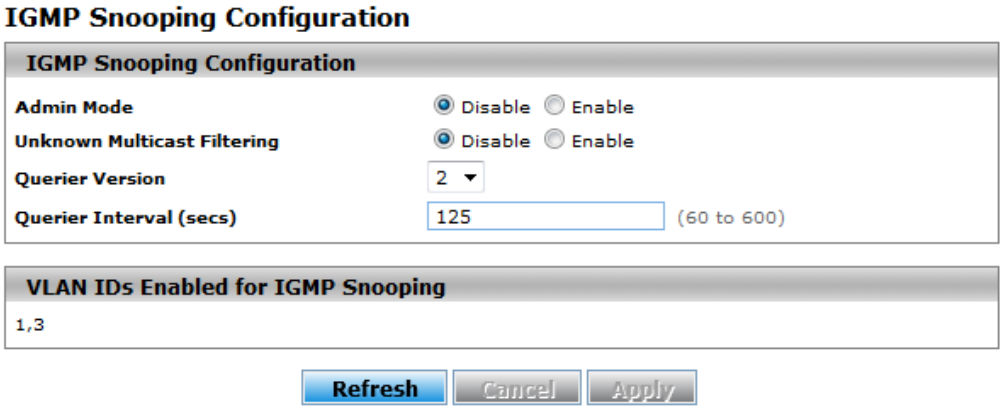
(Only the host which belongs to the group can receive the traffic.)

IGMP Snooping manages multicast traffic by making use of switches, routers, and hosts that support IGMP. Enabling IGMP Snooping allows the ports to detect the IGMP queries, report packets, and manage multicast traffic through the switch. IGMP has three fundamental types of messages, as shown below:

Message	Description
Query	A message is sent from the querier (an IGMP router or a switch) which asks for a response from each host that belongs to the multicast group.
Report	A message is sent by a host to the querier to indicate that the host wants to be or is a member of a given group indicated in the report message.
Leave Group	A message is sent by a host to the querier to indicate that the host has quit as a member of a specific multicast group.

3.5.1 IGMP Snooping Configuration

On this page, you can enable or disable IGMP Snooping. And it displays the VLAN which enables the IGMP Snooping function.



IGMP Snooping Configuration

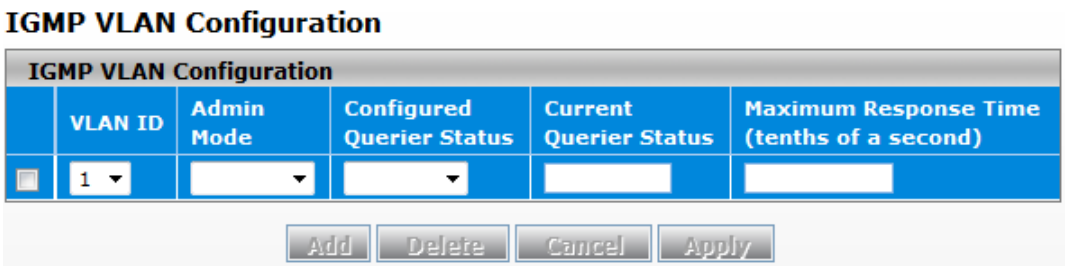
Description	Factory default
Admin Mode	
Specify the status of IGMP Snooping: • **Disable:** The IGMP Snooping is disabled. The IGMP setting still can be configured, but the settings do not take effect after you have applied them. • **Enable:** The IGMP Snooping is enabled. The switch snoops all the IGMP packets it receives to determine which segments should receive the packets directed to the group address.	Disable
Unknown Multicast Filtering	
Specify the status of the unknown multicast filtering: • **Disable:** Unknown multicast traffic is not filtered and is forwarded. • **Enable:** Unknown multicast traffic is filtered and dropped.	Disable
Querier Version	
Specify the IGMP protocol version used in periodic IGMP queries. • **IGMP v1:** Support the member query and the report function. • **IGMP v2:** Support the general query (the same as IGMPv1), the group-specific query, the maximum response time, and the leave group message function.	2
Querier Interval (secs)	
The Querier interval is the amount of time in seconds between IGMP General Query messages sent by the router (if the router is the querier on this subnet). Enter a period between 60 and 600 seconds.	125

VLAN IDs Enabled for IGMP Snooping

This field displays the VLANs that are enabled for IGMP Snooping. For information about how to configure a VLAN for IGMP Snooping, see the following section.

3.5.2 IGMP VLAN Configuration

This page can configure the IGMP Snooping and the querier status for each VLAN.



IGMP VLAN Configuration

Description	Factory default
VLAN ID	
Select a VLAN ID for which you want to create an IGMP snooping configuration.	None
Admin Mode	
Specify the IGMP querying status for VLAN: • **Disable:** The query can not be forwarded to all multicast groups in VLAN. • **Enable:** The query can be forwarded to all multicast groups in VLAN.	Enable
Configured Querier Status	
Specify the configured querier status: • **Disable:** The IGMP querying is disabled for VLAN. You can still configure VLAN for the snooping, but the settings do not take effect after you have applied them. • **Enable:** The IGMP querying is enabled for the VLAN.	Disable
Current Querier Status	
The field displays the current querier status in the VLAN.	Disable

Description	Factory default
Maximum Response Time (tenths of a second)	
Enter the maximum response time for the IGMP query for VLAN. This field specifies the maximum period that the switch waits for a response from a host if the switch is the querier for VLAN. Enter a period in tenths of seconds in the range of 0 to 255. Enter 0 to disable the maximum response time.	100

3.5.3 IGMP Snooping Multicast Forwarding Table

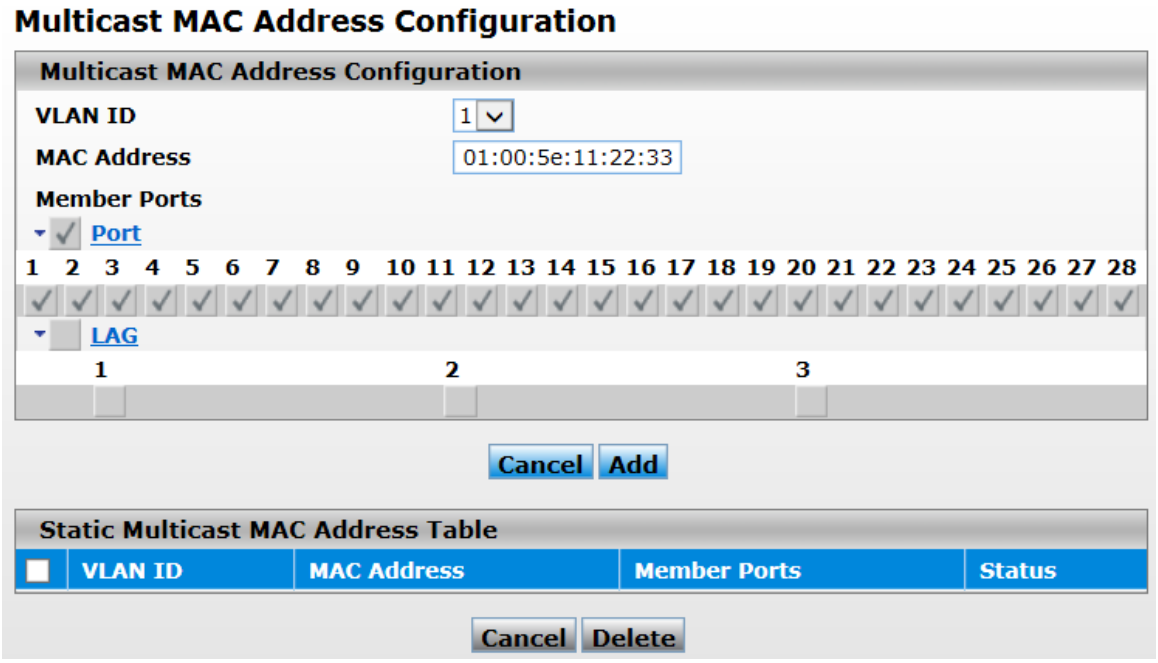
The multicast forwarding table displays how packets that arrive with a multicast destination MAC address are forwarded.
The destination MAC address is combined with the VLAN ID when a packet is sent into the switch. And the multicast searching status and the multicast forwarding status are displayed in the multicast forwarding table. If there is no match found, the packet is flooded to all interfaces in VLAN or discarded. It depends on the configuration. If there is a match found, the packet is forwarded to the interfaces which are the members of the multicast group.

IGMP Snooping Multicast Forwarding Table

Item	Description
VLAN ID	The VLAN ID for the IGMP snooping configuration.
MAC address	The multicast MAC address from which multicast traffic is requested and sent.
Forwarding Interfaces	The interfaces that request the multicast traffic and to which incoming multicast traffic is forwarded.

3.5.4 Multicast MAC Address Configuration

If required, the Delta switch also supports adding multicast groups manually. You can add a multicast MAC address with a VLAN ID on this page. Before you add a multicast MAC address with a VLAN ID to switch, you have to make sure that the member ports have been assigned to the VLAN ID.



Multicast MAC Address Configuration

Description	Factory default
VLAN ID	
Specify the VLAN ID.	None
MAC Address	
Specify the multicast MAC address.	None
Member Ports	
Select the member port or LAGs for this multicast group.	None

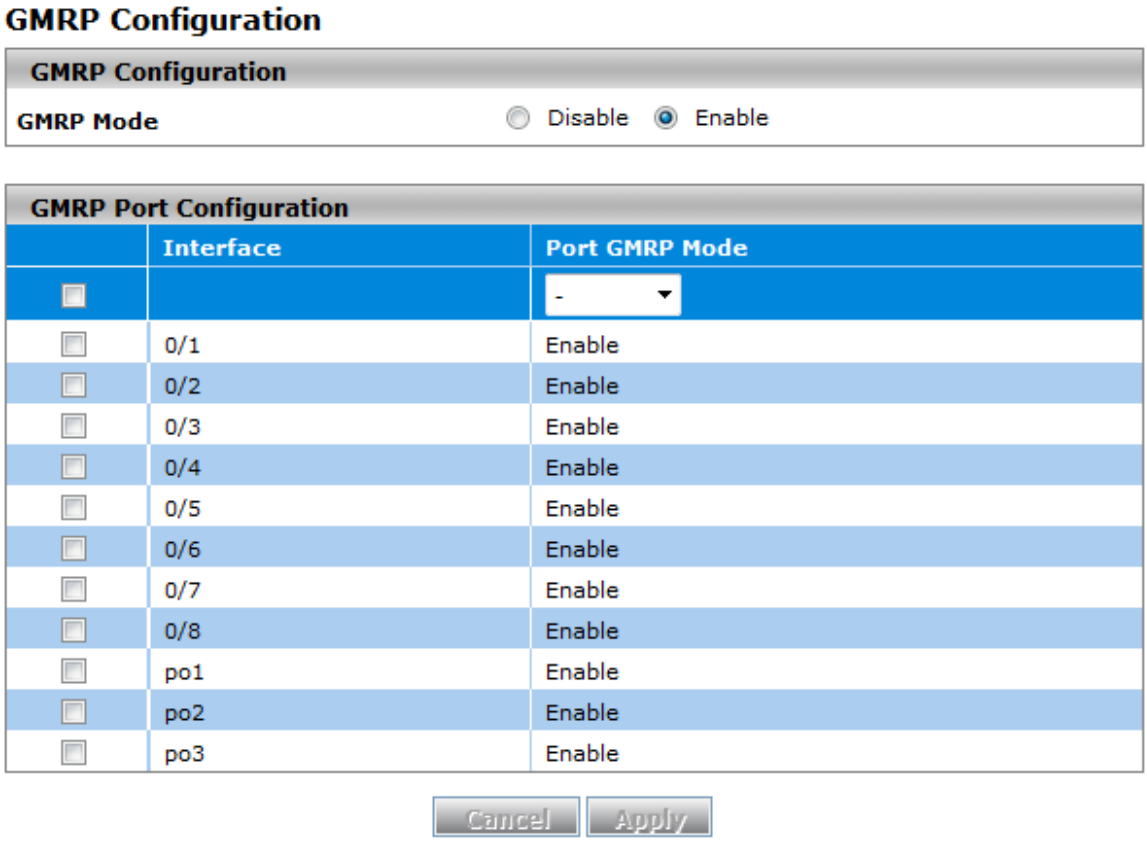
Static Multicast MAC Address Table

Item	Description
VLAN ID	The field displays the identifier of VLAN.
MAC Address	The field displays the multicast MAC address.
Member Ports	The field displays the multicast member ports.
Status	The field displays the status of the multicast MAC address.

3.5.5 GMRP Configuration

The GARP (Generic Attribute Registration Protocol) Multicast Registration Protocol helps control the flooding of multicast packets. The GMRP-enabled switches dynamically register and de-register group membership information with the MAC networking devices attached to the same segment.

Note:
If you need to configure the GMRP Port Configuration, we suggest that you make sure that GMRP Configuration is enabled, or the function can not be actived on Port Configuration.



GMRP Configuration

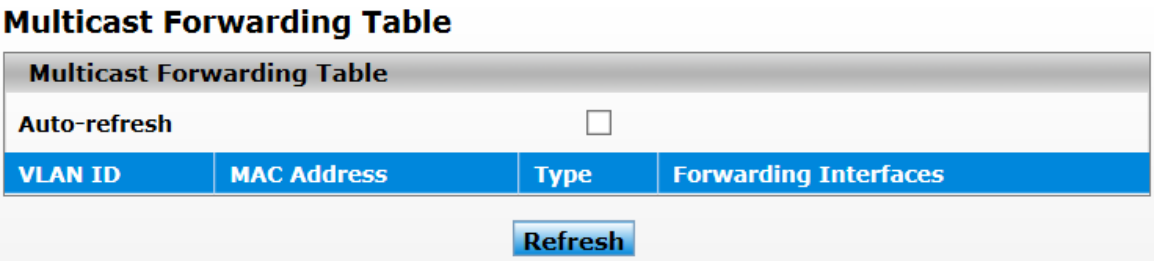
Description	Factory default
Specify whether the GMRP mode is enabled. • **Disable:** The GMRP mode is disabled. • **Enable:** The GMRP mode is enabled.	Enable

GMRP Port Configuration

Description	Factory default
Interface	
This field displays the interface number.	*interface number*
Port GMRP Mode	
Specify whether the GMRP mode is enabled on the interface. • **Disable:** The GMRP mode on the interface is disabled. • **Enable:** The GMRP mode on the interface is enabled.	Enable

3.5.6 Multicast Forwarding Table

The multicast MAC address can be added manually, and it also can be added by the GMRP function. This multicast forwarding table can display the type of the MAC address.



Multicast Forwarding Table

Item	Description
Auto-refresh	Checkmark this box, it will refresh the multicast forwarding table automatically.
VLAN ID	The field displays the identifier of VLAN.
MAC Address	The field displays the multicast MAC address.
Type	The field displays that the learning type is static or dynamic.
Forwarding Interfaces	The field displays the forwarding interface number.

3.6 Traffic Prioritization

The traffic prioritization allows you to make sure that the time-sensitive and system-critical data can be transferred with the minimal delay. It uses four queues that are present in UI from the high priority to the low priority.

The Delta switch supports the DSCP trust mode, the 802.1p trust mode, the queue scheduling (Support Weighted Round Robin and Strict-Priority) and 4 level priority queues. The traffic prioritization depends on 2 methods:

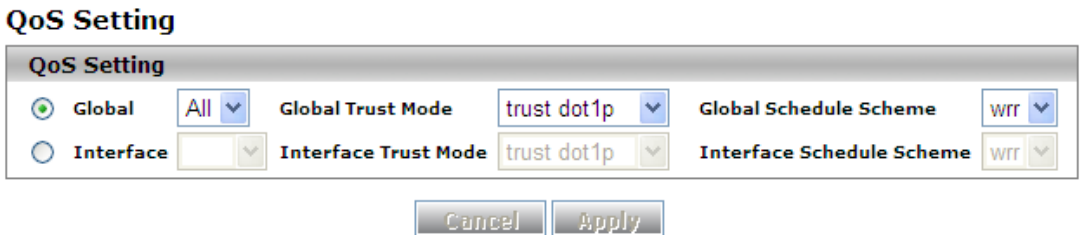
- **IEEE 802.1P:** a layer 2 marking scheme.
- **Differentiated Services (DiffServ):** a layer 3 marking scheme.

> **IMPORTANT:**
> **Make sure that you save the configuration in the Save Configuration page after you have applied the configuration changes. (Save Config→Save Configuration) If you do not save the configuration, then the configuration will be cleared after the switch is rebooted.**

3.6.1 QoS

Quality of Service (QoS) provides a traffic prioritization for you to alleviate the congestion problem, and ensure that high-priority traffic is delivered first. If the bandwidth of the network is limited, you can use QoS to schedule the priority of a different service packet flow.

3.6.1.1 QoS Setting



QoS Setting

- **Global:** Specify the trust mode settings for all interfaces and aggregation groups. Then, make a selection from the Global Trust Mode drop-down list.

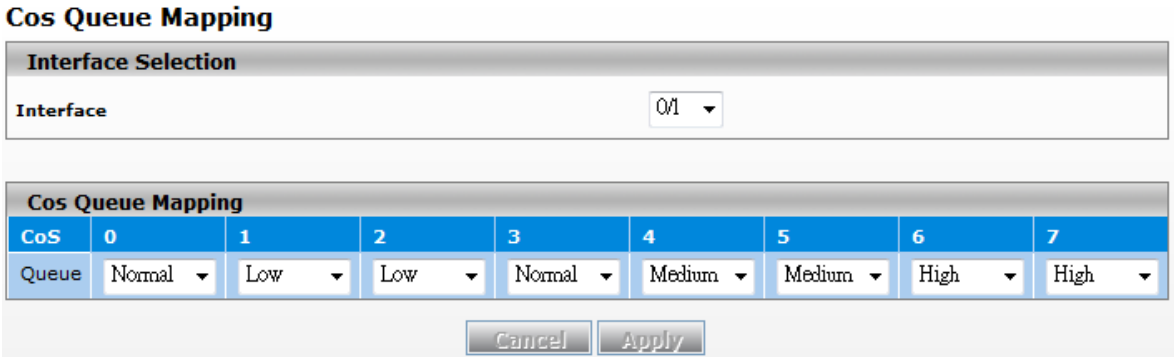
Description	Factory default
Global Trust Mode	
Make a selection from the Global Trust Mode drop-down list that affects all interfaces or aggregation groups: • **trust dot1p:** All interfaces or aggregation groups are configured for the 802.1p marking to classify traffic. • **trust ip-dscp:** All interfaces and aggregation groups are configured for the IP DSCP packet matching to classify traffic.	trust dot1p
Global Schedule Scheme	
Make a selection from the Global Schedule Scheme drop-down list that affects all interfaces: • **sp:** SP (Strict-Priority) classifies the queue from the high priority to the low priority. If the higher priority of the queue is empty, the lower priority data of the queue starts to be sent. • **wrr:** WRR (Weighted Round Robin) schedules the queue by turns, so each queue has a service time. Each queue can be allocated a weight value or percentage for the bandwidth.	Wrr

- **Interface:** Specify the trust mode settings for an individual interface and aggregation groups. Select an interface or aggregation groups from the Interface drop-down list, and then make a selection from the Interface Trust Mode drop-down list.

Description	Factory default
Interface Trust Mode	
Make a selection from the Interface Trust Mode drop-down list that affects an individual interfaces or aggregation groups: • **trust dot1p:** The interface or aggregation groups are configured for the 802.1p marking to classify traffic. • **trust ip-dscp:** The interface and aggregation groups are configured for the IP DSCP packet matching to classify traffic.	trust dot1p
Interface Schedule Scheme	
Make a selection from the Global Schedule Scheme drop-down list that affects all interfaces: • **sp:** SP (Strict-Priority) classifies the queue from the high priority to the low priority. If the higher priority of the queue is empty, the lower priority data of the queue starts to be sent. • **wrr:** WRR (Weighted Round Robin) schedules the queue by turns, so each queue has a service time. Each queue can be allocated a weight value or percentage for the bandwidth.	Wrr

3.6.1.2 CoS Queue Mapping

This page allows you to configure the CoS value for the physical queue mapping table. The field specifies a priority value between 0 and 7, and the Delta switch provides 4 physical queues which can be used by Quality of Service (QoS) for differentiate network traffic.



Interface Selection

Specify one of the following selections:

- **Select from 0/1 through 0/9:** Specify an individual interface.
- **Select from po1 through po3:** Specify a link aggregation group.
- **Select All:** Specify all interfaces and link aggregation groups.

CoS Queue Mapping

Select a queue to which you want to map the priority. The traffic class is the selected queue (Low, Normal, Medium, or High) for an interface.

The default queues of the CoS are mapped in the way described below.

CoS	0	1	2	3	4	5	6	7
Queue	Normal	Low	Low	Normal	Medium	Medium	High	High

3.6.1.3 DSCP Queue Mapping

This page allows you to configure the DSCP value to the physical queue mapping table. The field specifies a priority value between 0 and 63, and the Delta switch provides 4 physical queues which can be used by Quality of Service (QoS) for differentiate network traffic. Users can configure the mapping table to follow the upper layer 3 switch or the routers' DSCP setting.

DSCP Queue Mapping

Interface Selection

Interface: 0/1

DSCP Queue Mapping

IP DSCP	Queue	IP DSCP	Queue	IP DSCP	Queue	IP DSCP	Queue
0	Normal	16	Low	32	Medium	48	High
1	Normal	17	Low	33	Medium	49	High
2	Normal	18	Low	34	Medium	50	High
3	Normal	19	Low	35	Medium	51	High
4	Normal	20	Low	36	Medium	52	High
5	Normal	21	Low	37	Medium	53	High
6	Normal	22	Low	38	Medium	54	High
7	Normal	23	Low	39	Medium	55	High
8	Low	24	Normal	40	Medium	56	High
9	Low	25	Normal	41	Medium	57	High
10	Low	26	Normal	42	Medium	58	High
11	Low	27	Normal	43	Medium	59	High
12	Low	28	Normal	44	Medium	60	High
13	Low	29	Normal	45	Medium	61	High
14	Low	30	Normal	46	Medium	62	High
15	Low	31	Normal	47	Medium	63	High

Cancel Apply

Interface Selection

Specify one of the following selections:

- **Select from 0/1 through 0/9:** Specify an individual interface.
- **Select from po1 through po3:** Specify a link aggregation group.
- **Select All:** Specify all interfaces and link aggregation groups.

DSCP Queue Mapping

Select a queue to which you want to map the priority. The traffic class is the selected queue (Low, Normal, Medium, or High).

The previous figure shows the default queues for each IP DSCP value:

- IP DSCP values 0 through 7 and 24 through 31 at queue **Normal**
- IP DSCP values 8 through 23 at queue **Low**
- IP DSCP values 32 through 47 at queue **Medium**
- IP DSCP values 48 through 63 at queue **High**

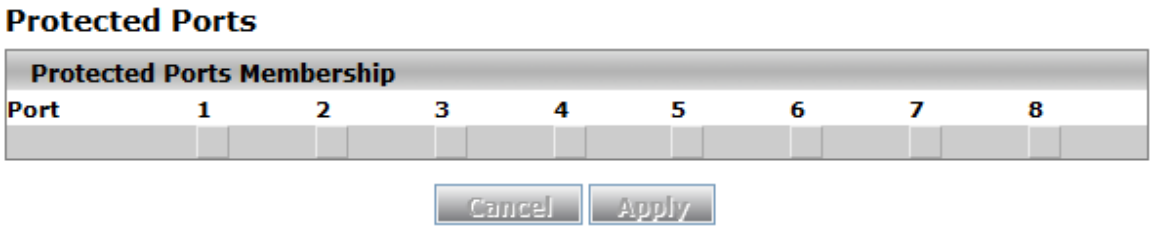
3.7 Traffic Control

You can see the MAC addresses which the Delta switch had learned, and configure a port which is to be protected or unprotected in this group.

> **IMPORTANT:**
> **Make sure that you save the configuration in the Save Configuration page after you have applied the configuration changes. (Save Config→Save Configuration) If you do not save the configuration, then the configuration will be cleared after the switch is rebooted.**

3.7.1 Port Protected

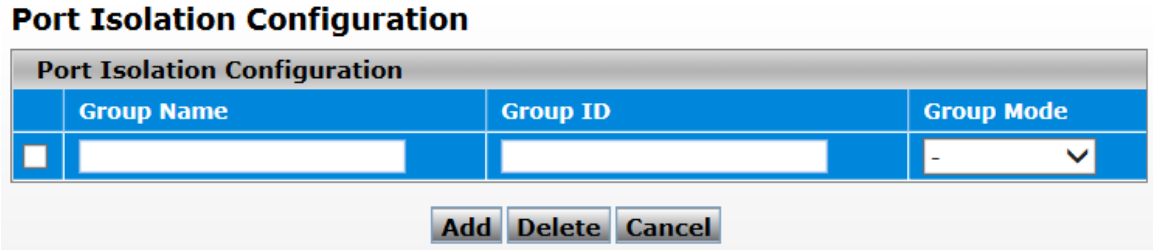
A protected port does not forward traffic to any other protected ports on the switch, but can forward traffic to unprotected ports on the switch.



- **Enable:** Select one interface or more interfaces by clicking the square.
- **Disable:** Click second time to clear the interface.

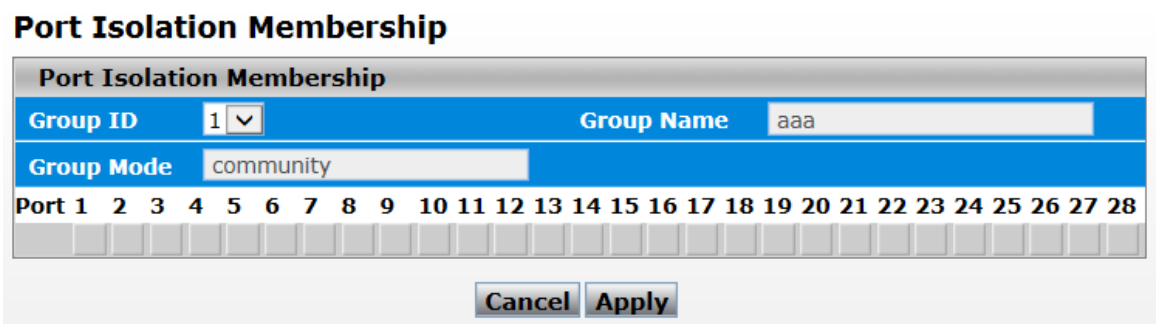
3.7.2 Port Isolation Configuration

This function supports two mode group which are isolated or community.When enabled, the member port in the group cannot forward its engress traffic to any other members in the same group.The ingress traffic from a port in isolated group can be forwarded to anyone in the same VLAN that are not in an isolated group.



Port Isolation Configuration

Description	Factory default
Group Name	
Specify the Port Isolation group name, and the name string can be up to 24 bytes of non-blank characters.	None
Group ID	
Specify the Port Isolation group ID, and the range of group is 1 to 24.	None
Group Mode	
Specify the Port Isolaion group mode. • **Isolated:** The members in the group cannot forward its engress traffic to any other member ports in the same group. • **Community:** Each member port can forward traffic to other mebers in the same group, but not to member ports in other group.	None



Port Isolation Membership

Description	Factory default
Group ID	
Display the Group IDs which added in the Port isolation configuration.	Fixed
Group Name	
Display the Group Name and it's related to the Group ID.	Fixed
Group Mode	
Display the Group mode and it's related to the Group ID	Fixed
Port Number	
Select the member port which you want to add in the specific group.	None

3.8 Port Bandwidth

A Delta switch allows you to configure bandwidth for each port to avoid a network traffic storm.

> **IMPORTANT:**
> **Make sure that you save the configuration in the Save Configuration page after you have applied the configuration changes. (Save Config→Save Configuration) If you do not save the configuration, then the configuration will be cleared after the switch is rebooted.**

3.8.1 Storm Control

A traffic storm occurs when incoming packets flood the LAN, which causes the decreasing of the network performance. The storm control can prevent flooding packets from affecting the network performance. The Delta switch allows you to configure both storm control for each interface and rate limiting of each interface for incoming and outgoing traffic.

3.8.1.1 Storm Control Setting

A broadcast storm occurs when a large number of broadcast messages are transmitted from a single interface across a network at the same time. Forwarding these messages can overload too much network resources or cause the network timeout.
The Delta switch can measure the incoming packet rate of the broadcast, multicast, and unknown unicast packets for each interface and discards packets when the rate exceeds the defined value. You can enable storm control for each interface by a different packet type and define the threshold of the traffic flow.

Storm Control Setting

Port Configuration

	Port	Broadcast Storm			Multicast Storm		
		Recovery Mode	Recovery Level Type	Recovery Level	Recovery Mode	Recovery Level Type	Recovery Level
	0/1	Enable	Mbps	5	Disable	Mbps	5
	0/2	Enable	Mbps	5	Disable	Mbps	5
	0/3	Enable	Mbps	5	Disable	Mbps	5
	0/4	Enable	Mbps	5	Disable	Mbps	5
	0/5	Enable	Mbps	5	Disable	Mbps	5
	0/6	Enable	Mbps	5	Disable	Mbps	5
	0/7	Enable	Mbps	5	Disable	Mbps	5
	0/8	Enable	Mbps	5	Disable	Mbps	5

Apply Cancel

Unicast Storm		
Recovery Mode	Recovery Level Type	Recovery Level
Disable	Mbps	5
Disable	Mbps	5
Disable	Mbps	5
Disable	Mbps	5
Disable	Mbps	5
Disable	Mbps	5
Disable	Mbps	5
Disable	Mbps	5

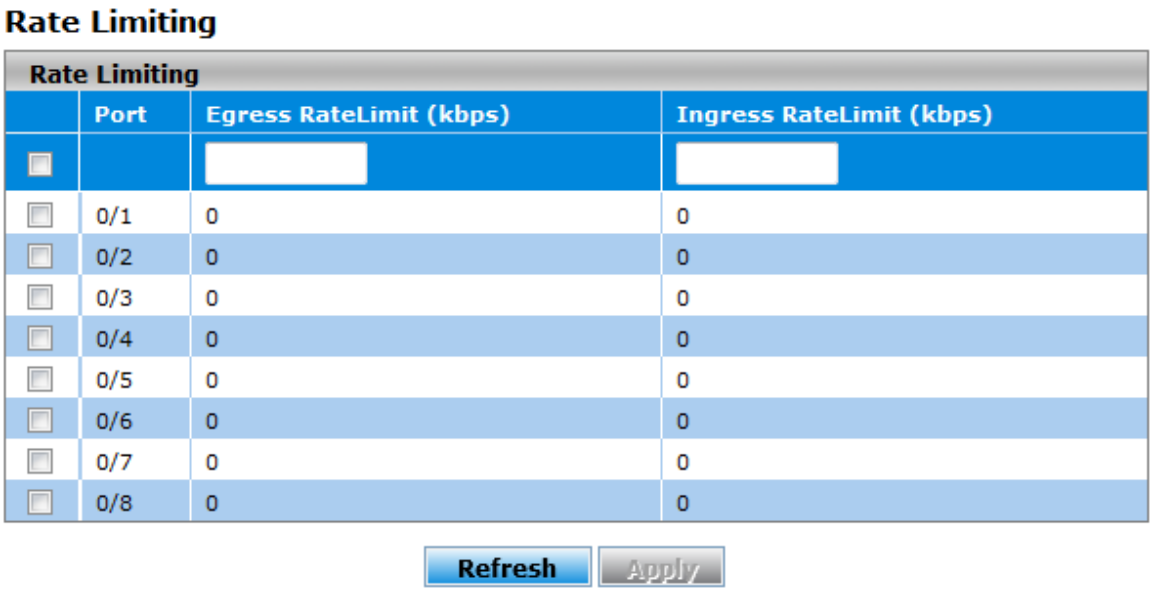
Storm Control Setting

Description	Factory default
Port	
The interface number.	*interface number*
Recovery Mode	
Specify the recovery mode by making a selection from the drop-down list: • **Disable:** The recovery mode is disabled. No traffic is discarded. • **Enable:** When traffic on the port exceeds the threshold that is configured in the Recovery Level field, the switch discards the traffic.	Enable
Recovery Level Type	
Specify the link speed recovery level type.	Mbps
Recovery Level	
Specify the threshold at which storm control is activated. If the value is 5, it indicates 5 Mbps. By default, when the traffic exceeds 5 Mbps of the link speed, the switch discards the traffic.	5

Note:
For each interface and each of the three types of traffic, you can set the recovery mode and recovery level. The drop-down lists and the fields functions the same for each of the three types of traffic.

3.8.1.2 Rate Limiting

You can configure the traffic rate for each interface in both directions on this page.

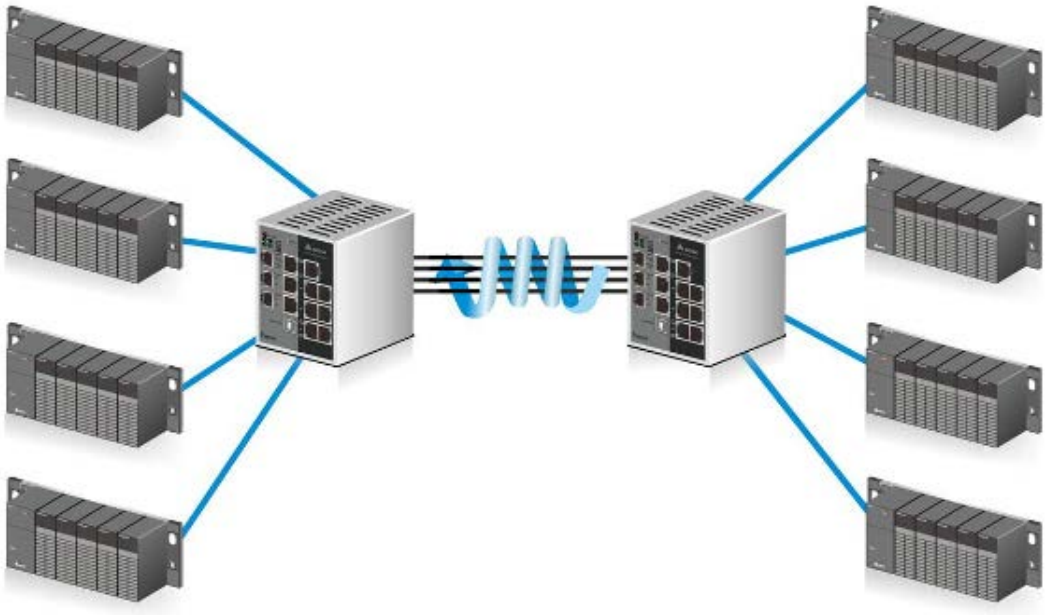


Rate Limiting

Description	Factory default
Port	
The interface number	*interface number*
Egress RateLimit (kbps)	
Enter the egress port rate limit as a value in the range of 1 to 1,000,000 kbits per second (kbits/s). The value that you enter is actually applied in increments of 64 kbits/s. If the value is 0, it effectively disables the rate limit.	0
Ingress RateLimit (kbps)	
Enter the ingress port rate limit as a value in the range of 1 to 1,000,000 kbits per second (kbits/s). The value that you enter is actually applied in increments of 64 kbits/s. If the value is 0, it effectively disables the rate limit.	0

3.9 Port Trunking

Port Trunking can help you aggregate more links to form one link group. The LAG function of Delta DVS series switch supports 3 trunk groups, and you can assign 8 ports to one group. But there is a limit of 3 gigabit ports or 7 10/100Mbps ports for each lag ID. Link Aggregation (LA) increases the capacity and availability of the communication channel between devices (both switches and end stations) using existing Fast Ethernet and the Gigabit Ethernet technology. LA also provides load balancing where the processing activity and the communication activity are distributed across several links in a trunk.
If there are 4 ports in a trunk group, and one port fails, then the other seven ports will provide backups and share the traffic automatically. LA also can be used to combine 4 ports between Delta DVS series switches. If all ports on these two switches are configured as 100BaseTX and full duplex, then the potential bandwidth of the connection can be 400Mbps.The function theory is shown in the figure below.



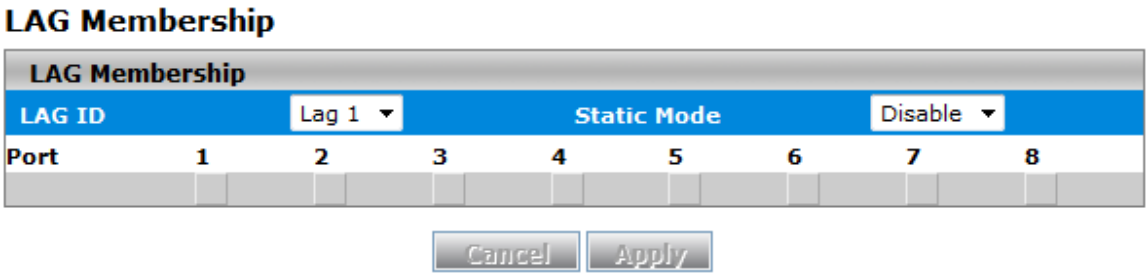
IMPORTANT:
Make sure that you save the configuration in the Save Configuration page after you have applied the configuration changes. (Save Config→Save Configuration) If you do not save the configuration, then the configuration will be cleared after the switch is rebooted.

3.9.1 LAG

Link aggregation groups (LAGs) let you combine multiple full-duplex Ethernet links into a single logical link. LAG increases fault tolerance and provide traffic sharing. You can assign LAG VLAN membership after you have added interfaces as members of a LAG.
After you have added interfaces to a LAG and enabled the LAG, Link Aggregation Control Protocol (LACP) can automatically configure a port channel link between the switch and another device.

3.9.1.1 LAG Membership

When the static mode of the port-channel is enabled, it does not transmit or receive LACPDUs. For example, the member ports do not transmit LACPDUs and all the LACPDUs which are received may be dropped. The factory default is disabled, which means the port-channel is dynamic.
If you want to enable the static mode of a LAG on the Delta switch, make sure that the static mode of a LAG of the other switch which connects to the Delta switch is enabled, too.

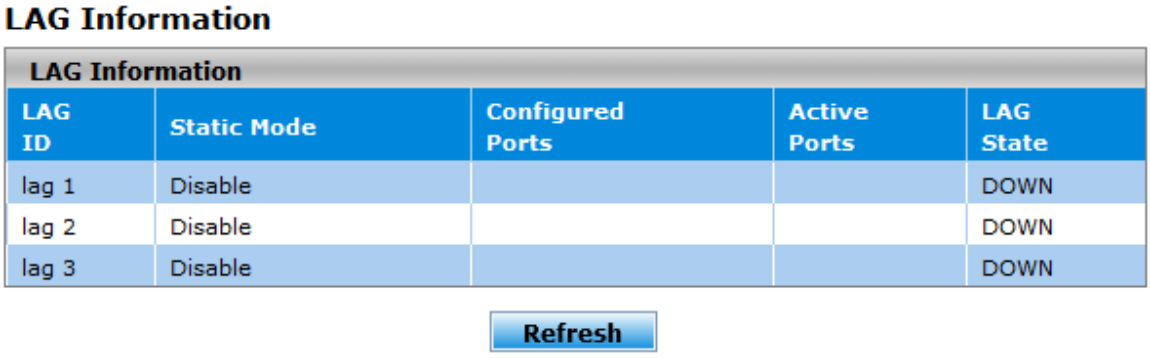


LAG Membership

Item	Description
LAG ID	Select the LAG ID from the drop-down list.
Static Mode	Specify whether the static mode of the LAG ID is enabled.
Port	Select one or more interfaces by clicking the square or click for the second time to clear the interface.

3.9.1.2 LAG Information

The LAG information is displayed on this page.



LAG Information

Item	Description
LAG ID	This field displays the LAG identifier.
Static Mode	The field displays whether the static mode is enabled.
Configured Ports	The field displays the ports which have been configured to the LAG ID.
Active Ports	The field displays the active ports.
LAG State	The field displays whether the LAG state is link up or link down.

3.10 Access Control List

Access control lists (ACLs) can make sure that only authorized devices have access to specific resources when any unauthorized devices which are blocked attempt to access network resources. ACLs provide security for the network, traffic flow control, and determine which types of traffic can be forwarded or blocked.
The Delta switch supports ACLs based on the MAC addresses of the source and destination devices (MAC ACLs).

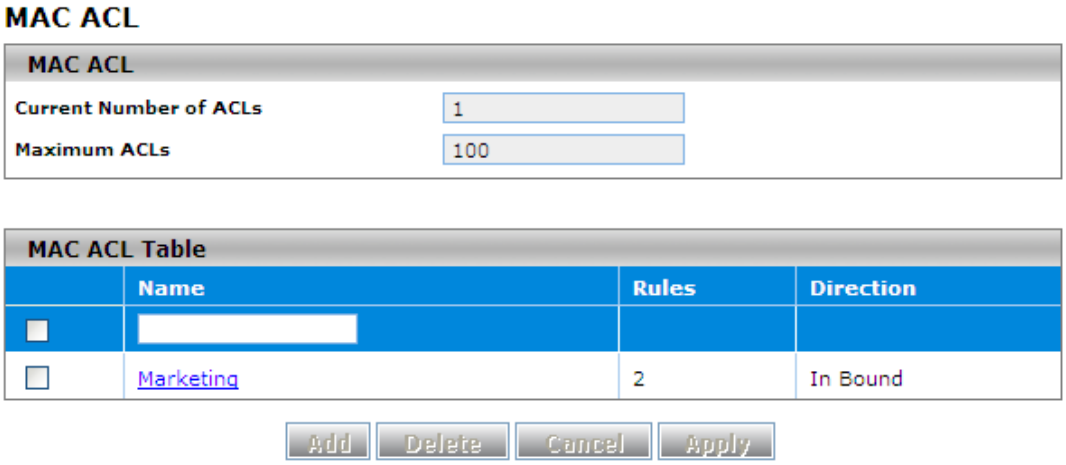
The steps of configuring an ACL:

1. Create a MAC-based ACL name.
2. Create a rule and assign it to an ACL.
3. Assign an ACL to an interface.

IMPORTANT:
Make sure that you save the configuration in the Save Configuration page after you have applied the configuration changes. (Save Config→Save Configuration) If you do not save the configuration, then the configuration will be cleared after the switch is rebooted.

3.10.1 MAC ACL

A MAC ACL consists of a set of rules that are matched sequentially to compare the packets. With a MAC ACL, you can specify the MAC address of the source device, destination device, or both. When a packet matches the criteria with a rule, and the specified rule action(permit or deny) is applied, then any additional rules will not be checked whether the packet is matched or not.



MAC ACL

Setting	Description
Current Number of ACLs	The field displays the sum of the configured ACLs.
Maximum ACLs	The field displays the maximum number of MAC ACLs that can be configured (100).

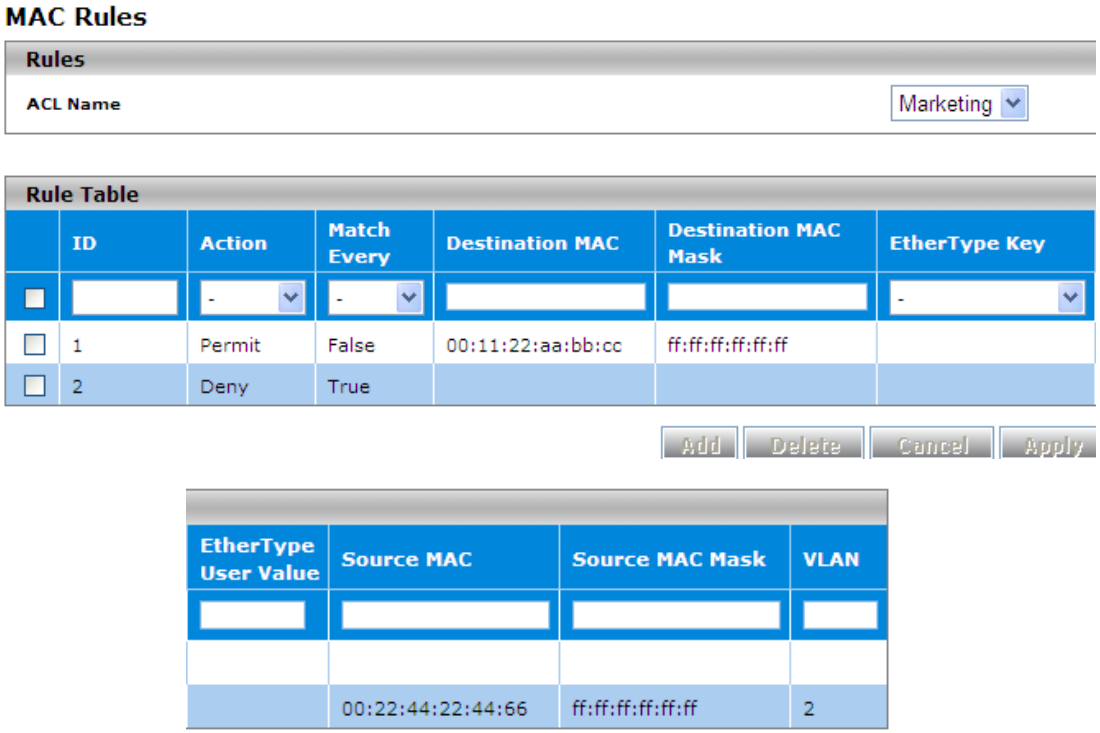
MAC ACL Table

Setting	Description
Name	Specify a name for an ACL. The name can include alphabetic, numeric, dash, underscore, or space characters. It must start with an alphabetic character.
Rules	The number of rules that are configured for the MAC ACL.
Direction	The direction of the packet traffic that is affected by the MAC ACL. This is a fixed entry that always shows In Bound; only inbound traffic is subject to the MAC ACL.

3.10.1.1 MAC Rules

After creating an ACL name, you can configure the action, match, destination MAC, source MAC and VLAN on this page. It can determine whether the packet is forwarded normally or discarded.

Note:
You need to create an implicit *deny all* rule at the end of an ACL rule table to make sure that a packet is dropped if an ACL is applied to the packet and none of the explicit rules match.



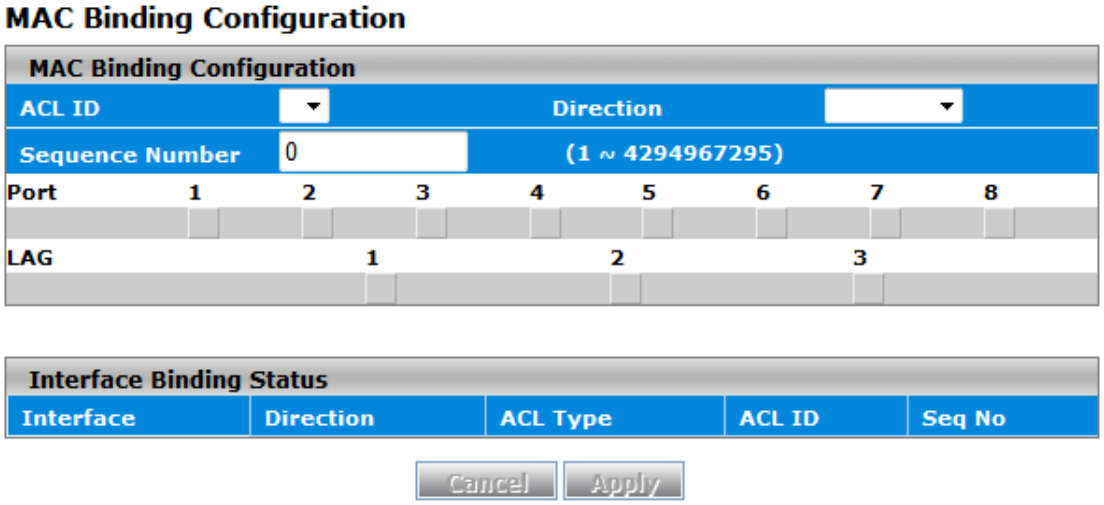
Rule Table

Description	Factory default
ID	
Enter an ID for the rule. Enter a number between 1 and 10. This means that you can create up to 10 rules for a single MAC ACL name.	None
Action	
Specify the action for the rule: • **Permit:** Packets that meet the ACL criteria are forwarded. • **Deny:** Packets that meet the ACL criteria are dropped.	None
Match Every	
Specify whether all packets need to match the rule: • **True:** All packets need to match the rule. Other rules are not considered, and the fields to the right of the Match Every field are disabled. • **False:** Not all packets need to match the rule. Other rules are also considered.	True
Destination MAC	
Specify the MAC address of the destination device that needs to be compared with the information in a packet. Enter a MAC address in the xx:xx:xx:xx:xx:xx format.	None
Destination MAC Mask	

Description	Factory default
Specify the MAC mask that is associated with the destination MAC address. The MAC mask specifies the bits in the destination MAC address which need to be compared with the information in a packet. **Note:** Use zeros and Fs in the MAC mask. An F means that the bit is not checked, and a zero in a bit position means that the data needs to be equal to the value given to that bit. For example, if the MAC address is aa:bb:cc:dd:ee:ff, and the mask is 00:00:ff:ff:ff:ff, all MAC addresses with aa:bb:xx:xx:xx:xx result in a match (where x is any hexadecimal number).	None
EtherType Key	
Specify the EtherType that needs to be compared with the information in a packet: **Appletalk, ARP, IBM SNA, IPv4, IPv6, IPX, MPLS multicast, MPLS unicast, NetBIOS, Novell, PPPoE, Reverse ARP, EthernCAT, Profinet-RT, SERCOS III, CC-link IE, Powerlink, User Value**. If you select User Value, enter the value in the EtherType User Value field.	None
EtherType User Value	
If you select User Value from the EtherType Key drop-down list, enter the value, which is a number in the range of 1536 to 65535.	None
Source MAC	
Specify the MAC address of the source device that needs to be compared with the information in a packet. Enter a MAC address in the xx:xx:xx:xx:xx:xx format.	None
Source MAC Mask	
As an option, specify the MAC mask that is associated with the source MAC address. The MAC mask specifies the bits in the source MAC address which need to be compared with the information in a packet. **Note:** Use zeros and Fs in the MAC mask.An F means that the bit is not checked, and a zero in a bit position means that the data needs to be equal to the value given to that bit. For example, if the MAC address is aa:bb:cc:dd:ee:ff, and the mask is 00:00:ff:ff:ff:ff, all MAC addresses with aa:bb:xx:xx:xx:xx result in a match (where x is any hexadecimal number).	None
VLAN	
Specify the VLAN ID that needs to be compared with the information in a packet. Enter a number in the range of 0 to 4095. You can not enter a VLAN range. **Note:** Most VLAN configurations on the switch are in the range of 1 to 4093. However, an ACL can detect a VLAN in the range of 0 to 4095.	None

3.10.1.2 MAC Binding Configuration

When you bind a MAC ACL to an interface, all rules that you have defined for the MAC ACL are applied to the interface.



MAC Binding Configuration

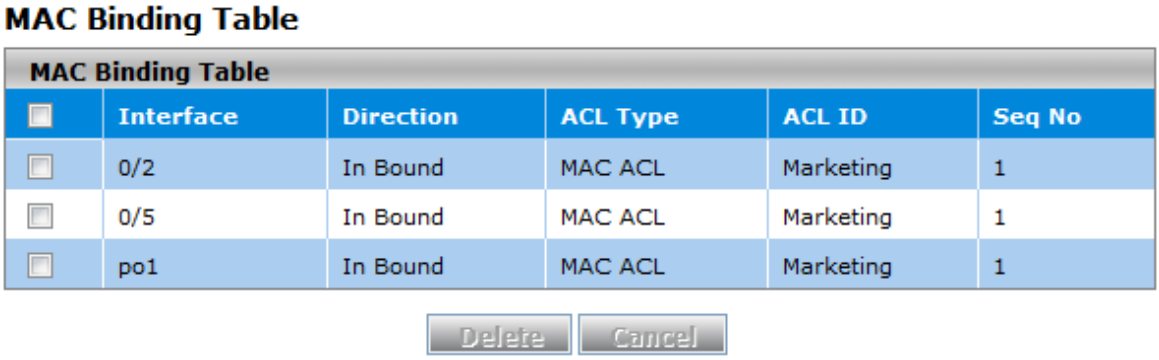
Setting	Description
ACL ID	Select an ACL ID to bind MAC.
Direction	The Direction drop-down list is fixed at Inbound. Only incoming packets can be filtered.
Sequence Number	Enter a number in the range of 1 to 4,294,967,295.
Port	Select one interface or more interfaces by clicking the square or click for the second time to clear the interface.
LAG	Select one LAG or more LAGs by clicking the square or click for the second time to clear the interface.

Interface Binding Status

Setting	Description
Interface	The interface to which the MAC ACL is bound
Direction	The packet filtering direction for the MAC ACL. The only valid direction is Inbound, which means the MAC ACL rules are applied to traffic entering the interface.
ACL Type	The type of ACL to which the interface is bound. This is a fixed field that always shows MAC ACL.
ACL ID	The name of the ACL to which the interface is bound
Seq No	The sequence number that signifies the order of the ACL to which the interface is bound. The number should be configured from 1 to 4,294,967,295. The sequence number specifies the order of the ACL relative to the existing ACLs that are bound to the same interface or interfaces. A lower number specifies a higher precedence order. If a sequence number is already in use for the interface or interfaces, the ACL replaces the existing ACL that uses the same sequence number.

3.10.2 Binding Table

The MAC binding information is displayed on this page.



MAC Binding Table

Setting	Description
Interface	The interface to which the MAC ACL is bound
Direction	The packet filtering direction for the MAC ACL. The only valid direction is Inbound, which means the MAC ACL rules are applied to traffic entering the interface.
ACL Type	The type of ACL to which the interface is bound. This is a fixed field that always shows MAC ACL.
ACL ID	The name of the ACL to which the interface is bound
Seq No	The sequence number that signifies the order of the ACL to which the interface is bound.

3.11 Security Settings

The Delta DVS series switch provides many ways to verify the packets, authenticate users or block the attack traffic. You can choose and configure these security settings according to your network environment.

> **IMPORTANT:**
> **Make sure that you save the configuration in the Save Configuration page after you have applied the configuration changes. (Save Config→Save Configuration) If you do not save the configuration, then the configuration will be cleared after the switch is rebooted.**

3.11.1 Security

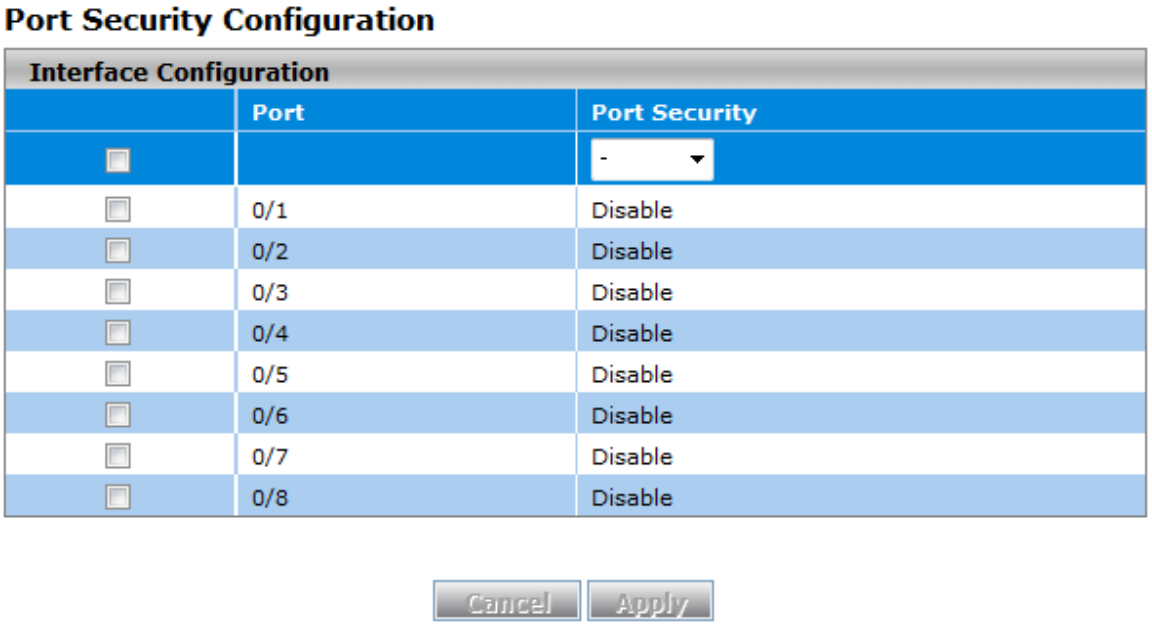
This group allows you to configure a MAC address, an IP address or the Port authentication to reach the security purpose.

3.11.1.1 Port Security

The port security lets you lock the interface. If the port security of the interface is enabled, then it can only forward the traffic from the MAC addresses that you specified.
The Port Security feature allows you to stop the MAC address learning for a specific port. After you stop the MAC learning (enable Port Security), only the source MAC address of the packet listed in the Static MAC address table with the binding port can access the switch through the port, and other packets will be discarded.

Port Security Configuration

You can specify the interface and enable or disable the port security on this page.

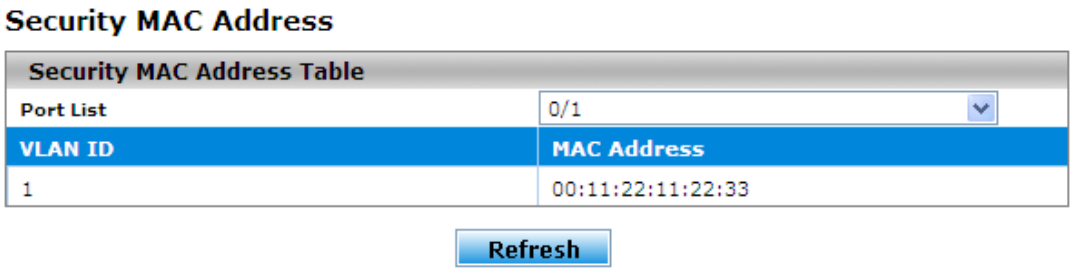


Interface Configuration

Description	Factory default
Port	
The interface number	*interface number*
Port Security	
Specify whether the port security is enabled: • **Enable:** The port security is enabled for the individual interface. The port security also needs to be globally enabled for it to be effective. • **Disable:** The port security is disabled for the individual interface. This setting overrides the global port security setting.	Disable

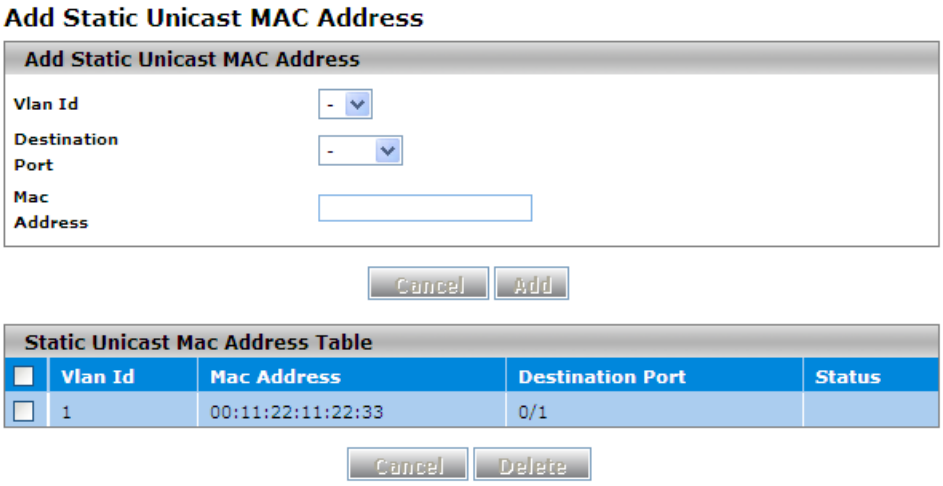
Security MAC Address

The security MAC address table shows the static MAC addresses which is associated with the VLANs. Select the interface for which you want to display the static MAC addresses and their associated VLANs.



Add Static MAC Address

You can specify the MAC address for a port with a VLAN ID on this page.



Add Static Unicast MAC Address

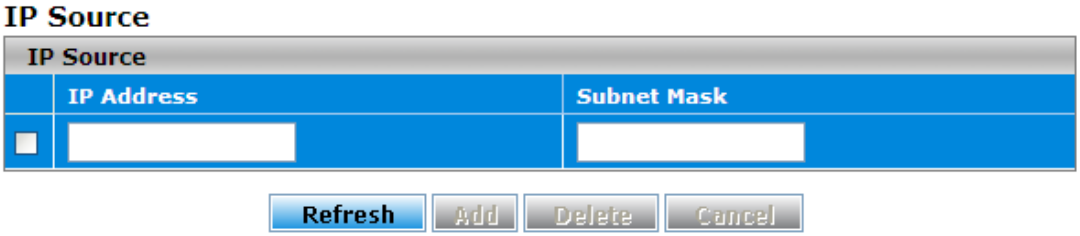
Setting	Description
VLAN ID	Specify the VLAN ID to which the unicast traffic is assigned.
Destination Port	Specify the switch interface or link aggregation group to which the unicast traffic is directed. **Note:** Make sure that the destination port you choose is the member of VLAN ID that you select
MAC Address	Enter the MAC address of the device that is the source of the unicast traffic.

Static Unicast Mac Address Table

Setting	Description
VLAN ID	Display the VLAN ID to which the unicast traffic is assigned.
MAC Address	Display the MAC address of the device that is the source of the unicast traffic.
Destination Port	Display the switch interface or link aggregation group to which the unicast traffic is directed.
Status	Display the timeout status. It is fixed in the **Permanent** status.

3.11.1.2 IP Source

You can configure a specific IP address to access the Delta switch. Only the IP addresses which is added to this list can access and configure the Delta switch.

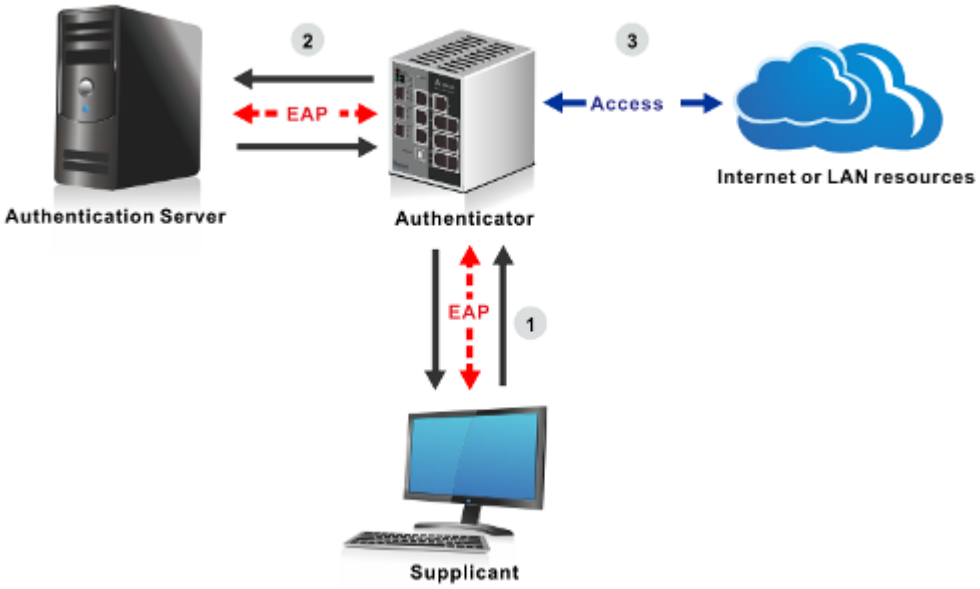


IP Source

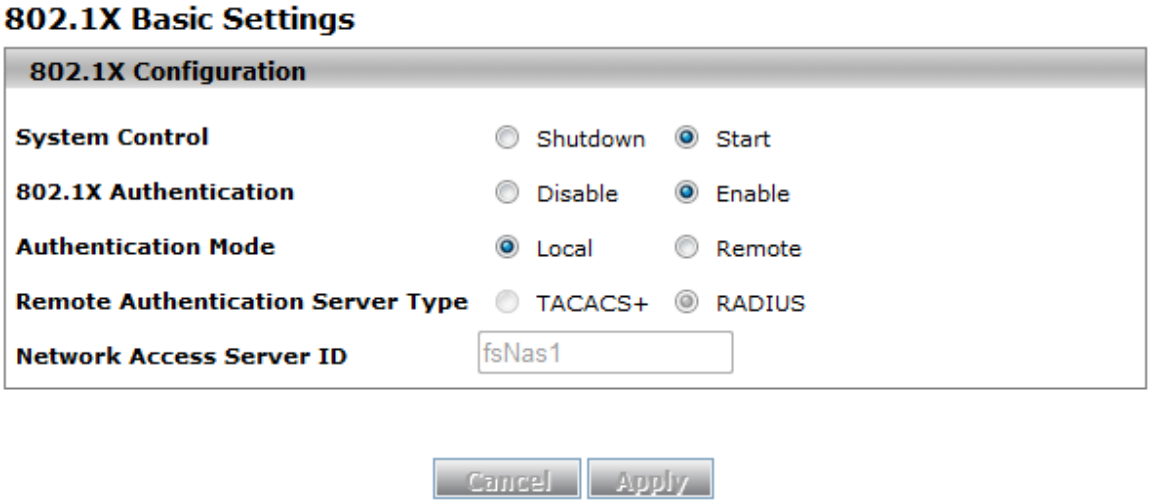
Setting	Description
IP Address	
Enter the source IP address for security.	None
Subnet Mask	
Enter the subnet mask of the IP address.	None

3.11.1.3 802.1X

The Delta switch can act as an authenticator in the 802.1X environment. You can either use an external authentication server, or implement the authentication server in the Delta switch by using a Local User Database.
There are three components used to create a port-based authentication mechanism based on 802.1X:
Supplicant: The end of the station that requests the access to the LAN resource and switch services.
Authentication Server: The external server that performs the actual authentication of the supplicant, for example, a RADIUS server. It performs the authentication to indicate whether the user is authorized to access services.
Authenticator: It acts as a proxy between the supplicant and the authentication server. This kind of role is usually the edge switch or the wireless AP. It requests identity information from the supplicant, verifies the information with the authentication server, and relay a response to the supplicant.
The function theory is shown in the figure below.



802.1X Basic Settings
IEEE 802.1X is an IEEE Standard for port-based Network Access Control (PNAC). It is a part of the IEEE 802.1 group of networking protocols. It provides an authentication mechanism for devices which attempt to connect with a LAN or WLAN. IEEE 802.1X defines the encapsulation of the Extensible Authentication Protocol (EAP) over IEEE 802 which is known as "EAP over LAN" or EAPOL.



802.1X Basic Settings

Description	Factory default
System Control	
Specify whether the 802.1X authentication module on the switch is running or shut down. • **Shutdown:** The 802.1X authentication is shut down. You can not configure or enable the 802.1X authentication. • **Start:** The 802.1X authentication is running, and you can configure and enable it.	Start
802.1X Authentication	
Specify the status of the 802.1X authentication on the switch. • **Disable:** The 802.1X authentication is disabled. You can still configure the 802.1X authentication, but the settings do not take effect after you have applied them. The switch does not check the 802.1X authentication before allowing traffic on any interfaces, even if the interfaces are configured to allow only authenticated users. • **Enable:** The 802.1X authentication is enabled. You can configure the 802.1x authentication, and the settings take effect after you have applied them.	Enable
Authentication Mode	
Specify the 802.1X authentication mode. • **Local:** A locally stored user ID and password are used for port authentication. You need to set up a user account on the Local Authentication Server page. This is the default setting. • **Remote:** A RADIUS or TACACS+ server is used for the port authentication. With this selection, the Remote Authentication Server Type radio buttons and Network Access Server ID become available.	Local
Remote Authentication Server Type	
If you select the Remote mode of Authentication Mode, specify whether a RADIUS or TACACS+ server should be used. • **TACACS+:** The user ID and the password are authenticated through a TACACS+ server. • **RADIUS:** The user ID and the password are authenticated through a RADIUS server.	RADIUS
Network Access Server ID	
If you select the Remote radio button next to Authentication Mode, enter the network access server (NAS) ID, or use the default ID (fsNas1).	Fixed

Port Authentication

You can configure the authentication settings for each interface.

Port Authentication

Port Authentication

	Port	Control Mode	Periodic Reauthentication	Reauthentication Period	EAPOL Packets Flood
☐		-	-		-
☐	0/1	ForceAuthorized	Disabled	3600	Disabled
☐	0/2	ForceAuthorized	Disabled	3600	Disabled
☐	0/3	ForceAuthorized	Disabled	3600	Disabled
☐	0/4	ForceAuthorized	Disabled	3600	Disabled
☐	0/5	ForceAuthorized	Disabled	3600	Disabled
☐	0/6	ForceAuthorized	Disabled	3600	Disabled
☐	0/7	ForceAuthorized	Disabled	3600	Disabled
☐	0/8	ForceAuthorized	Disabled	3600	Disabled

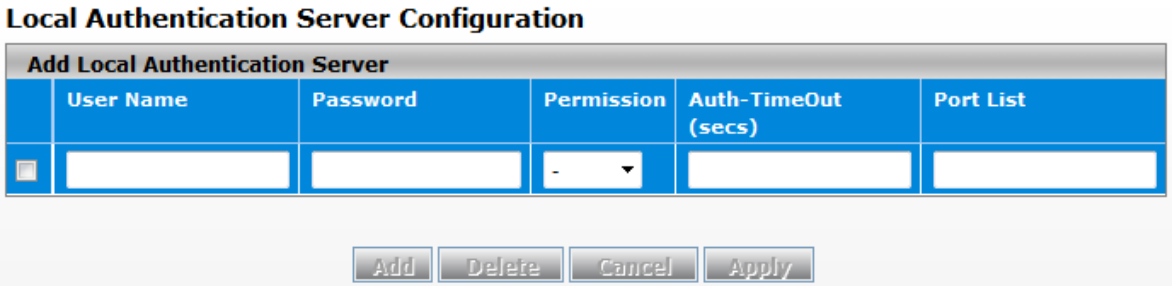
Apply Cancel Refresh

Port Authentication

Description	Factory default
Port	
This field displays the port number.	Port number
Control Mode	
Specify the control mode for the port authorization. The control mode is active only if the link status of the interface is up. • **ForceUnauthorized:** Places the interface in the unauthorized state. The switch can not provide authentication services for a client through the interface. • **Auto:** After any supplicant completes the authentication successfully on the interface, others can access the network service through the same interface without the authentication. • **ForceAuthorized:** Places the interface in the authorized state. The interface sends and receives normal traffic without the client port-based authentication.	ForceAuthorized
Periodic Reauthentication	
Specify whether the supplicant is periodically reauthenticated for the interface: • **Enabled:** The supplicant is reauthenticated according to the reauthentication period. • **Disabled:** The supplicant is not reauthenticated.	Disable
Reauthentication Period	
Specify the reauthentication period for the interface. The reauthentication period determines when the supplicant is reauthenticated when period reauthentication is enabled. Enter a period in the range of 1 to 65535 seconds.	3600
EAPOL Packets Flood	
Specify whether the EAPOL packet flood mode is enabled for the interface: • **Enabled:** The EAPOL packet flood mode is enabled. Enabling this mode does not provide any protection from an EAPOL packet flood denial of service (DoS) attack. If the switch is used as a hub, you might want to enable the EAPOL packet flood mode. • **Disabled:** The EAPOL packet flood mode is disabled.	Disable

Local Authentication Server

The user list on this page and the user list on the Local Users Management page of Management Security are independent. The user list on this page is for 802.1X authentication. So you can configure a different user name with the user on the Local Management page of Management Security.



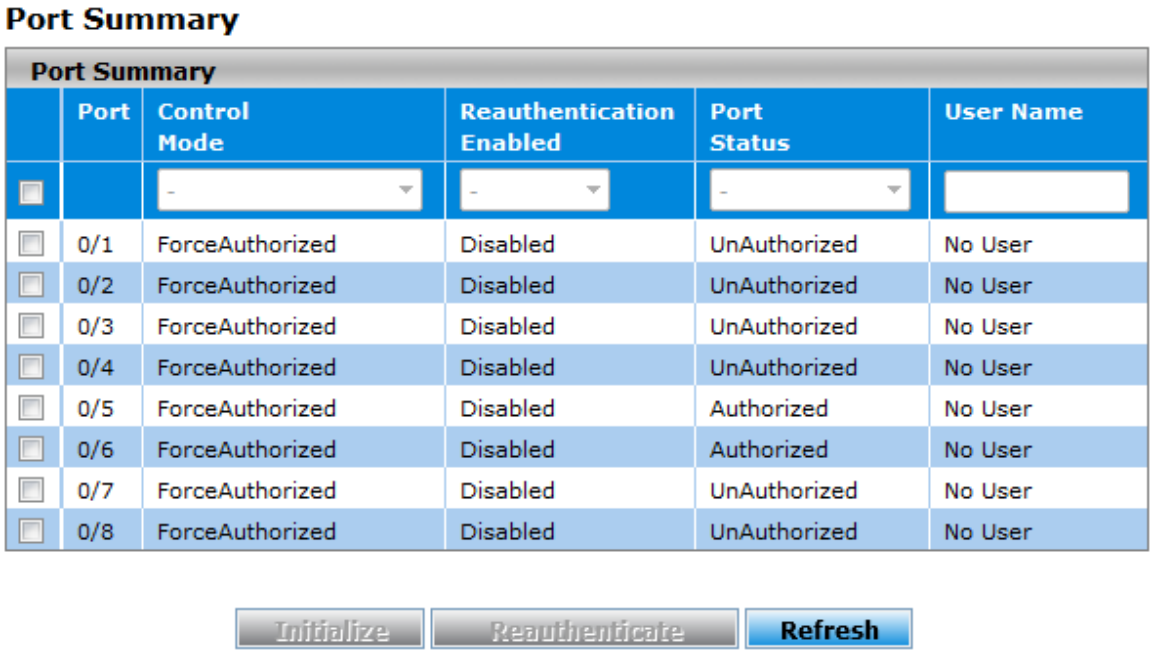
Local Authentication Server Configuration

Description	Factory default
User Name	
Enter a user name.	None
Password	
Enter a password. Passwords should consist of 1 through 20 alphanumeric characters and are case-sensitive. The password is displayed as asterisks (*).	None
Permission	
Specify whether the user is allowed or denied interface access:	None

Description	Factory default
• **Allow:** Allows the user access to the interface. • **Deny:** Denies the user access to the interface.	
Auth-TimeOut (secs)	
Specify the period in seconds after which the server authentication timeout occurs and the user needs to be reauthenticated by the local authentication server. Enter a period between 1 and 7200 seconds. After the supplicant is authorized, the server authentication timeout period overrides the reauthentication period that is configured for the individual interface (see the Port Authentication page). Leave the Auth-TimeOut field blank to use the reauthenticaiton period that is configured for the individual interface. **Note:** If you enable the server reauthentication after a user has already been authenticated by the server, the server authentication timeout period does not take effect, and the reauthentication period value that is configured for the individual interface is used. **Note:** If the server reauthentication is enabled, a user is authenticated by the server. If you change the authentication timeout period, the new authentication timeout period takes effect after the next reauthentication by the server is complete.	None
Port List	
Specify the interfaces from which the authentication needs to be obtained. Leave the field blank to include all interfaces. **Note:** The range of port list is dependant on what type of DVS managed switch you used.	None

Port Summary

This page allows you to view the information about the access control of each interface; you can initialize or reauthenticate the interface manually.

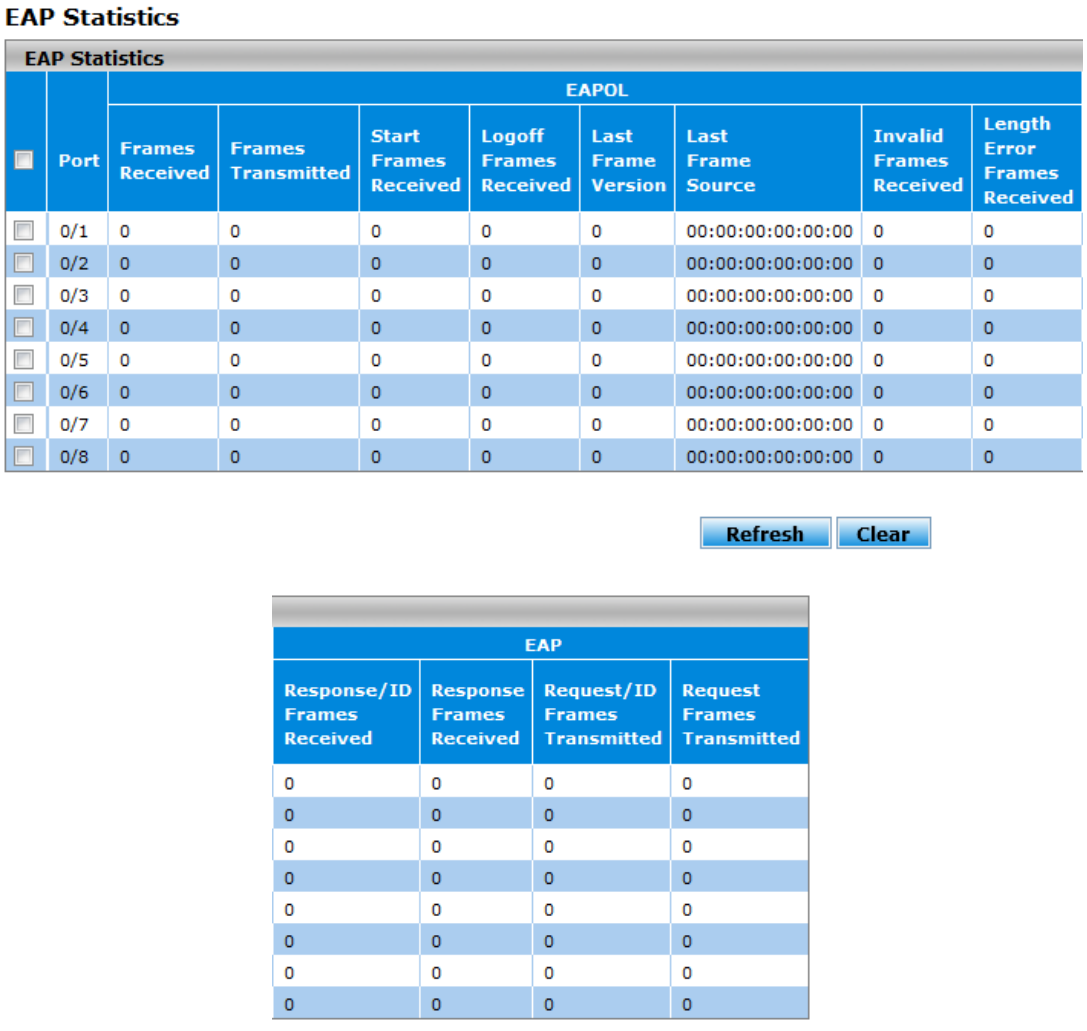


Port Summary

Description	Factory default
Port	
This field displays the port number.	Port number
Control Mode	
The port authorization state that you have configured on the Port Authentication page (see Port Authentication on page 189). One of the following options is displayed: • **ForceUnauthorized:** The interface functions in the unauthorized state. The switch can not provide authentication services for a client through the interface. • **Auto:** The interface automatically detects the control mode through authentication exchanges among the supplicant, the authenticator, and the authentication server. • **ForceAuthorized:** The interface functions in the authorized state. The interface sends and receives normal traffic without the client port-based authentication.	ForceAuthorized
Reauthentication Enabled	
Indicates whether you have enabled or disabled the reauthentication on the interface.	Disabled
Port Status	
The authorization status of the interface (Authorized or Unauthorized)	UnAuthorized
User Name	
The name of the user most recently authenticated on the port. The user name is for a user account that is defined on the **Local Authentication Server** page.	None

EAP Statistics

This page allows you to view the EAP statistics.



EAP Statistics

Item	Description
Port	The interface number
EAPOL (Extensible Authentication Protocol over LAN)	
Frames Received	The total number of received valid EAPOL frames
Frames Transmitted	The total number of transmitted EAPOL frames
Start Frames Received	The total number of received EAPOL start frames
Logoff Frames Received	The total number of received EAPOL logoff frames
Last Frame Version	The protocol version number attached to the most recently received EAPOL frame
Last Frame Source	The source MAC address attached to the most recently received EAPOL frame
Invalid Frames Received	The total number of received unrecognized EAPOL frames
Length Error Frames Received	The total number of received EAPOL frames with an invalid packet body length
EAP (Extensible Authentication Protocol)	
Response/ID Frames Received	The total number of received EAP response ID frames
Response Frames Received	The total number of received valid EAP response frames
Request/ID Frames Transmitted	The total number of transmitted EAP requested ID frames
Request Frames Transmitted	The total number of transmitted EAP request frames

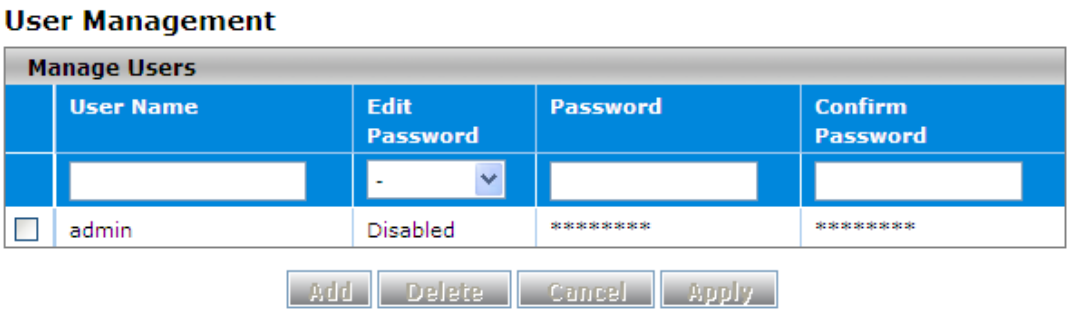
3.11.2 Management Security

In the Management Security group, you can manage local users, the Remote Authorization Dial-In User Service (RADIUS) settings, the Terminal Access Controller Access Control System (TACACS+) settings, and Login Authentication Mode, and monitor the sessions of login users.

3.11.2.1 Local Users Management

For information security, the Delta managed switch provides two access levels of the user to log on the Web management page.Beside the admin account, other user accounts can modify the basic feature which will display in the window when they login. The Web management pages contained in this manual are subject to the admin's login without any explanation.

Note:
If you need the record of the user's log, you can configure the log severity information in Log Configuration of SYSLOG.
Please refer to **Show logs** and **Log Configuration**.

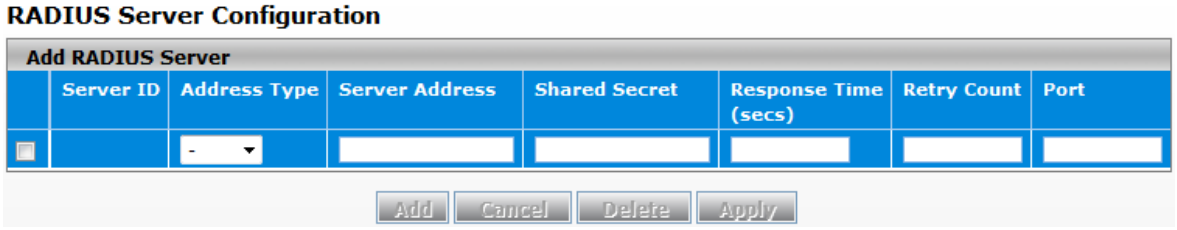


User Management

Description	Factory default
User Name	
Enter a user name. It supports up to 20 users, and a user name consists of up to 20 characters and is case sensitive. Only alphanumeric characters, dashes (-) and underscores (_) are accepted.	None
Edit Password	
Select Enabled, and then edit the password.	None
Password	
Enter a password. Passwords are 1–20 alphanumeric characters in length and are case sensitive. The password is displayed as eight asterisks (*).	None
Confirm Password	
Enter the same password that you entered in the **Password** field.	None

3.11.2.2 RADIUS Server Config

RADIUS (Remote Authentication Dial In User Service) is a networking protocol that provides the centralized Authentication, Authorization, and Accounting (AAA) management for computers to connect and use a network service. The system implements the RADIUS client and provides the authentication functionality. RADIUS uses UDP port 1812 by default.

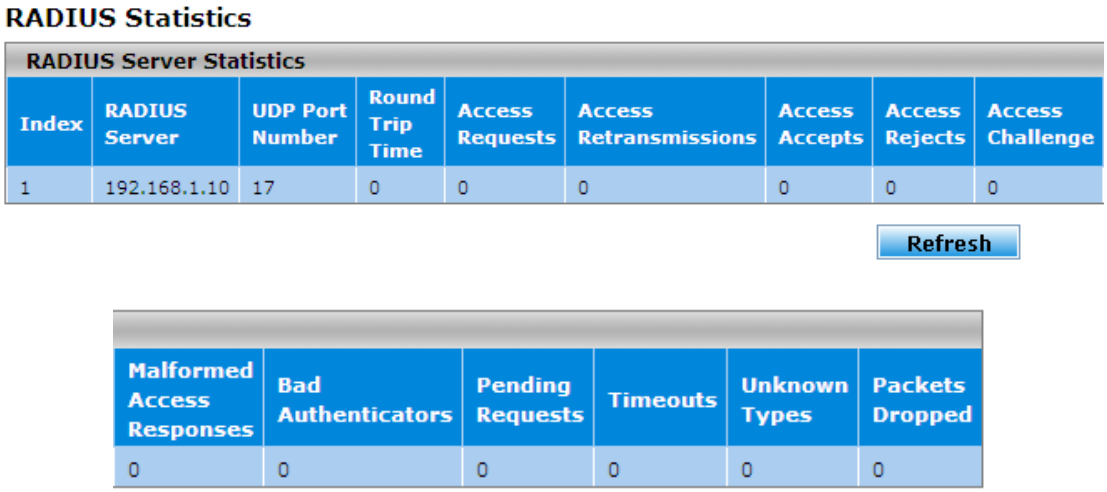


RADIUS Server Configuration

Description	Factory default
Server ID	
The identifier of the server	None
Address Type	
Specify a type of address for the RADIUS server: • **IPv4:** The RADIUS server has an IPv4 address. • **DNS:** The RADIUS server has a DNS host name.	None
Server Address	
Enter the IP address or the DNS host name of the RADIUS server. (It depends on whether the Address Type field is IPv4 or DNS.)	None
Shared secret	
Enter the shared secret (only characters and numbers) that is used to authenticate and encrypt communications between the switch and the RADIUS server. This secret needs to match the one on the RADIUS server.	None
Response Time (secs)	
Enter the response time in seconds. This is the maximum period that the switch waits for a response from the RADIUS server before retransmitting the authentication request. Enter a period in the range of 1 to 120 seconds.	10
Retry Count	
Enter the maximum number of times an authentication request is retransmitted. Enter a number in the range of 1 to 254.	3
Port	
Enter the UDP port number of the RADIUS server that is used for the authentication.	1812

3.11.2.3 RADIUS Statistics

After you add a server to the RADIUS Server Configuration page, the statistics is displayed on this page.

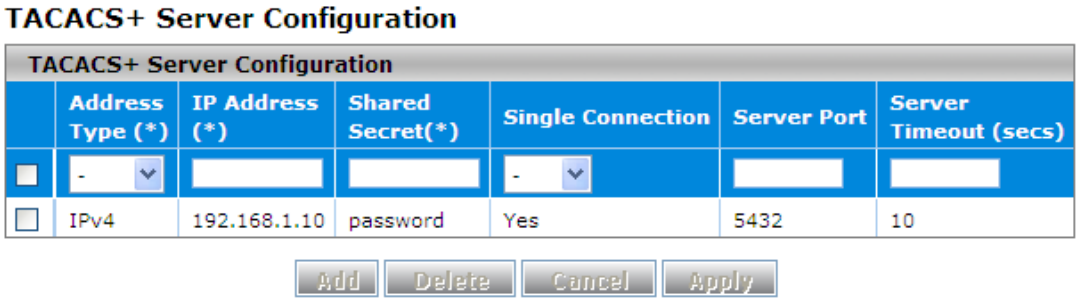


RADIUS Statistics

Item	Description
Index	The index number of the RADIUS server in the table
RADIUS Server	The IP address of the RADIUS server
UDP Port Number	The UDP port of the RADIUS server that is used for the authentication
Round Trip Time	The period, in hundredths of a second, between the most recent access reply/access challenge and the access request that matched it from the RADIUS server
Access Requests	The number of access-request packets that were transmitted to the RADIUS server. This number does not include retransmissions.
Access Retransmissions	The number of access-request packets that were retransmitted to the RADIUS server
Access Accepts	The number of access-accept packets, including both valid and invalid packets, which were received from the RADIUS server
Access Rejects	The number of access-reject packets, including both valid and invalid packets, which were received from the RADIUS server
Access Challenge	The number of access-challenge packets, including both valid and invalid packets, which were received from the RADIUS server
Malformed Access Responses	The number of malformed access-response packets that were received from the RADIUS server. Malformed packets include packets with an invalid length. Bad authenticators or signature attributes or unknown types are not included as malformed access responses.
Bad Authenticators	The number of access-response packets containing invalid authenticators or signature attributes that were received from the RADIUS server
Pending Requests	The number of access-request packets destined for the RADIUS server that have not yet timed out or received a response
Timeouts	The number of authentication requests that were sent to the RADIUS server and that timed out
Unknown Types	The number of packets of an unknown type that were received from the RADIUS server
Packets Dropped	The number of packets that were received from the RADIUS server and that were dropped

3.11.2.4 TACACS+ Server

TACACS+ (Terminal Access Controller Access-Control System Plus) provides access control for routers, network access servers (NAS) and other networked computing devices. The system implements the TACACS+ client and provides authentication functionality.
TACACS+ uses TCP port 49 by default. You can configure it according to your TACACS+ server. The Delta switch supports multi TACACS+ servers' configuration and the number is up to 5.

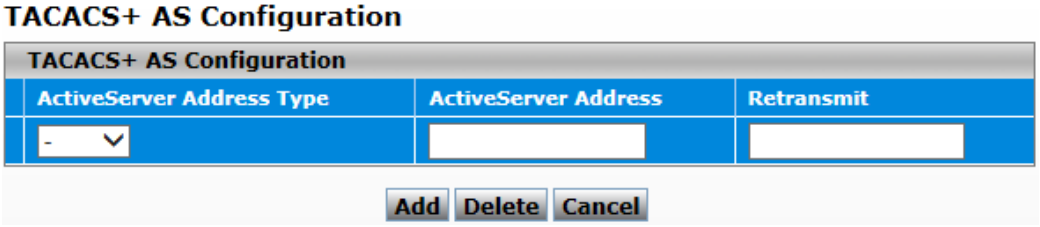


TACACS+ Server Configuration

Description	Factory default
Address Type (*)	
Specify a type of address for the TACACS+ server. • **IPv4:** The TACACS+ server has an IPv4 address. • **DNS:** The TACACS+ server has a DNS host name.	None
IP Address (*)	
Depending on the selection from the Address Type drop-down list, enter the IP address or the DNS host name of the TACACS+ server.	None
Shared Secret (*)	
Enter the shared secret (up to 63 characters and numbers) that is used to authenticate and encrypt communications between the switch and the TACACS server. This secret needs to match the one on the TACACS server.	None
Single Connection	
Specify a type of connection: • **Yes:** Allows only a single TCP connection with the TACACS server. • **No:** Allows multiple TCP connections with the TACACS server.	No
Server Port	
Enter the TCP port number of the TACACS server that is used for authentication. The port number should be in the range of 1 to 65535.	49
Server Timeout (secs)	
Enter the period in seconds after which the connection between the client device and the TACACS server times out. Enter a period in the range of 1 to 255 seconds.	5

3.11.2.5 TACACS+ AS

If you do not specify a TACACS+ AS (TACACS+ Active Service), the switch uses one of the TACACS+ servers that you specify on the TACACS+ Server Configuration page. If you specify a TACACS+ Active Server (AS), the switch uses only that server as the active TACACS+ server. So you can only specify one active server on this page.

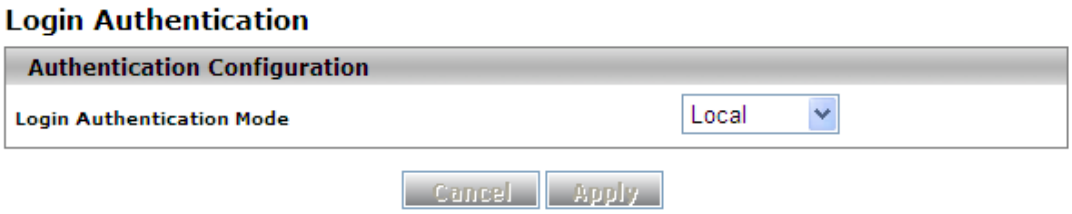


TACACS+ AS Configuration

Description	Factory default
Active Server Address Type	
Specify a type of address for the TACACS+ AS. • **IPv4:** The TACACS+ AS server has an IPv4 address. • **DNS:** The TACACS+ AS server has a DNS host name.	None
Active Server Address	
Depending on the selection from the Active Server Address Type drop-down list, enter the IP address or the DNS host name of the TACACS+ AS. The IP address or the DNS host name needs to be already listed in the TACACS+ Server Configuration table.	None
Retransmit	
The number of times the switch searches for the AS in the TACACS+ Server Configuration table if the switch can not establish a connection with the AS at the first attempt. Enter a number in the range of 1 to 100.	2

3.11.2.6 Login Authentication

The Delta switch provides three authentication methods: Local, RADIUS, and TACACS+. If there is no RADIUS or TACACS+ server in your network environment, you can use the local authentication method for the login authentication.

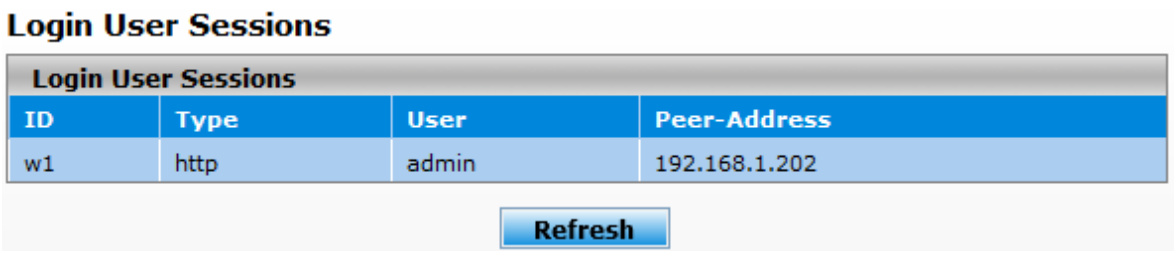


Login Authentication

Description	Factory default
Login Authentication Mode	
Specify the login authentication method: • **Local:** A locally stored user ID and a password are used for the authentication. This is the default setting. You need to set up a user account on the Local User Management page. • **RADIUS:** The user ID and the password are authenticated through a RADIUS server. • **TACACS+:** The user ID and the password are authenticated through a TACACS+ server.	Local

3.11.2.7 Login User Sessions

The login user session is displayed on this page. The Delta switch supports up to 20 users, including the default user admin.

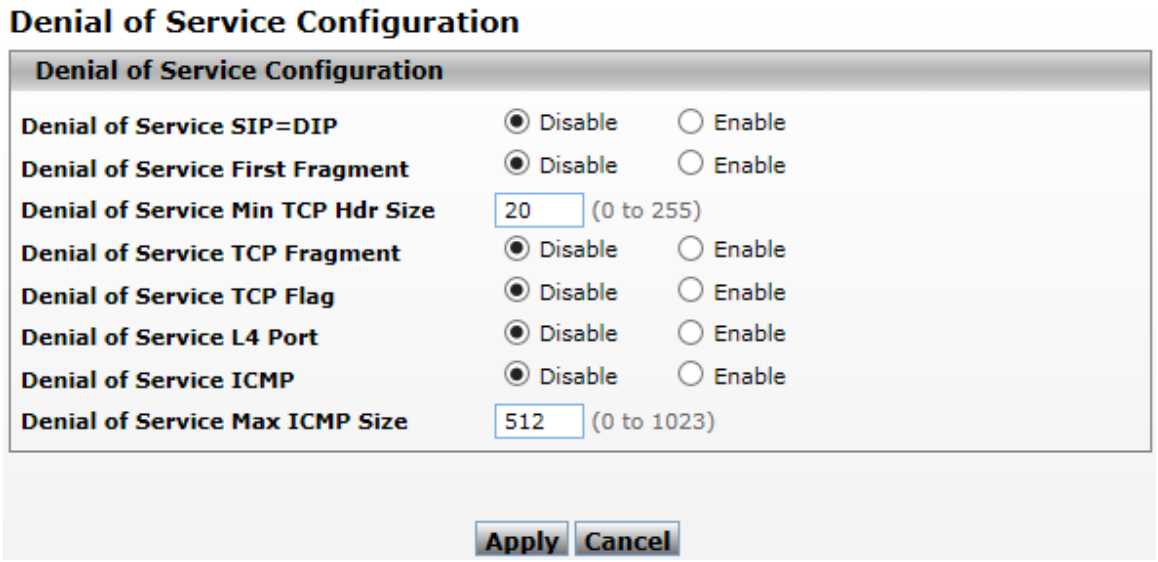


Login User Sessions

Item	Description
ID	The unique session identifier
Type	The session types: • console • telnet • ssh • http • https
User	The name of the user who log in.
Peer-Address	The IP address to which the user log in.

3.11.3 Denial of Service

The Delta switch provides six types of denial of service (DoS) attacks for you to block and monitor attacks. Please refer to the following table for description.



Denial of Service Configuration

Description	Factory default
Denial of Service SIP=DIP	
Select one of the following radio buttons: • **Disable:** This is the default setting. • **Enable:** Packets that have a source IP (SIP) address equal to the destination IP (DIP) address are dropped.	Disable
Denial of Service First Fragment	
Select one of the following radio buttons: • **Disable:** This is the default setting. • **Enable:** Packets with a TCP header that is smaller than the configured minimum TCP header size are dropped.	Disable
Denial of Service Min TCP Hdr Size	
Specify the minimum TCP header size. Enter a value in the range of 0 to 255 bytes.	20
Denial of Service TCP Fragment	
Select one of the following radio buttons: • **Disable:** This is the default setting. • **Enable:** Packets that have an IP fragment offset equal to 1 are dropped.	Disable
Denial of Service TCP Flag	
Select one of the following radio buttons: • **Disable:** This is the default setting.	Disable

Description	Factory default
• **Enable:** All of the following packets are dropped: - Packets that have a TCP flag SYN set and a TCP source port with a number lower than 1024 - Packets that have TCP control flags set to 0 and the TCP sequence number set to 0 - Packets that have TCP flags FIN, URG, and PSH set and TCP sequence number set to 0 - Packets that have both the TCP flags SYN and FIN set	
Denial of Service L4 Port	
Select one of the following radio buttons: • **Disable:** This is the default setting. • **Enable:** Packets that have a TCP source port that is equal to the TCP destination port are dropped, and packets that have a UDP source port that is equal to the UDP destination port are dropped.	Disable
Denial of Service ICMP	
Select one of the following radio buttons: • **Disable:** This is the default setting. • **Enable:** The ICMP packets that have the type set to ECHO_REQ (ping) and a size greater than the configured ICMP packet size are dropped.	Disable
Denial of Service Max ICMP Size	
Specify the maximum ICMP packet size. Enter a value in the range of 0 to 1023 bytes. The default setting is 512 bytes.	512

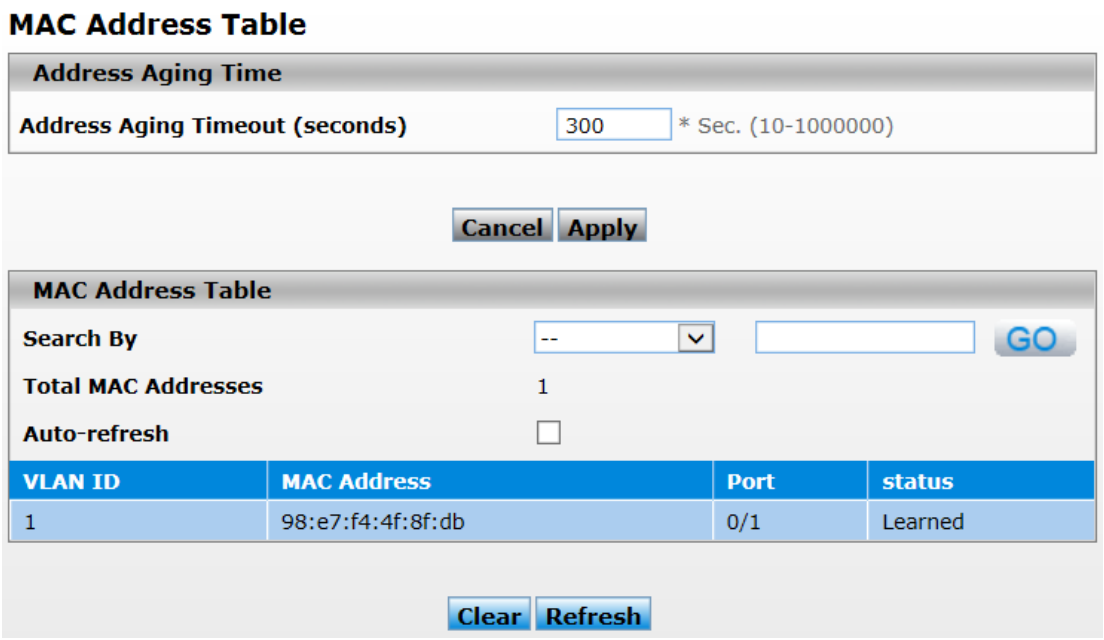
3.12 Monitoring Settings

You can monitor the status of the Delta switch in real time via the functions in this group.

> **IMPORTANT:**
> **Make sure that you save the configuration in the Save Configuration page after you have applied the configuration changes. (Save Config→Save Configuration) If you do not save the configuration, then the configuration will be cleared after the switch is rebooted.**

3.12.1 MAC Address Table

The MAC address table displays the MAC address which is learned and manually added. There is a search function which can be used to display the information about the entry in the table.



Address Aging Time

Description	Factory default
Address Aging Timeout (seconds)	
Enter the period in seconds. If a learned MAC address has not been updated during the address aging time, then it will be removed from the address table automatically. Enter a period in the range of 10 to 1000000 seconds.	300

MAC Address Table

Item	Description
Auto-refresh	Checkmark the box,the MAC address Table will??，幾秒會更新一次??
VLAN ID	The VLAN ID that is associated with the MAC address.
MAC Address	The dynamically learned or manually added MAC address for which the switch has forwarded or filtered information, or both.
Port	This field displays the interface which was learned or added manually. It also means the interface through which the MAC address can be reached.
Status	The status of this entry: • **Invalid:** The MAC address is invalid. Normally, invalid MAC addresses are deleted, so this is an error condition. • **Self:** The MAC address is the address of a physical interface of the switch. • **Learned:** The MAC address was learned through incoming traffic and is being used. • **Static:** The MAC address was manually added and can not be relearned. • **Other:** The MAC address does not fall into one of the other categories.

3.12.2 SFP DDM (Only for SFP Module)

You can monitor the status of each SFP (small form-factor pluggable) port on this page.

SFP Status

Port Status

Port	Ethernet Compliance Code	SFP Vendor	Wave Length	Distance
0/7	unknown	unknown	unknown	unknown
0/8	unknown	unknown	unknown	unknown

SFP DDM

Port	Status	Temperature		Voltage		Bias		Tx Power		Rx Power	
		Current	Range	Current	Range	Current	Range	Current	Range	Current	Range
0/7	Not Present	unknown	unknown	unknown	unknown	unknown	unknown	unknown	unknown	unknown	unknown
0/8	Not Present	unknown	unknown	unknown	unknown	unknown	unknown	unknown	unknown	unknown	unknown

Refresh Eject

Note:
Before you use the SFP DDM function, please make sure the SFP module you used are support SFP DDM function.
DDM function and SFP modules tramsissiom are fully compatible with Delta managed switches ONLY. If users are intending to use SFP modules of 3rd-party vendors, please do a proper evaluation of installation firstly.

3.12.3 System CPU Status

You can monitor the CPU status of the Delta switch on this page.

System CPU Status

CPU Memory Status

Total System Memory	63428 KBytes
Available Memory	10984 KBytes

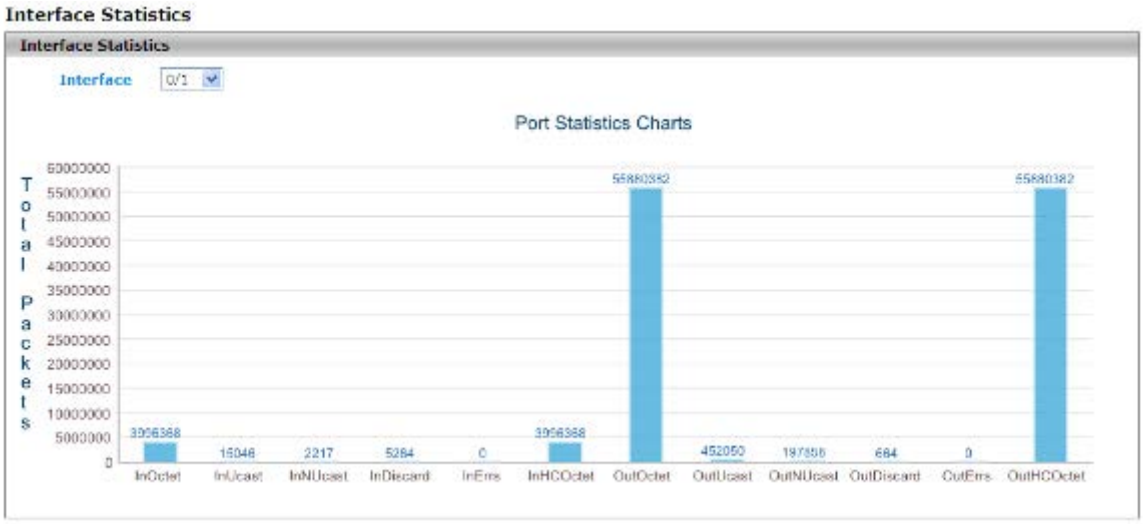
CPU Utilization

```
Memory Utilization Report
status      bytes
------ ----------
  free    11247616
 alloc    53702656

CPU Utilization:

 PID     Name                 5 Sec     1 Min     5 Min
-------------------------------------------------------
   1     init                 0.0 %     0.0 %     0.0 %
   2     kthreadd             0.0 %     0.0 %     0.0 %
   3     ksoftirqd/0          0.0 %     0.0 %     0.0 %
   4     watchdog/0           0.0 %     0.0 %     0.0 %
   5     events/0             0.0 %     0.0 %     0.0 %
   6     khelper              0.0 %     0.0 %     0.0 %
  16     kblockd/0            0.0 %     0.0 %     0.0 %
  32     pdflush              0.0 %     0.0 %     0.0 %
  33     pdflush              0.0 %     0.0 %     0.0 %
```

Refresh

3.12.4 Interface Statistics

You can monitor the statistics of each interface of the Delta switch on this page. The data will be refreshed every second.



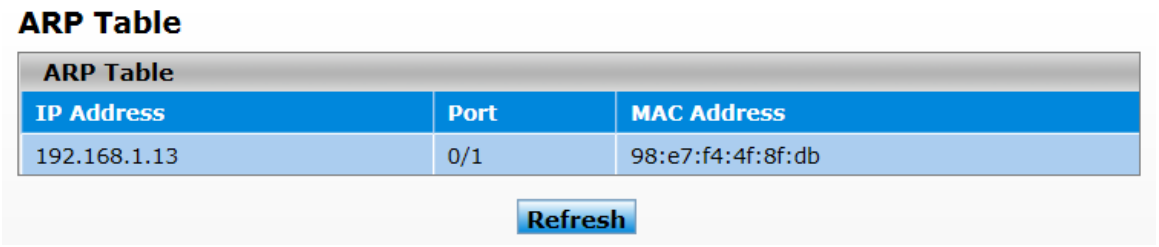
Note:
Make sure that the port you want to monitor is connected to another device.

3.12.5 ARP Configure

ARP protocol is a process to mapping a MAC address to an IP address, and there are two types of ARP entries-static and dynamic. It will store these mapping entries to a database which called ARP cache. The Delta managed switches provide dynamic and manual ARP configuration

3.12.5.1 Basic

The ARP table includes dynamic ARP entries and static ARP entries.



ARP Table

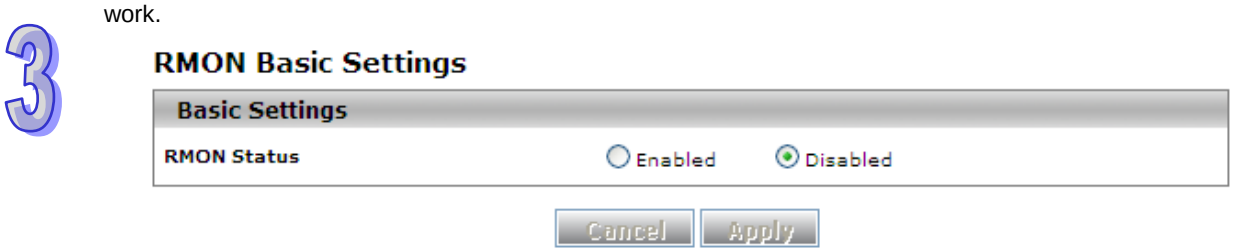
Item	Description
IP Address	The VLAN ID that is associated with the MAC address
Port	This field displays the interface which was learned or added manually. It also means the interface through which the MAC address can be reached.
MAC Address	The status of this entry: • **Invalid:** The MAC address is invalid. Normally, invalid MAC addresses are deleted, so this is an error condition. • **Self:** The MAC address is the address of a physical interface of the switch. • **Learned:** The MAC address was learned through incoming traffic and is being used. • **Static:** The MAC address was manually added and can not be relearned. • **Other:** The MAC address does not fall into one of the other categories.

3.12.6 RMON

Remote network monitoring (RMON) mainly provides the statistics and the alarm functions for the remote monitoring and the management of the network management devices on the managed device. It is the functionality expansion for the simple network management protocol (SNMP), particularly useful for monitoring and managing a network. RMON specifically defines that any network monitoring system must be able to provide information (defined in RFC2819) about the MIB which is the base of seamless multi-vendor interoperability between the SNMP management station and the monitoring agent.

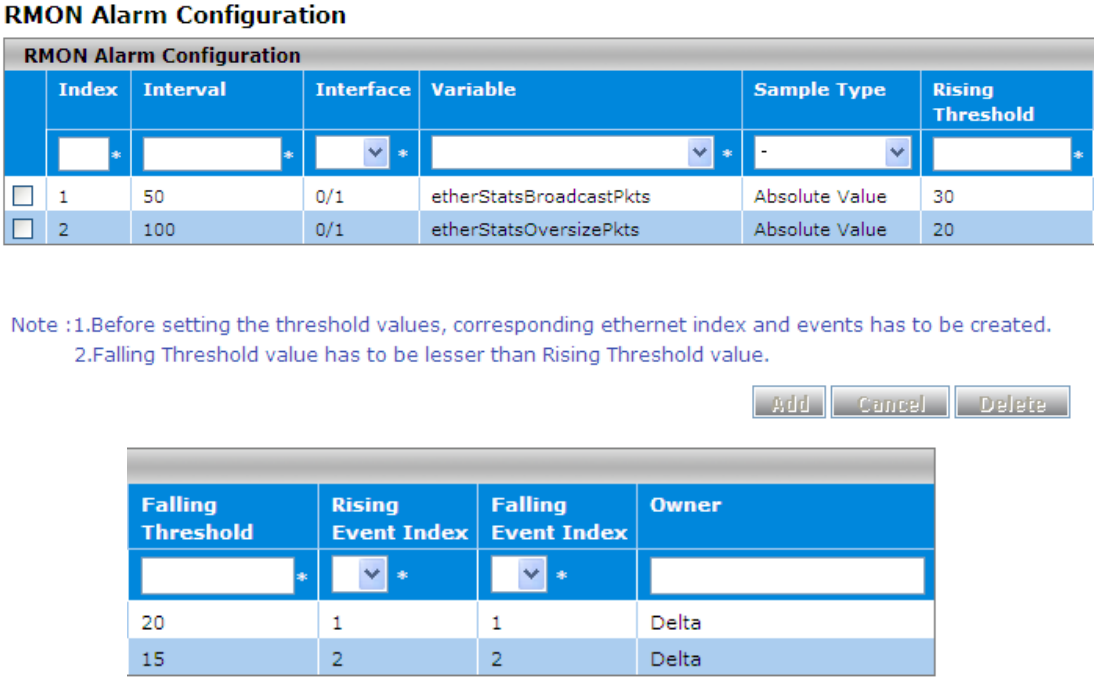
3.12.6.1 Basic Settings

The default setting of RMON is disabled. If RMON Status is disabled, the functions in RMON group will not work.



3.12.6.2 Alarms

RMON Alarm Configuration allows you to specify the threshold and generate the alarm. When the alarm occurs, an event can be generated. Before you configure alarms, you need to specify logs and the SNMP traps that can be generated when an alarm occurs by configuring entries on the **RMON Event Configuration** page.

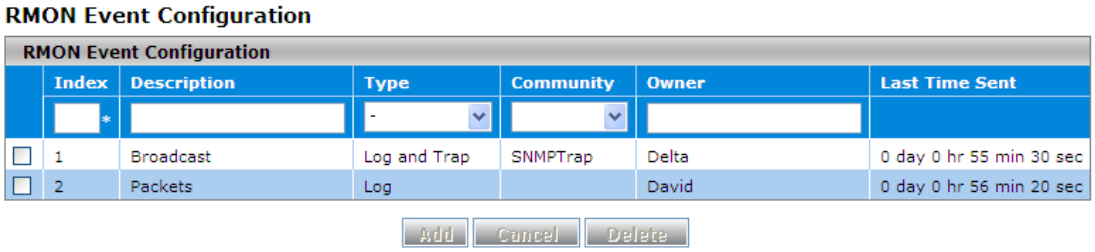


RMON Alarm Configuration

Description	Factory default
Index	
Enter an index that uniquely identifies the entry in the RMON Alarm Configuration table. Enter a number between 1 and 65535.	None
Interval	
Specify the period in seconds over which the data is sampled and compared with the rising and falling thresholds. Enter a number between 1 and 65535 seconds.	None
Interface	
Specify the interface number.	None
Variable	
Specify the SNMP event that you want to sample.	None
Sample Type	
Specify the sample type for the alarm, which defines how the variable is sampled, and how the value is calculated and compared with the thresholds that you configure. Make a selection from the drop-down list: • **Absolute Value:** The value of the variable is compared directly with the thresholds at the end of the sampling interval. • **Delta Value:** The value of the variable that was obtained at the last sample is subtracted from the current value, and the difference is compared with the thresholds.	None
Rising Threshold	
Specify the rising threshold for the sampled statistic. If the configured threshold value is reached, an alarm is raised. If the current sampled value is greater than or equal to this threshold, and the value at the last sampling interval was less than this threshold, a single event is generated. Enter a value between 0 and 2147483647. **Note:** The rising threshold value needs to be greater than the falling threshold value.	None
Falling Threshold	
Specify the falling threshold for the sampled statistic. If the configured threshold value is reached, an alarm is raised. If the current sampled value is less than or equal to this threshold, and the value at the last sampling interval was greater than this threshold, a single event is generated. Enter a value between 0 and 2147483647. **Note:** The falling threshold value needs to be less than the rising threshold value.	None
Rising Event Index	
Specify the index of the event that needs to be raised when a rising threshold is crossed. T he value is between 1 and 65535. **Note:** The drop-down list is associated with the **RMON Event Configuration table**. If there is no corresponding entry in the **RMON Event Configuration table**, no association can exist.	None
Falling Event Index	
Specify the index of the event that needs to be raised when a falling threshold is crossed. **Note:** The drop-down list is associated with the **RMON Event Configuration table**. If there is no corresponding entry in the **RMON Event Configuration table**, no association can exist.	None
Owner	
Specify the owner of the entry by entering a name.	None

3.12.6.3 Events

You can specify events that create log entries, the SNMP traps, or both. And assign these configurations to the alarms on the **RMON Alarm Configuration** page.

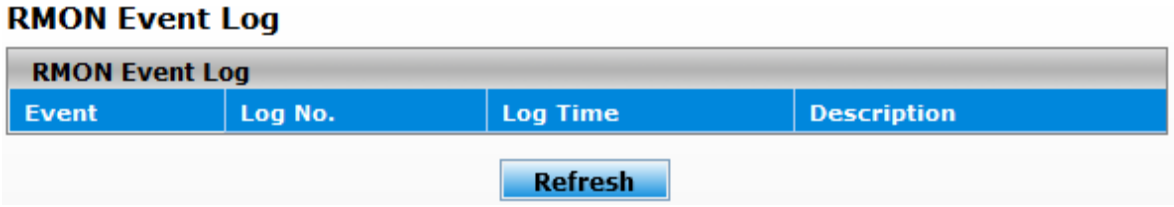


RMON Event Configuration

Description	Factory default
Index	
Enter an index that uniquely identifies the entry in the RMON Alarm Configuration table. Enter a number between 1 and 65535.	None
Description	
Enter a brief description of the event. You can enter up to 127 characters.	None
Type	
Specify the type for this event: • **None:** No entry is made in the RMON Event Log table and no trap is sent. The community field is disabled. • **Log:** An entry is made in the RMON Event Log table. The community field is disabled. • **SNMP Trap:** An SNMP trap is sent to one or more management stations. • **Log and Trap:** An entry is made in the RMON Event Log table and an SNMP trap is sent to one or more management stations.	None
Community	
If the Type setting is SNMP Trap or Log and Trap, enter an existing community name.	None
Owner	
Specify the owner of the entry by entering a name.	None
Last Time Sent	
Specify the last time the entry created an event.	None

3.12.6.4 Event Log

The events that have been triggered are displayed on this page.

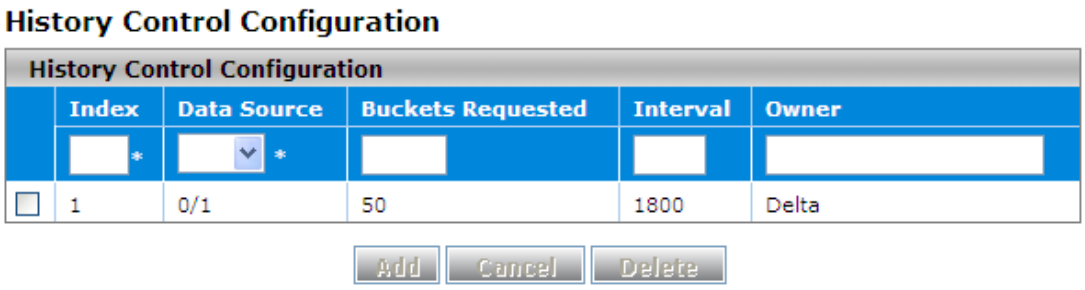


RMON Event Log

Item	Description
Event	The index that corresponds to the index value of the entry in the RMON Event Configuration table
Log No.	The entry in the RMON Event Log table
Log Time	The time when the entry was created
Description	The description that corresponds to the description of the index value of the entry in the RMON Event Configuration table

3.12.6.5 History

You can specify the polling period, the buckets (the number of samplings or how many times the polling occurs) and the source interface for the historical statistical data sampling for the individual interfaces on this page.



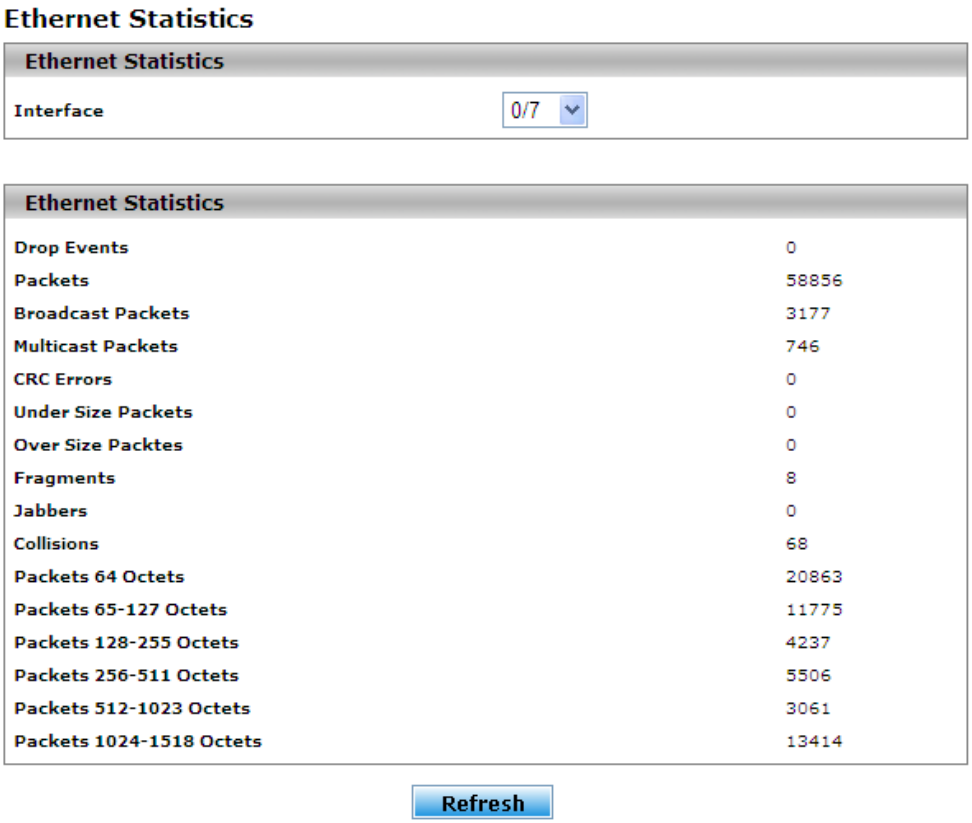
History Control Configuration

Description	Factory default
Index	
Enter an index that uniquely identifies the entry in the History Control Configuration table. Enter a number between 1 and 65535.	None
Data Source	
Specify a source interface.	None
Buckets Requested	
Specify the number of buckets for collecting the RMON statistics. Enter the requested number of discrete time intervals over which data is to be collected and saved. Enter a number between 1 and 50.	50
Interval	
Specify the period in seconds between two successive pollings to collect the statistics. Enter a number between 1 to 3600 seconds.	1800
Owner	
Specify the owner of the entry by entering a name.	None

3.12.6.6 RMON Ethernet Statistics

The cumulative RMON Ethernet statistics information is displayed on this page.

Note:
The counters on the **RMON Ethernet Statistics** page provide cumulative statistical information from multiple pollings.
The counters on the RMON Ethernet History Statistics page provide statistical information from individual pollings.



Ethernet Statistics

Item	Description
Interface	Specify one interface for Ethernet Statistics.
Drop Events	The cumulative number of events in which packets were dropped on the interface because of lack of resources. This number does not specify the number of packets that were dropped but the number of times the packets were dropped.
Packets	The cumulative number of packets received on the interface.
Broadcast Packets	The cumulative number of broadcast packets received on the interface.
Multicast Packets	The cumulative number of multicast packets received on the interface.
CRC Errors	The cumulative number of packets which are received on the interface, have a length (excluding the framing bits, but including the FCS octets) between 64 and 1518 octets, and have either a bad frame check sequence (FCS) with an integral number of octets (FCS error) or a bad FCS with a nonintegral number of octets (alignment error).
Under Size Packets	The cumulative number of packets which are received on the interface, less than 64 octets in length (excluding the framing bits, but including the FCS octets), and well formed.
Over Size Packets	The cumulative number of packets which are received on the interface, more than 1518 octets in length (excluding the framing bits, but including the FCS octets), and well formed.
Fragments	The cumulative number of packets which are received on the interface, are less than 64 octets in length (excluding the framing bits, but including the FCS octets), and have either a bad frame check sequence (FCS) with an integral number of octets (FCS error) or a bad FCS with a nonintegral number of octets (alignment error).
Jabbers	The cumulative number of packets which are received on the interface, are longer than 1518 octets in length (excluding the framing bits, but including the FCS octets), and have either a bad frame check sequence (FCS) with an

Item	Description
	integral number of octets (FCS error) or a bad FCS with a non integral number of octets (alignment error).
Collisions	The best estimate of the cumulative number of collisions on the interface
Packets 64 Octets	The cumulative number of packets (including bad packets) which are received on the interface, and 64 octets in length (excluding the framing bits, but including the FCS octets).
Packets 65-127 Octets	The cumulative number of packets (including bad packets) which are received on the interface, and between 65 and 127 octets in length (excluding the framing bits, but including the FCS octets).
Packets 128-255 Octets	The cumulative number of packets (including bad packets) which are received on the interface, and between 128 and 255 octets in length (excluding the framing bits, but including the FCS octets).
Packets 256-511 Octets	The cumulative number of packets (including bad packets) which are received on the interface, and between 256 and 511 octets in length (excluding the framing bits, but including the FCS octets).
Packets 512-1023 Octets	The cumulative number of packets (including bad packets) which are received on the interface, and between 512 and 1023 octets in length (excluding the framing bits, but including the FCS octets).
Packets 1024-1518 Octets	The cumulative number of packets (including bad packets) which are received on the interface, and between 1024 and 1518 octets in length (excluding the framing bits, but including the FCS octets).

3.12.6.7 Ethernet History Statistics

The historical data for the interface is collected, and the statistics information for the interface is displayed on **RMON Ethernet History Statistics** page.

Note:
The counters on the RMON Ethernet Statistics page provide cumulative statistical information from multiple pollings.
The counters on the **RMON Ethernet History Statistics** page provide statistical information from individual pollings.

RMON Ethernet History Statistics

Ethernet History Statistics

Index	Sample Index	Interval Start	Drop Events	Octets	Packets	Broadcast Packets	Multicast Packets
1	0	Jan 1 00:00:00 1970	0	0	0	0	0
2	1	Jan 1 01:27:48 1970	0	8204300	17753	835	221
2	2	Jan 1 01:28:48 1970	0	4161973	11636	861	220
2	3	Jan 1 01:29:49 1970	0	7998440	14127	767	145

Refresh

CRC Errors	Under Size Packets	Over Size Packtes	Fragments	Jabbers	Collisions	Utilization
0	0	0	0	0	0	0
0	0	0	7	0	23	11
0	0	0	1	0	1	5
0	0	0	0	0	34	11

RMON Ethernet History Statistics

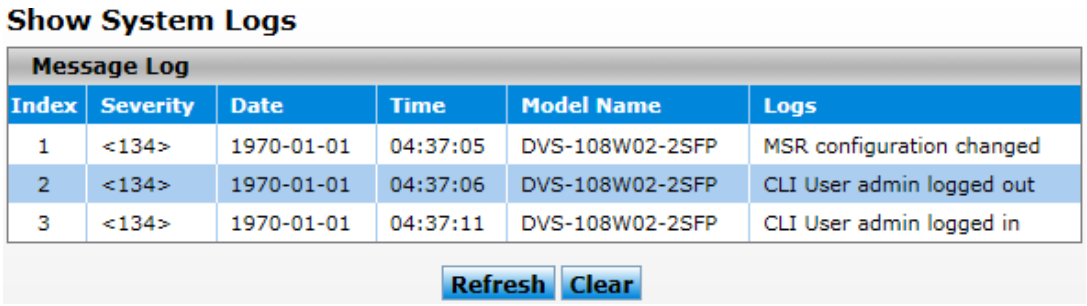
Item	Description
Index	The index that uniquely identifies the entry in the History Control Configuration table.
Sample Index	An index that uniquely identifies the particular polling sample that this entry represents among all polling samples associated with the same entry in the History Control Configuration table. This index starts at 1 and increases by one as each new polling sample is taken.
Interval Start	The time when the polling (sampling) interval started.
Drop Events	The number of events during the sampling interval in which packets were dropped on the interface because of the lack of resources. This number does not specify the number of packets that were dropped but the number of times the packets were dropped.
Octets	The number of data octets (including those in bad packets) received on the interface (excluding the framing bits, but including the FCS octets) during the sampling interval.
Packets	The number of packets received on the interface (including the bad packets, the broadcast packets, and the multicast packets) during the sampling interval.
Broadcast Packets	The number of broadcast packets received on the interface during the sampling interval. These packets were directed to the broadcast addresses.
Multicast Packets	The number of multicast packets received on the interface during the sampling interval. These packets were directed to the multicast addresses. (This number does not include the packets addressed to a broadcast addresses.)
CRC Errors	The number of packets which are received on the interface during the sampling interval, have a length (excluding the framing bits, but including the FCS octets) between 64 and 1518 octets, and have either a bad frame check sequence (FCS) with an integral number of octets (FCS error) or a bad FCS with a non integral number of octets (alignment error).
Under Size Packets	The number of packets which are received on the interface during the sampling interval, less than 64 octets in length (excluding the framing bits, but including the FCS octets), and were well formed.
Over Size Packets	The number of packets which are received on the interface during the sampling interval, more than 1518 octets in length (excluding the framing bits, but including the FCS octets) and that were well formed.
Fragments	The number of packets which are received on the interface during the sampling interval, are less than 64 octets in length (excluding the framing bits, but including the FCS octets), and have either a bad frame check sequence (FCS) with an integral number of octets (FCS error) or a bad FCS with a non integral number of octets (alignment error).
Jabbers	The number of packets which are received on the interface during the sampling interval, are longer than 1518 octets in length (excluding the framing bits, but including the FCS octets) , and have either a bad frame check sequence (FCS) with an integral number of octets (FCS error) or a bad FCS with a non integral number of octets (alignment error).
Collisions	The best estimate of the number of collisions on the interface during the sampling interval.
Utilization	The best estimate of the mean physical layer network utilization on the interface during the sampling interval, in hundredths of a percent.

3.12.7 SYSLOG

The SYSLOG function allows you to monitor the switch. When faults, errors, configuration changes or specified events happen, this function can generate messages, store the messages locally or forward the messages to one syslog server or more syslog servers. You can choose the severity level to filter the message according to your requirement.

3.12.7.1 Show Logs

The numbers of messages which can be shown on this page depend on the setting of the severity on the Logs Configuration page. The logs are cleared after the switch is rebooted. To save the logs after the switch is rebooted, you have to send them to a syslog server or use the email function.

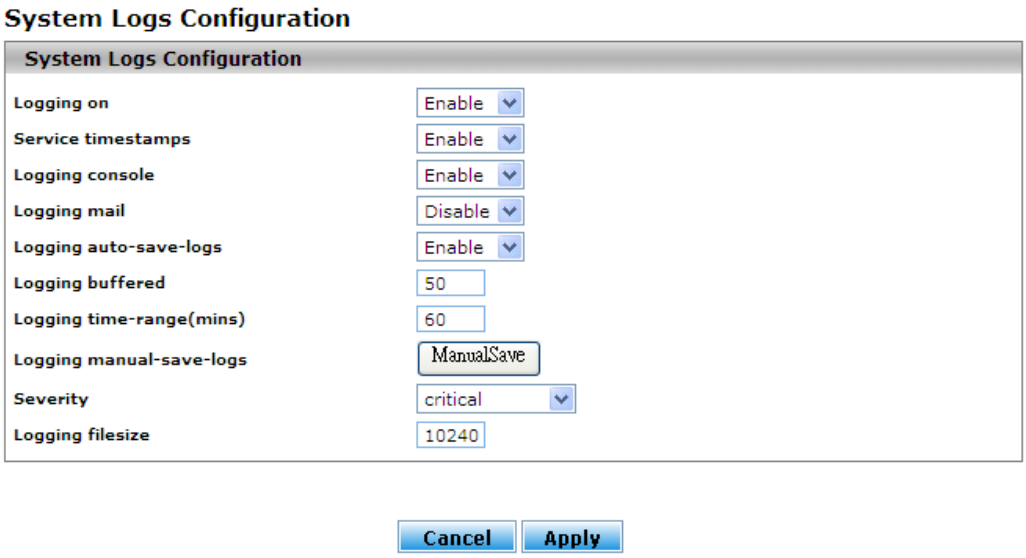


The log message format is described below:
<134>1970-01-01 03:26:33 DVS-108W02-2SFP MSR configuration changed

Log message component	Description
<134>	The number contained in the angle brackets represents the message priority, which is derived from the following values: Priority = facility value + severity level. In the example, the facility value is local0 (128). The severity value is notification (5). For more information about the severity of a log message, please see ***Logs Configuration***.
1970-01-01 03:26:33	The message was generated on 1970-01-01 00:02:50
DVS-108W02-2SFP	The device name
MSR	The module that generated the message
configuration changed	The major description of the message: The configuration has been changed.

3.12.7.2 Logs Configuration

You can enable, disable and configure other system log settings on this page.



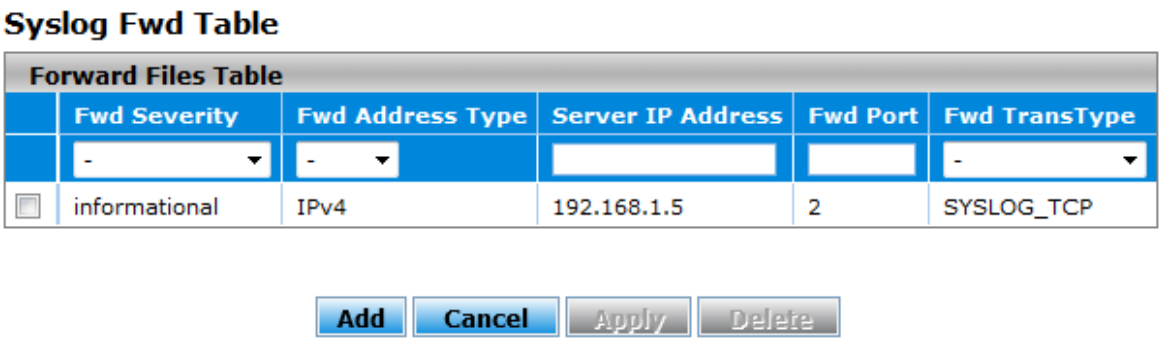
System Logs Configuration

Description	Factory default
Logging on	
Specify whether the logging is enabled or disabled: • **Enable:** The logging is enabled. • **Disable**: The logging is disabled. Log messages are not displayed on the Show System Logs page and can not be saved in a log file or a syslog server, and the logging over the console port is disabled.	Enable
Service timestamps	
Specify whether or not a time stamp is added to log messages: • **Enable:** A time stamp is added. • **Disable:** A time stamp is not added.	Enable
Logging console	
Specify whether the logging over the console port is enabled or disabled: • **Enable:** The logging over the console port is enabled. • **Disable:** The logging over the console port is disabled.	Enable
Logging mail	
Specify whether log messages can be sent to a specified email address: • **Enable:** The sending of log messages to a specified email is enabled. • **Disable:** The sending of log messages to a specified email is disabled.	Disable
Logging auto-save-logs	
• Specify whether log messages can be saved in a flash memory automatically: • **Enable:** Log messages can be saved in a flash memory automatically. The saving time depends on the Logging time-range setting. • **Disable:** Log messages can not be saved in a flash memory automatically.	Enable
Logging buffered	
Specify the number of log messages that can be displayed on the Show System Logs page. Enter a number in the range of 1 to 200. The default setting is 50 log messages.	50
Logging time-range (min)	
Specify the time-range to save the log automatically. It only works when the Logging auto-save-logs function is enabled. Enter a value in the range of 60 to 43200. The default value is 60.	60
Logging manual-save-logs	
Click the button to save logs in a flash memory manually.	None

Description	Factory default
Severity	
Specify the level of the severity that determines which events are logged. A log records the messages equal to or above a configured severity threshold. For example, if you select an error, the logged messages include error (3), critical (2), alert (1), and emergency (0). The default level of the severity is critical (2). Make a selection from the drop-down list: • **emergency:** The highest warning level (level 0). An emergency message is saved if the switch is down or not functioning correctly. • **alert:** The second-highest warning level (level 1). An alert message is saved if there is a serious switch malfunction, for example, an important switch function goes down. Action needs to be taken immediately. • **critical:** The third-highest warning level (level 2). A critical message is saved if a critical switch malfunction occurs, for example, two interfaces stop functioning while the rest of the interfaces remain functional. • **error:** The level that indicates that a device error has occurred (level 3), such as an interface going offline • **warning:** The lowest level of a device warning (level 4). • **notice:** Normal but significant conditions (level 5). Provides the network administrators with the switch information. • **Informational:** Provides the switch information (level 6). • **debug:** Provides the detailed information about the switch (level 7). This level generates a lot of messages.	critical
Logging filesize	
Specify the size of the system file in which the log files are saved. Enter a file size between 1024 and 102400 bytes. **Note:** The debug log file is not controlled by the size of the system file. The debug log file is a temporary file that is not stored in the flash memory. The file can always store the most recent 100 debug log messages, and each debug log message is less than 80 bytes in length.	10240

3.12.7.3 Syslog Fwd Table

You can add the syslog server IP address and configure the forward log severity on this page.

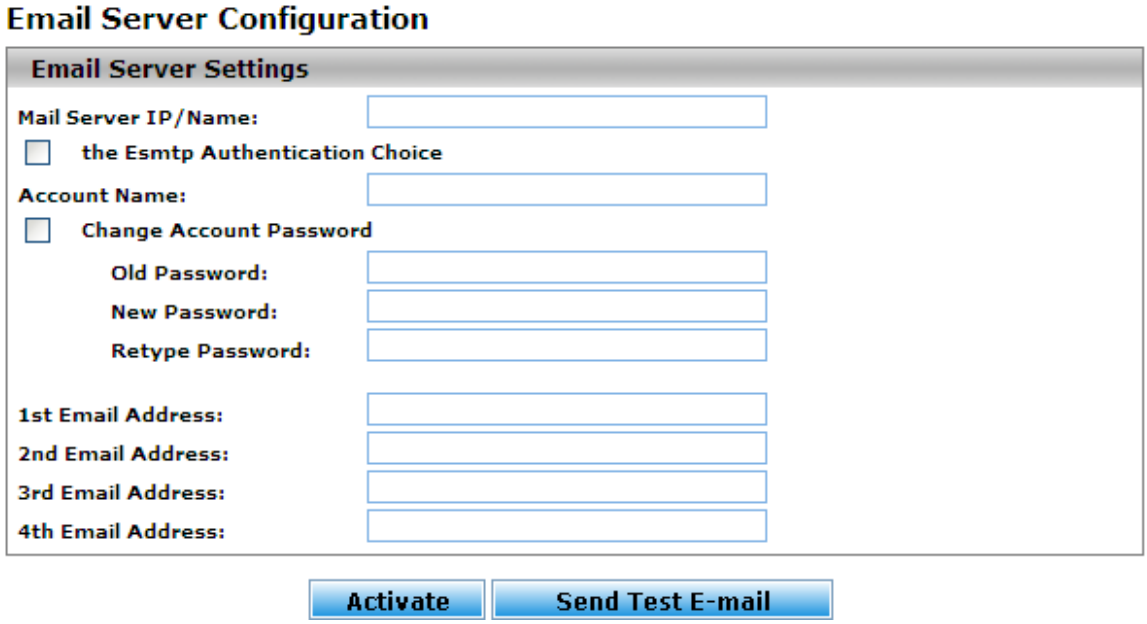


Syslog Fwd Table

Description	Factory default
Fwd Severity	
From the drop-down list, select a level of the severity that determines which events are sent to the syslog server. The log records the messages equal to the configured severity threshold. For example, if you select an error, the logged messages include error (3) messages only.	None
Fwd Address Type	
Specify a type of server address and enter the address or the host name in the Server IP Address field: • IPv4: The syslog server has an IPv4 address. • IPv6: The syslog server has an IPv6 address. • DNS: The syslog server has a DNS host name.	None
Server IP Address	
Enter the IP address or the host name of the syslog server. **Note:** For an IPv6 address, enter the address in the xxxx:xxxx:xxxx:xxxxx:xxxx:xxxx:xxxx:xxxx format.	None
Fwd Port	
Enter the port number to which syslog messages are sent on the syslog server. Enter a number between 0 and 65535. Enter 0 to prevent the syslog messages from being sent.	514
Fwd TransType	
Specify whether log messages are sent as UDP or TCP messages: • **SYSLOG_UDP:** Log messages are sent as UDP messages. • **SYSLOG_TCP:** Log messages are sent as TCP messages.	None

3.12.7.4 Syslog Email Configuration

Email Server Configuration allows you to monitor the switch when you can not stay in front of the computer. For example, when the alarm event happens, you can use a smart phone to get an alarm event email anywhere. And then you can contact a related maintainer or engineer to check the device and solve the problem.



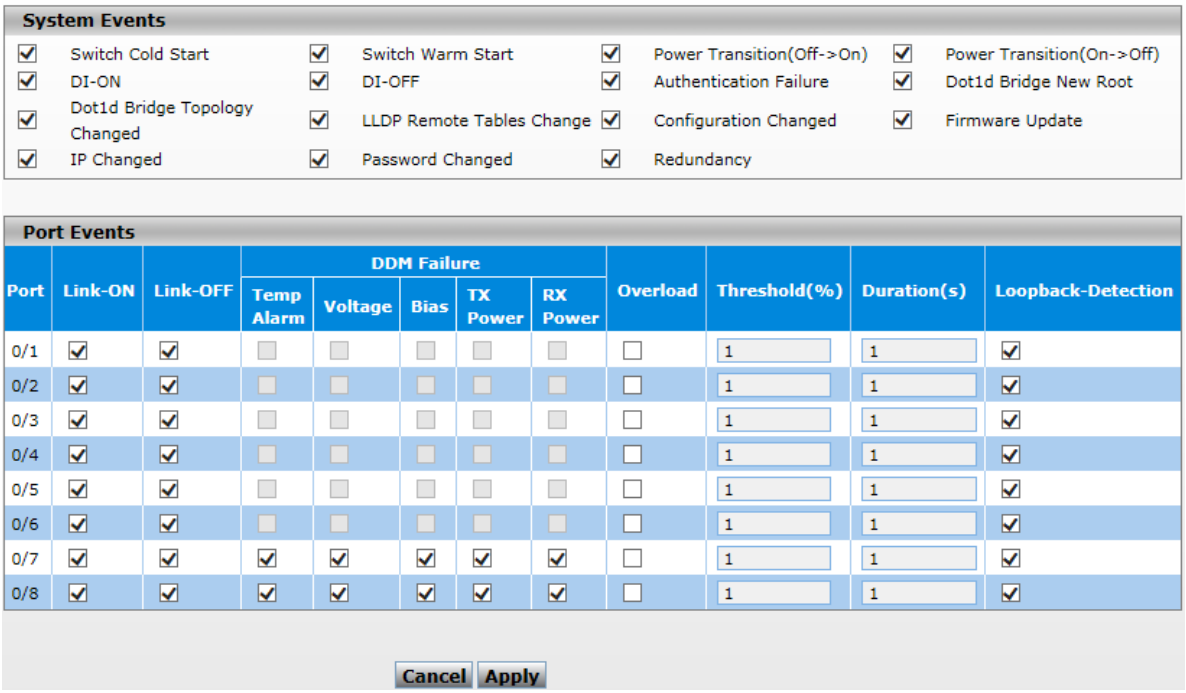
Email Server Configuration

Description	Factory default
Mail Server IP / Name	
Enter the IP address of the mail server.	None
The Esmtp Authentication Choice	
Specify whether the mail server needs the authentication. If the box is selected, please enter the account name of the email.	None
Change Account Password	
Specify whether you want to change the account password. If the box is selected, please enter the old password and enter the new password twice in New Password and Retype Password.	None
Email Address	
Specify the email address for the email alarm. You can specify 1 to 4 email addresses.	None

3.12.7.5 Syslog Email Alarm Table

The Email Alarm Events Settings page allows you to get an email message when the event you configured happened.

Email Alarm Events Settings



System Events

Description	Factory default
Switch Cold Start	
Specify whether to send an alarm email when switch cold starts.	Checked
Switch Warm Start	
Specify whether to send an alarm email when switch warm starts.	Checked
Power Transition (Off->On)	
Specify whether to send an alarm email when there is a transition in power from Off to On.	Checked
Power Transition (On->Off)	
Specify whether to send an alarm email when there is a transition in power from On to Off.	Checked

Description	Factory default
DI-ON	
Specify whether to send an alarm email when DI is On.	Checked
DI-OFF	
Specify whether to send an alarm email when DI is Off.	Checked
Authentication Failure	
Specify whether to send an alarm email when there is authentication failure.	Checked
Dot1d Bridge New Root	
Specify whether to send an alarm email when a new node is added to the 802.1d network.	Checked
Dot1d Bridge Topology Changed	
Specify whether to send an alarm email when the 802.1d bridge topology is changed.	Checked
LLDP Remote Tables Change	
Specify whether to send an alarm email when the LLDP remote table is changed.	Checked
Configuration-Changed	
Specify whether to send an alarm email when the configuration is changed.	Checked
Firmware Update	
Specify whether to send an alarm email when the firmware has been updated.	Checked
IP Changed	
Specify whether to send alarm email when the IP address has changed.	Checked
Password Changed	
Specify whether to send alarm email when the password has changed.	Checked
Redundancy	
Specify whether to send alarm email when the redundancy has changed.	Checked

Port Events

Description	Factory default
Port	
This field displays the interface number.	*interface number*
Link-ON	
Specify whether to send an alarm email when the Link is ON.	Checked
Link-OFF	
Specify whether to send an alarm email when the Link is OFF.	Checked
DDM Failure	
Specify whether to send an alarm email when the DDM failure event is detected.	Checked
Overload	
Specify whether to send an alarm email when the traffic of the port is overloaded. If the box is selected, you can configure the Threshold (%) and Duration (s) fields.	Unchecked
Loopback-Detection	
Specify whether to send an alarm email when the Loopback-Detection event is detected.	Checked

3.13 Diagnostic Settings

The Delta switch provides LLDP function, Port mirror function, and Cable Diagnostics function so that administrator can use these functions to diagnose network or settings.

> **IMPORTANT:**
> **Make sure that you save the configuration in the Save Configuration page after you have applied the configuration changes. (Save Config→Save Configuration) If you do not save the configuration, then the configuration will be cleared after the switch is rebooted.**

3.13.1 LLDP

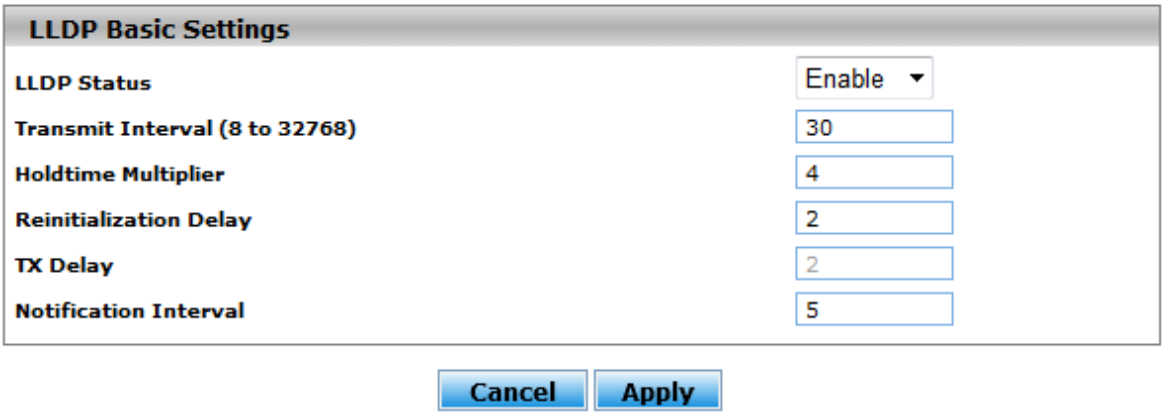
LLDP (Link Layer Discover Protocol) provides a method for switches, routers and access points to advertise their identification, configuration and capabilities to the neighboring devices that store the data in a MIB, and to learn information about the neighboring devices.
LLDP-MED (Link Layer Discovery Protocol for Media Endpoint Devices) is an extension of LLDP in that it operates between endpoint devices such as IP phones or switches.
LLDP-Media Endpoint Discovery (LLDP-MED) is an enhancement of LLDP with the following features:

- **Auto Discovery:** Autodiscovery of LAN policies (such as VLAN, Layer 2 priority, and DiffServ settings) and capability to enable a plug and play networking
- **Device Location:** Device location discovery for the creation of location databases
- **Power Management:** Extended and automated power management of Power over Ethernet (PoE) endpoints
- **Inventory Management:** Inventory management, which lets network administrators track network devices and determine their characteristics such as the manufacturer, the software and hardware versions, and the serial and asset numbers

3.13.1.1 LLDP Basic Settings

The default of the LLDP status is enabling. If you want to configure other settings, please refer to the following table.

LLDP Basic Settings

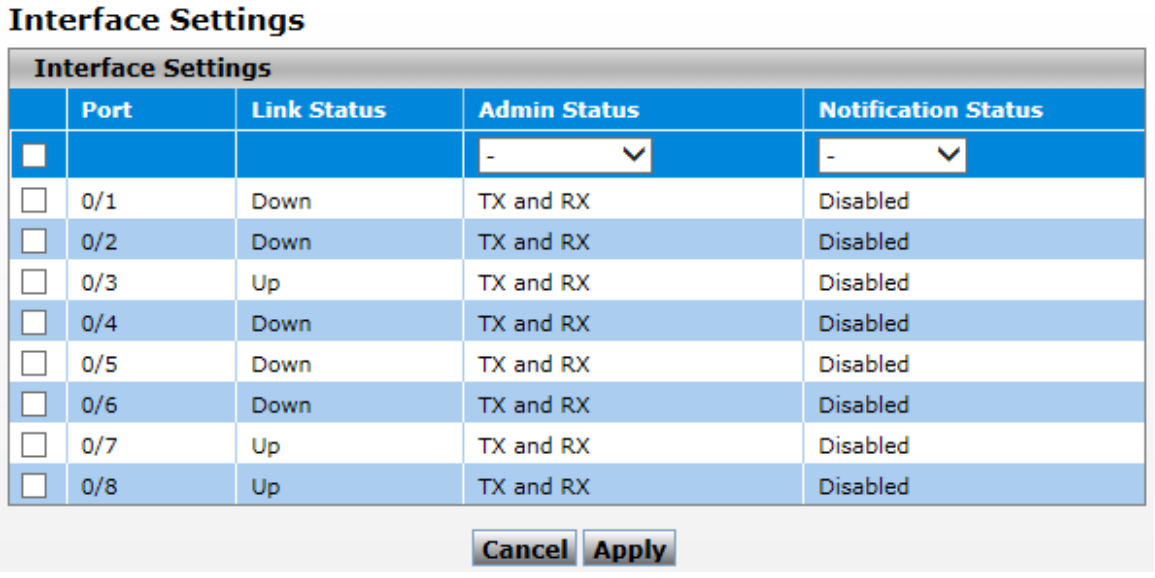


LLDP Basic Settings

Description	Factory default
LLDP Status	
Specify the status of LLDP on the switch: • **Enable:** LLDP is enabled. You can configure LLDP, and the settings take effect after you have applied them. • **Disable:** LLDP is disabled. You can still configure LLDP, but the settings do not take effect after you have applied them.	Enable
Transmit Interval (8 to 32768)	
Enter the interval in seconds to transmit the LLDP frames. Enter a number in the range of 8 to 32768 seconds.	30
Holdtime Multiplier	
Enter the hold time multiplier in seconds. The hold time multiplier multiplies the transmit interval to define the Time to Live (TTL) period. Enter a number in the range of 2 to 10 seconds.	4
Reinitialization Delay	
Enter the delay in seconds before reinitialization. Enter a number in the range of 1 to 10 seconds. A longer time prevents frequent reinitializations.	2
TX Delay	2
It is used to delay the tx_relay time and the value is fixed at 2 seconds.	
Notification Interval	
Enter the interval in seconds for the transmission of notifications. Enter a number in the range of 5 to 3600 seconds.	5

3.13.1.2 LLDP Interface Configuration

You can configure the LLDP settings for an individual interface on this page.



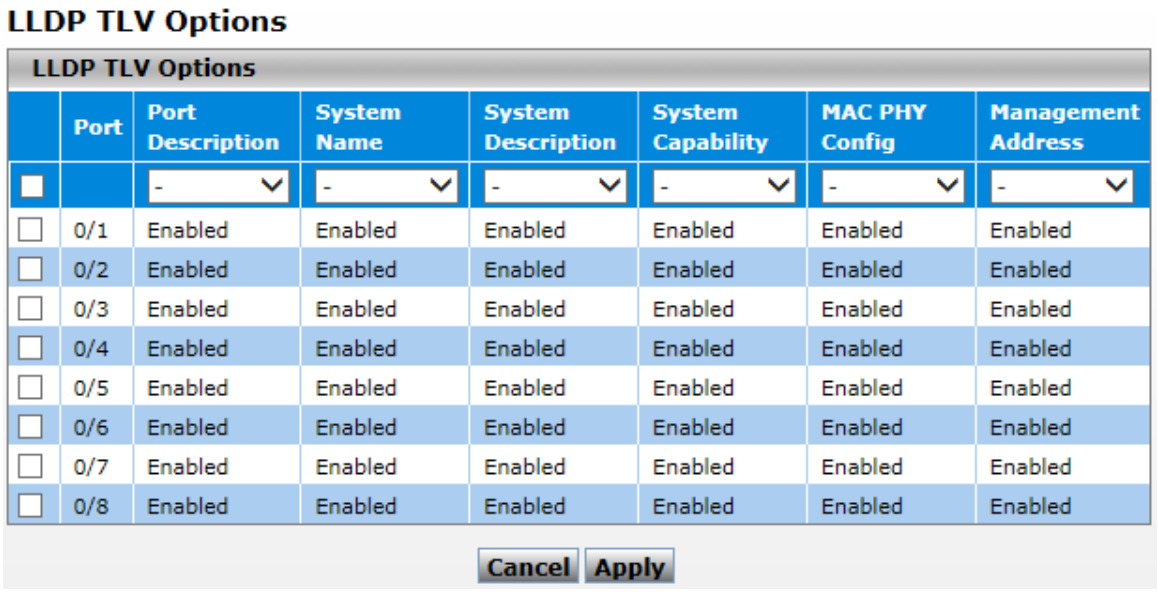
Interface Settings

Description	Factory default
Port	
This field displays the interface number.	*interface number*
Link Status	
This field displays the status of the interface link.	Up or Down
Admin Status	
Specify the status and the direction of the interface: • **TX:** The interface processes outgoing traffic only. • **RX:** The interface processes incoming traffic only.	TX and RX

Description	Factory default
• **TX and RX:** The interface processes both incoming and outgoing traffic. • **Disabled:** The interface is disabled.	
Notification Status	
Specify the notification status: • **Enabled:** Notifications are sent. • **Disabled:** Notifications are not sent.	Disabled

3.13.1.3 LLDP TLV Options

You can configure the LLDP type-length value (TLV) settings for each interface on this page.

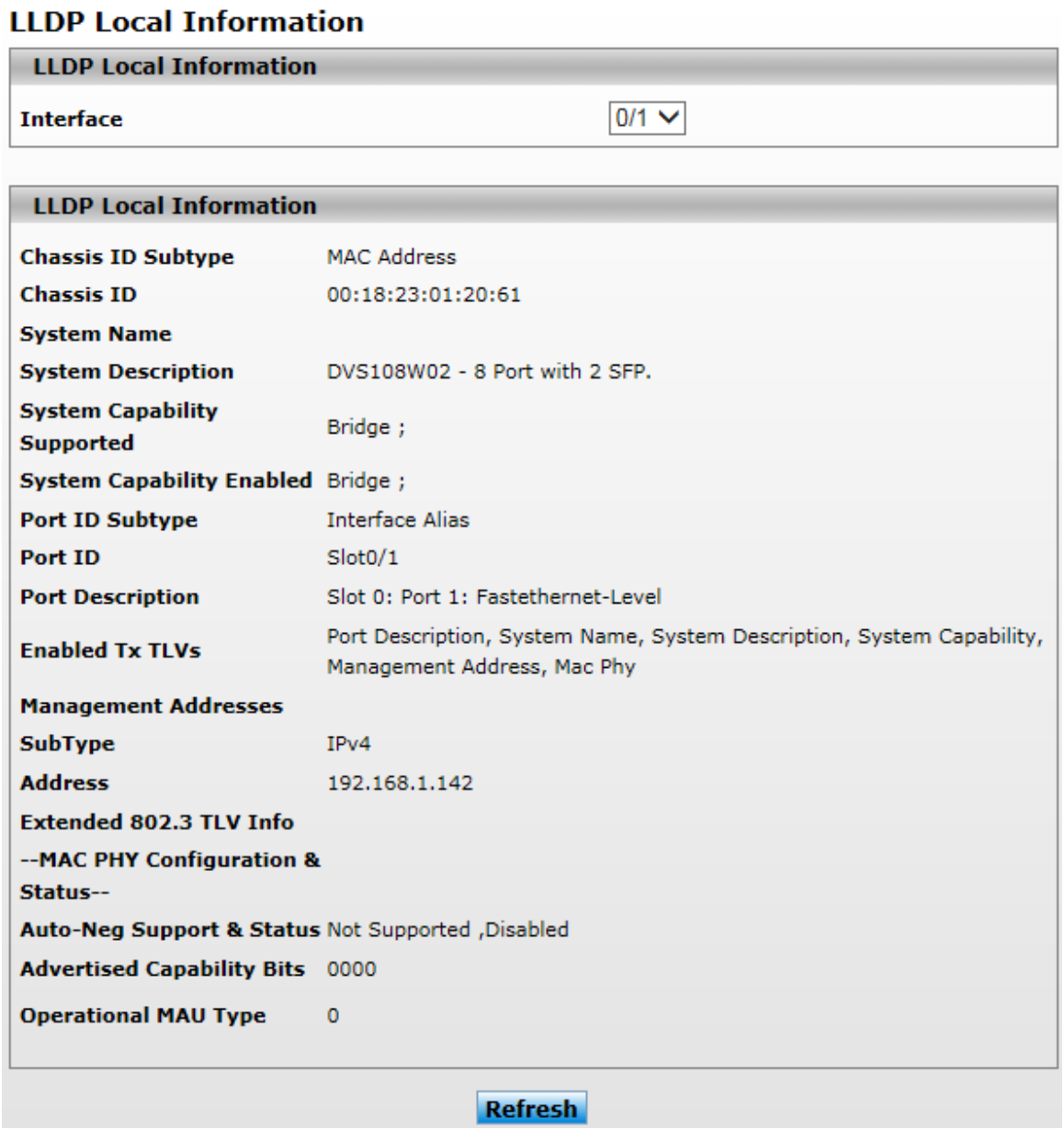


LLDP TLV Option

Item	Description
Port	Specify the interface number.
Port Description System Name System Description System Capability MAC PHY Config Management Address	Specify whether to send the options in the LLDP frames. • **Enable:** The information is transmitted. This is the default setting. • **Disable:** The information is not transmitted.

3.13.1.4 LLDP Local Information

You can view the LLDP local information about an individual interface on this page.



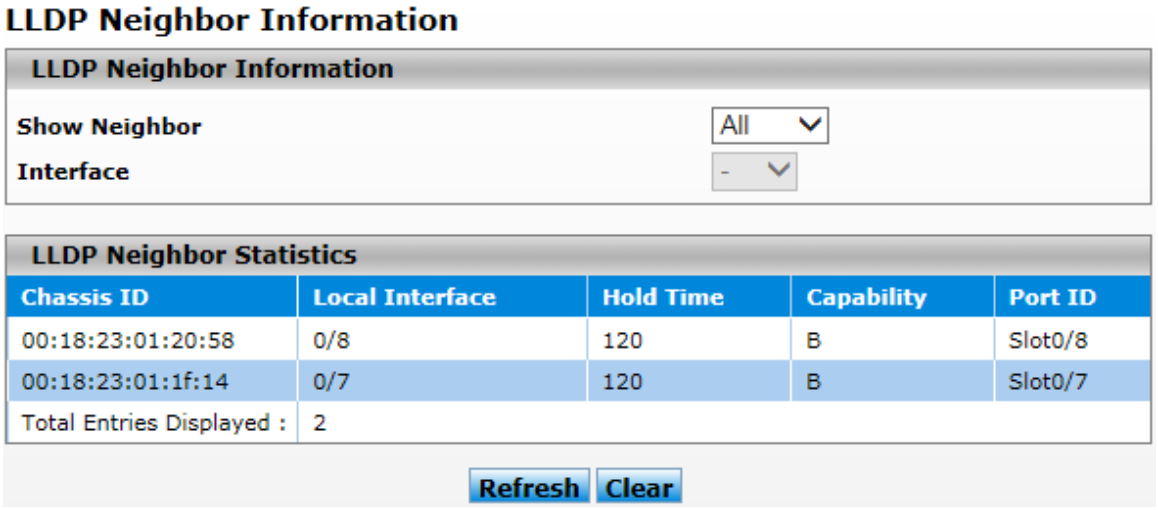
LLDP Local Information

Item	Description
Chassis ID Subtype	This field displays the MAC Address to be identified for the LLDP communication.
Chassis ID	This field displays the MAC address to identify the switch.
System Name	The system name that you specified on the **System Information** page
System Description	This is a fixed field that displays the model name and the description: DVS109W02-8 FE with 1 GE.
System Capability Supported	The device type. If the supported capabilities are identical to the enabled capabilities, the fields display the same information. The fields can display the following information: Router, Bridge, Telephone, DOCSIS Cable Device, WLAN Access Point, Repeater, Station, or Other.
System Capability Enabled	
Port ID Subtype	The data type displayed in the Port ID field.
Port ID	The physical address of the interface.
Port Description	The description of the port.
Enabled Tx TLVs	The Tx TLVs that are enabled, for example, if all TLVs are enabled: Port Description, System Name, System Description, System Capability,

Item	Description	
	Management Address, and Mac Phy.	
Management Address	Sub Type	The address type that the management interface uses, such as an IPv4 address
	Address	The address that is used to manage the switch
Extended 802.3 TLV Info		
MAC PHY Configuration & Status	Auto-Neg Support & Status	Displays whether the interface supports the port speed autonegotiation. For example: Supported, Enabled.
	Advertised Capability bits	The port speed autonegotiation capabilities
	Operational MAU Type	The Medium Attachment Unit (MAU) type. The MAU performs physical layer functions, including the digital data conversion from the Ethernet interface collision detection and the bit injection into the network.

3.13.1.5 LLDP Neighbor Information

You can view the LLDP neighbor statistics for an individual interface or all interfaces.



If you select **Detail** from the Show Neighbor item, the screen displays LLDP Neighbor Detail Statistics for the interface which you specified.

LLDP Neighbor Information

LLDP Neighbor Information

Description	Factory default
Show Neighbor	
• **All:** The information is for all interfaces. • **Detail:** The information is for one single interface.	All
Interface	
Specify one interface for information.	None

LLDP Neighbor Detail Statistics

Item	Description
Chassis ID	The chassis ID of the remote neighbor
Local Interface	The interface on the switch that receives the LLDP information from the remote neighbor
Hold Time	The period in seconds before an LLDP packet expires
Capability	The system capabilities of the remote system. The fields can display the following information: Router, Bridge, Telephone, DOCSIS Cable Device, WLAN Access Point, Repeater, Station, or Other.
Port ID	The port identification of the interface on the remote neighbor from which the information was sent

3.13.1.6 LLDP Traffic

LLDP Traffic Information

LLDP Traffic Information

Interface	Frames out	Entries Aged	Frames In	Frames Rx in Error	Frames Discarded	Unrecognized TLVs	Discarded TLVs
0/1	0	0	0	0	0	0	0
0/2	0	0	0	0	0	0	0
0/3	42	0	0	0	0	0	0
0/4	0	0	0	0	0	0	0
0/5	0	1	1	0	0	0	0
0/6	0	0	0	0	0	0	0
0/7	5412	0	5412	0	0	0	0
0/8	5412	0	5412	0	0	0	0

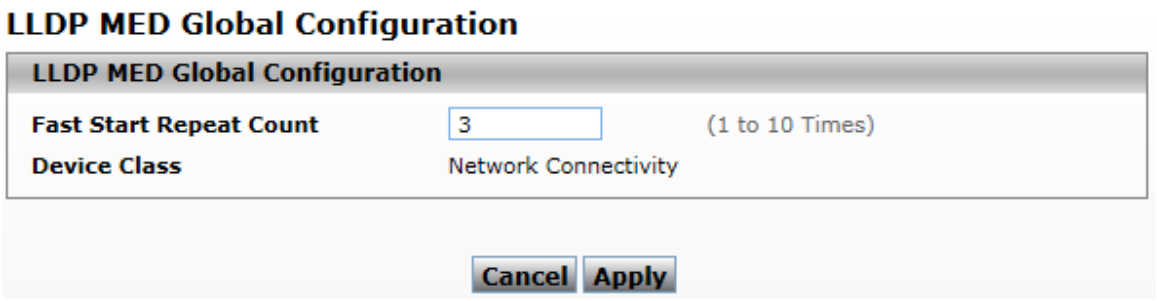
LLDP Traffic Statistics

Total Frames Out	10866
Total Entries Aged	1
Total Frames In	10825
Total Frames Received In Error	0
Total Frames Discarded	0
Total TLVs Unrecognized	0
Total TLVs Discarded	0

CLEAR

LLDP Traffic Information: The statistics of the fields are for each individual interface.
LLDP Traffic Statistics: These statistics are total quantities of LLDP traffic for the switch.

3.13.1.7 LLDP-MED Global Configuration

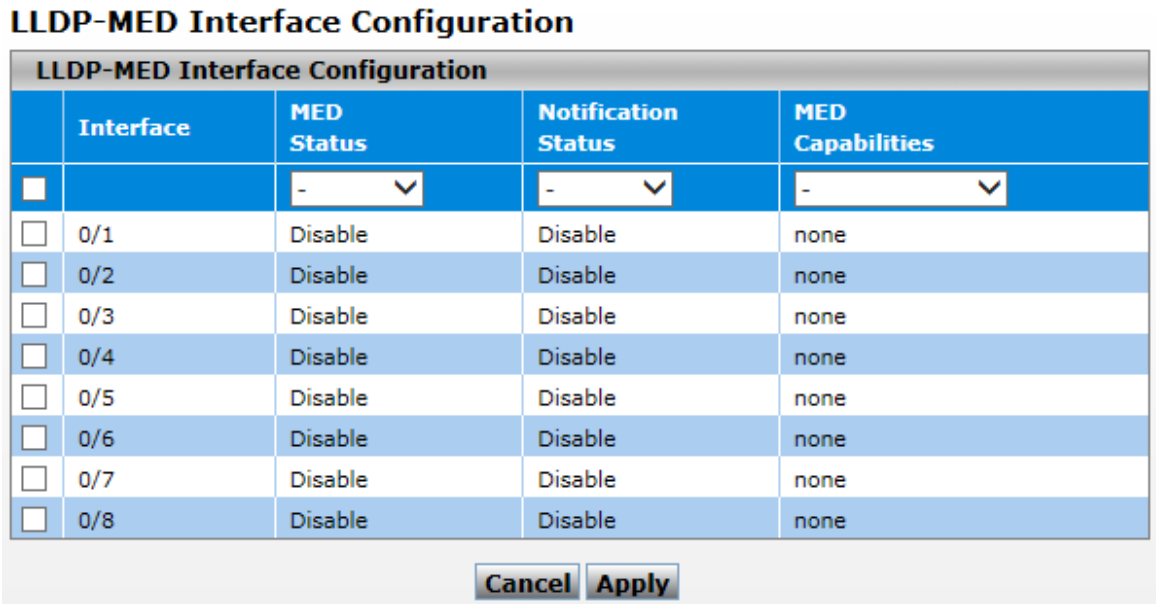


LLDP MED Global Configuration

Description	Factory default
Fast Start Repeat Count	
Enter the number of LLDP protocol data units (PDUs) that are transmitted when LLDP-MED is enabled for an interface. Enter a number in the range of 1 to 10.	3
Device Class	
This field displays the MED classification of the switch. There are four different kinds of devices, and the first three items represent the actual endpoints: • **Class I:** Generic (for example, an IP communication controller) • **Class II:** Media (for example, a conference bridge) • **Class III:** Communication (for example, an IP phone) • **Network Connectivity (device):** Generally a LAN switch or a router, an IEEE 802.1 bridge, or an IEEE 802.11 wireless access point	None

3.13.1.8 LLDP-MED Interface Configuration

You can configure the LLDP-MED settings for an individual interface on this page.



LLDP-MED Interface Configuration

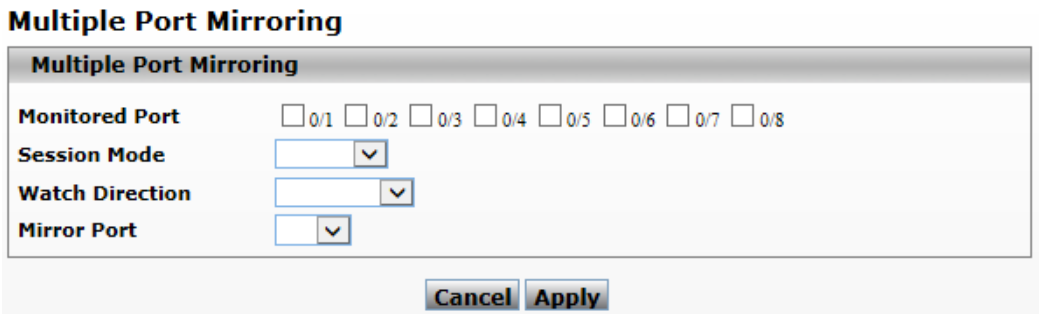
Description	Factory default
Interface	
This field displays the interface number or the port channel number.	*interface number*
Med Status	
Specify the MED status: • **Enabled:** MED is enabled for the interface. • **Disabled:** MED is disabled for the interface.	Disabled
Notification Status	
Specify the notification status: • **Enabled:** MED notifications are sent for the interface. • **Disabled:** MED notifications are not sent for the interface.	Disabled
MED Capabilities	
Specify the MED TLVs which are transmitted: • **none:** No MED TLVs are transmitted. • **network-policy:** The network policy information is transmitted. • **capabilities:** The capabilities information is transmitted. • **both:** Both the network policy information and the capabilities information are transmitted.	None

3.13.2 Port Mirroring

Port Mirror is used for monitoring the network traffic of the source port by the analyzer.

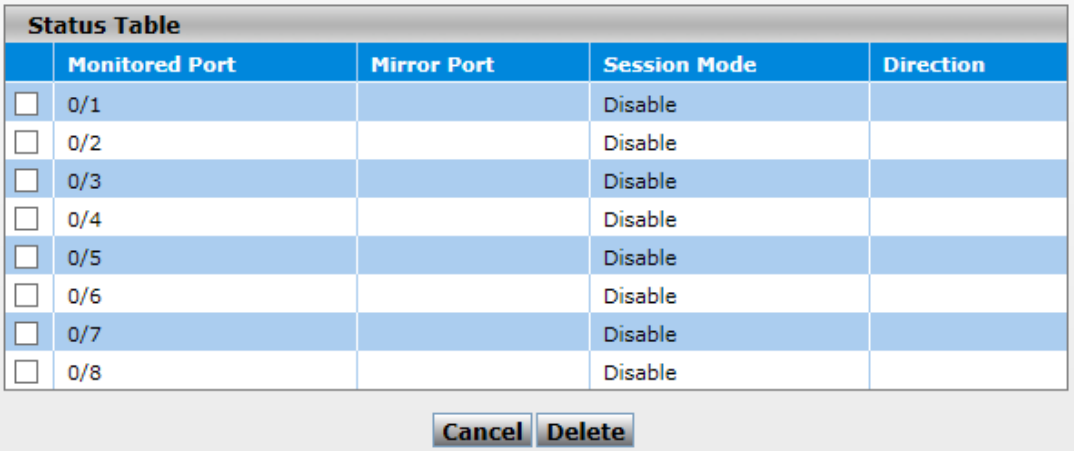
3.13.2.1 Multiple Port Mirroring

The Delta switch can select multiple interfaces as source ports and one interface as a destination or monitor port. The monitor port can monitor the source ports' incoming and outgoing packets. Port Mirroring supports the mirroring of the packets passing in, out the source port, or both at the same time. It supports N to 1 and up to 8 monitored ports per system. Ingress-mirrored packets are sent as unmodified packets (as the packets came in on the ingress port). Egress-mirrored packets are sent as modified packets with a VLAN tag. If the packet is not tagged, the packet will be tagged with tag 1. If the packet is tagged, the packet will not be modified. It does not support the use of the LAG port as a monitored port or a mirror port.



Multiple Port Mirroring

Description	Factory default
Monitored Port	
Specify the monitored port or ports for the monitoring.	Unchecked
Session Mode	
Specify whether the port mirroring session mode is enabled: • **Enable:** The port mirroring is enabled. The setting applies to all interfaces. • **Disable:** The port mirroring is disabled. The setting applies to all interfaces. **Note:** When you configure the session mode for an individual interface, it is applied to all interfaces. You can select **Enable** from the Session Mode drop-down list and control the port mirroring for individual interfaces. If you want to disable the port mirroring, make sure that the direction is not configured for the interfaces. If the direction is configured for the interfaces and you want to disable the port mirroring, select the check box of the interface, and click **Delete** to remove the port mirroring configuration for the interface.	None
Watch Direction	
Specify the direction in which the port mirroring occurs: • **Tx and Rx:** Both outgoing traffic and incoming traffic are mirrored. • **Tx Only:** Only outgoing traffic is mirrored. • **Rx Only:** Only incoming traffic is mirrored.	None
Mirror Port	
Specify the port which is the mirror port.	None

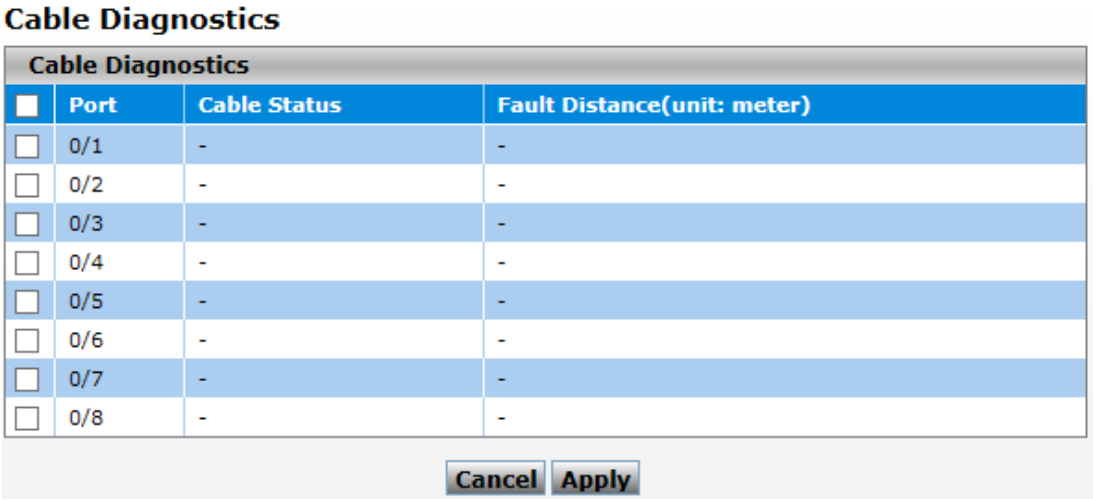


Status Table

Item	Description
Monitored Port	This field displays the monitored port number.
Mirror Port	This field displays the destination port or the monitored interface. Only one port can be the mirror port. This port is used as the mirror port for all ports which you configure for the port mirroring.
Session Mode	The port mirroring status of the port. • **Enable:** The port mirroring is enabled. • **Disable:** The port mirroring is disabled.
Direction	The direction of the port mirroring. • **Tx and Rx:** Both outgoing traffic and incoming traffic are mirrored. • **Tx Only:** Only outgoing traffic is mirrored. • **Rx Only:** Only incoming traffic is mirrored.

3.13.2.2 Cable Diagnostics

The Delta switch provides administrator the Cable Diagnostic function to detect whether the cable link status of the port is normal or not. The Cable status will show the cable link status of the port which you select.



Cable Diagnostics

Item	Description
Port	This field displays the port number.
Cable Status	This field displays the cable link status. For a different situation, there are five statuses: • Failure: The cable tester status is Failure. • Normal: The cable is working correctly. • Open: The cable is disconnected or there is a faulty connector. • Short: There is an electrical short in the cable. Or the cable is in an undetermined status, whether open or short. • Unknown: The cable is in a crosstalk status. Or a test is currently in progress. **Note:** The cable status of the combo port is always “normal”.
Fault Distance (Unit: meter)	The field displays the cable distance of the port which is in an abnormal link status.

3.14 Auto Warning

Industrial Ethernet devices in an industrial environment are very important. These devices usually need to work for a long time and are usually located at the end of the system. So if the devices which connect to the industrial Ethernet switch need to be maintained, the switch must provide some messages for the maintainer. Even when the maintainers or the engineers do not stay in the control room, they still need to be informed of the status of the devices. The Delta switch provides different approaches that can warn engineers automatically. In this section, you can get the information about a relay alarm.

> **IMPORTANT:**
> **Make sure that you save the configuration in the Save Configuration page after you have applied the configuration changes. (Save Config→Save Configuration) If you do not save the configuration, then the configuration will be cleared after the switch is rebooted.**

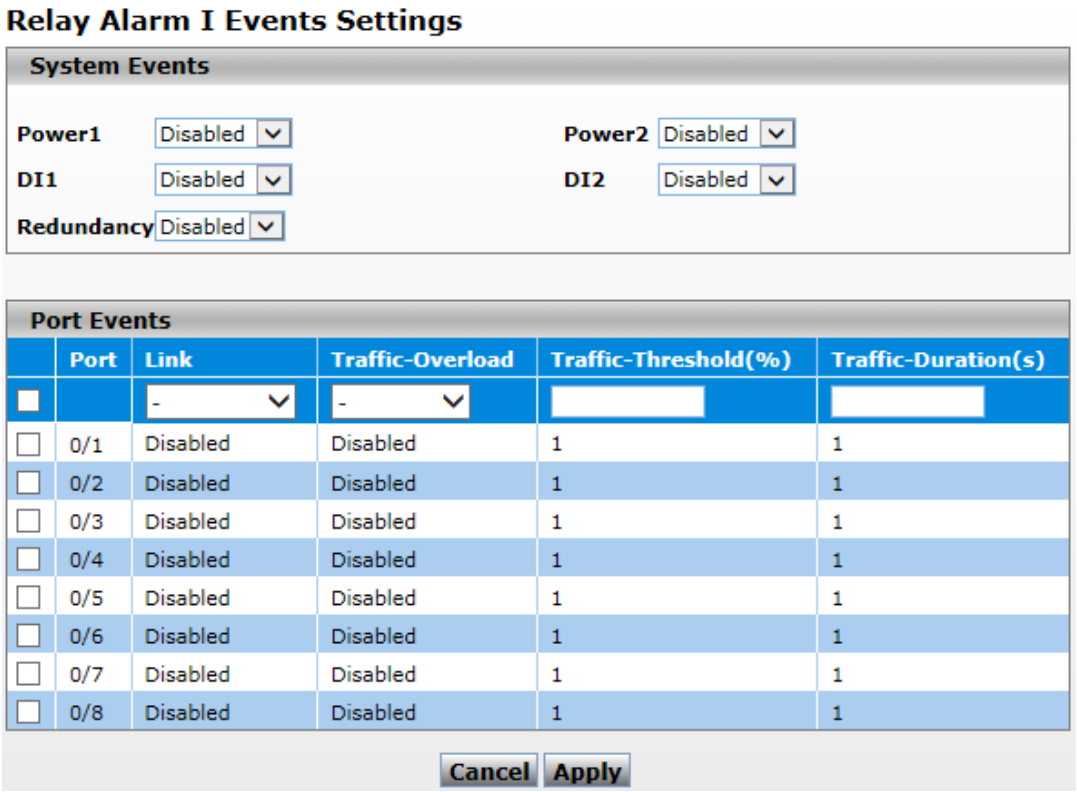
3

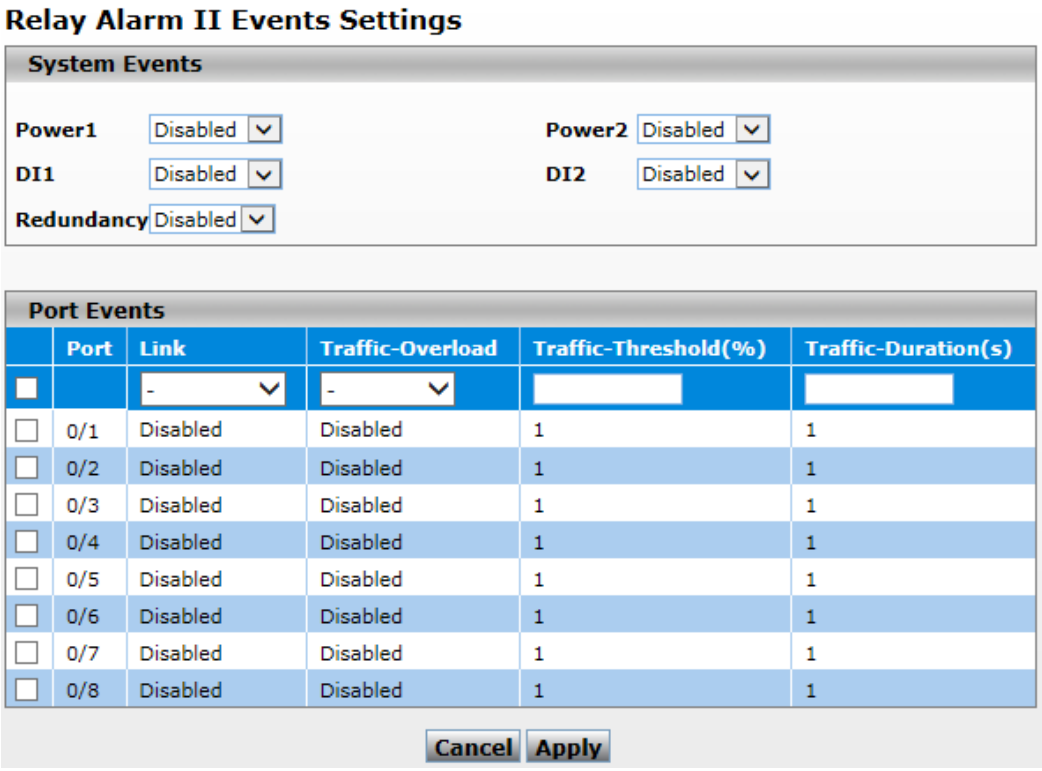
3.14.1 Relay Alarm

A relay alarm is used to monitor power, DI, the port status and redundancy. You can configure the power, DI, redundancy and the port link or the traffic overload alarm event to notice related engineers.

3.14.1.1 Relay Alarm Setting

The Delta switch provides flexible configuring items for you to configure events according to your requirement. If an event happens, it will trigger a relay alarm.





System Events

Description	Factory default
Power 1	
Specify the power event status: • **Disable:** Disable Power 1 to trigger relay alarm 1 or 2. • **On to Off:** When the status of Power 1 changes from On to Off, relay alarm 1 or 2 is triggered. • **Off to On:** When the status of Power 1 changes from Off to On, relay alarm 1 or 2 is triggered.	Disable
Power 2	
Specify the power event status: • **Disable:** Disable Power 2 to trigger relay alarm 1or 2. • **On to Off:** When the status of Power 2 changes from On to Off, relay alarm 1 or 2 is triggered. • **Off to On:** When the status of Power 2 changes from Off to On, relay alarm 1 or 2 is triggered.	Disable
DI 1	
Specify the DI event status: • **Disable:** Disable DI 1 to trigger relay alarm 1. • **On to Off:** When the status of DI 1 changes from On to Off, relay alarm 1 is triggered. • **Off to On:** When the status of DI 1 changes from Off to On, relay alarm 1 is triggered.	Disable
DI 2	
Specify the DI event status: • **Disable:** Disable DI 2 to trigger relay alarm 1 or 2. • **On to Off:** When the status of DI 2 changes from On to Off, relay alarm 1 or 2 is triggered. • **Off to On:** When the status of DI 2 changes from Off to On, relay alarm 1 or 2 **is** triggered.	Disable
Redundancy	
Specify the redundancy event status:	Disable

Description	Factory default
• **Disable:** Disable ONE RING, ONE CHAIN, or ONE COUPLING event to trigger relay alarm 1 or 2. • **Enable:** Enable ONE RING, ONE CHAIN, or ONE COUPLING event to trigger relay alarm 1 or 2. **Note:** If the hardware version is too old, this function will not be activated.	

Port Events

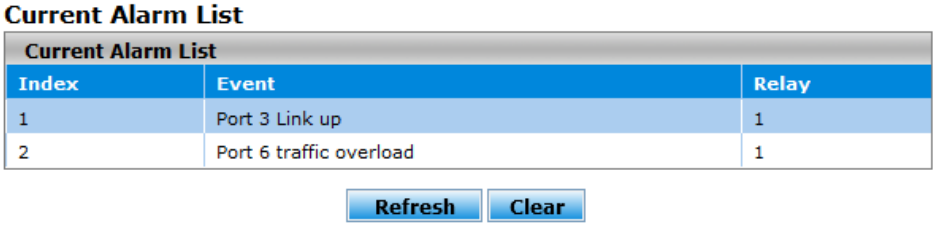
Description	Factory default
Link	
Specify the port link event status: • **Disable:** Disable the port link to trigger relay alarm 1 or 2. • **On to Off:** When the status of the port link changes from On to Off, relay alarm 1 is triggered. • **Off to On:** When the status of the port link changes from Off to On, relay alarm 1 is triggered.	Disable
Traffic-Overload	
Specify the traffic overload event status. The traffic overload is used to monitor the port's **ingress** traffic flow. It has two parameters: threshold and duration. • **Disable:** Disable traffic-overload to trigger relay alarm 1 or 2. • **Enabled:** Enable traffic-overload to trigger relay alarm 1 or 2.	Disable
Traffic-Threshold (%)	
Specify the traffic speed threshold percentage of the port. Enter the value between 1 and 100.	1
Traffic-Duration (s)	
Specify the traffic overload duration. If the average flow of the port overloads the threshold during this duration, it means the traffic is overloaded. Enter the value between 1 and 300.	1

Note:
If you want the Relay Alarm function to work properly, please make sure that the Delta switch has **one set of power at least**.
For example:

- The Power 1 system event is configured to "Off to On", and Power 1 & 2 have no power. If you provide power for Power 1, then Relay Alarm will not be triggered. Because when the event happened, the Delta switch has no power at that moment.
- The Power 1 system event is configured to "On to Off", and Power 1 has power, but Power 2 has no power. If you turn off Power 1, then Relay Alarm will not be triggered. Even though the Delta switch has power at the moment when the event happens, it has no power after that moment, so Relay Alarm will not be triggered.

3.14.1.2 Relay Alarm Table

The status of Relay Alarm is displayed on this page. This table only displays the current alarm, so if the event is not triggered, it is not displayed either.



Current Alarm List

Item	Description
Index	The index number in the list
Event	This field displays the alarm event.
Relay	This field displays the relay number.

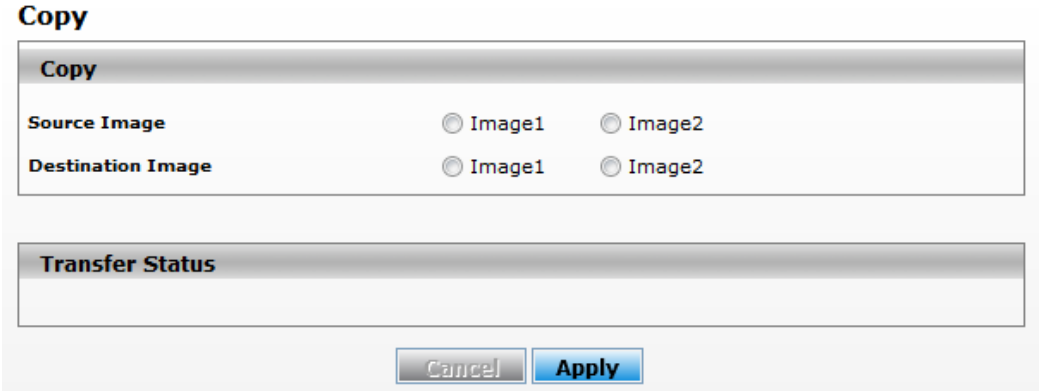
3.15 Dual Image

The Delta switch allows a user to maintain two image files. One image can function as an active image. The second image can function as a backup image, and you can put an older or the newest image in the second image. This function provides an efficient firmware upgrade or downgrade process, and reduces the time during the process.

IMPORTANT:
Make sure that you save the configuration in the Save Configuration page after you have applied the configuration changes. (Save Config→Save Configuration) If you do not save the configuration, then the configuration will be cleared after the switch is rebooted.

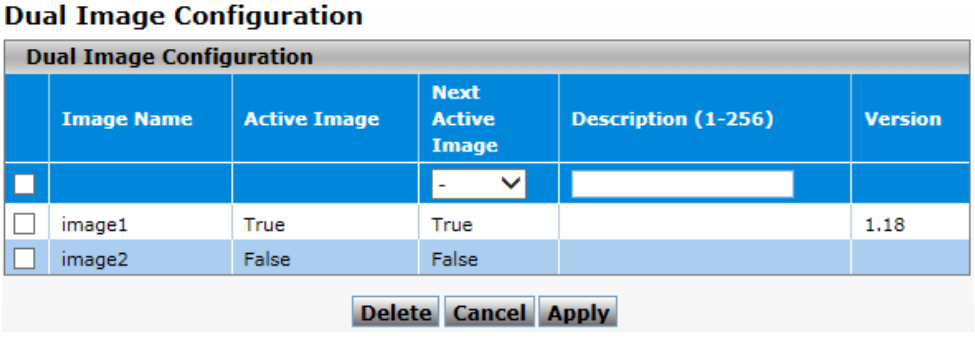
3.15.1 Copy

After upgrading firmware and running it as active firmware, you can keep the older image to image2, or you can copy the current firmware to image2 for backup.



3.15.2 Configuration

If you have two firmware image files, you can specify the firmware which is the active firmware, and it is loaded when the switch starts or restarts.



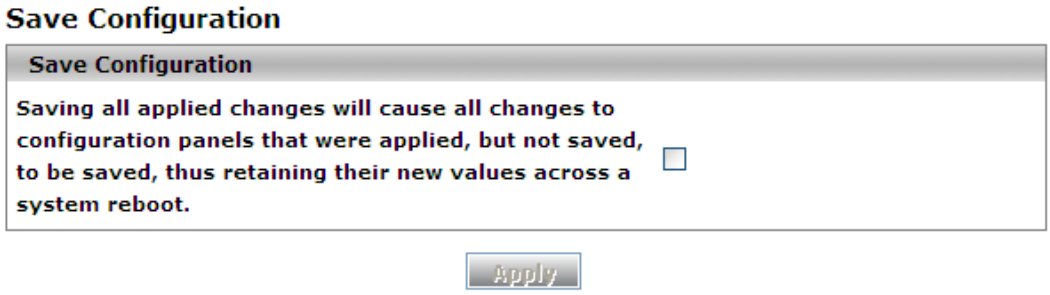
Note:
Please make sure that you have saved the settings on the switch before you restart the switch.

3.16 Save Config

Save Config allows users to save configuration, and erase configuration and logs.

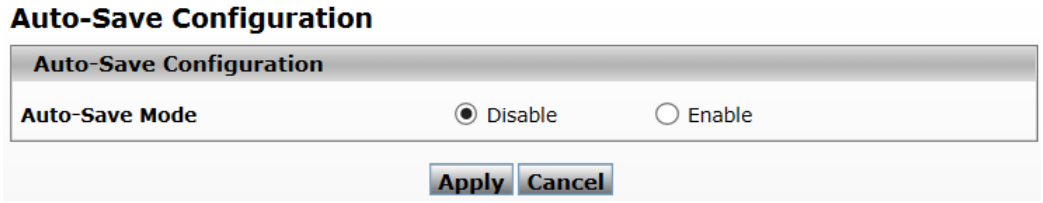
3.16.1 Save Configuration

After you select the box and click the **Apply** button, all the configuration will be saved in the **Startup Configuration** file. And if you reboot the switch, the configuration will be retained. If you do not save configuration before rebooting the switch, the configuration value that you have saved last time will be gone after you reboot the switch.



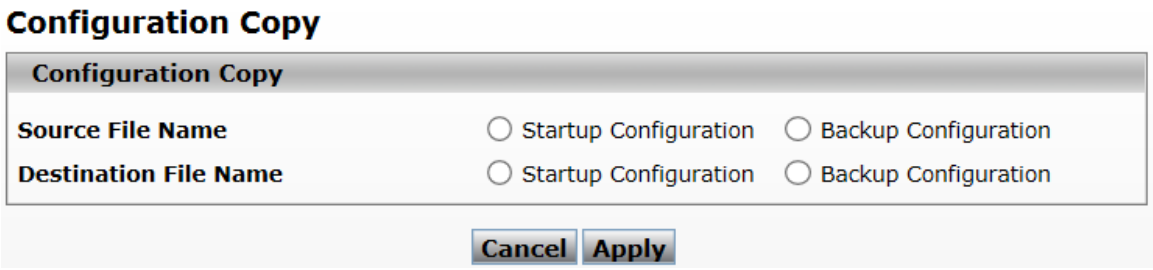
3.16.2 Auto-Save Configuration

When enable auto-save mode, all of the current configuration will be written to the Startup Configuration automatically. Users no need to check “Save Configuration” function when you are done configuring every time.



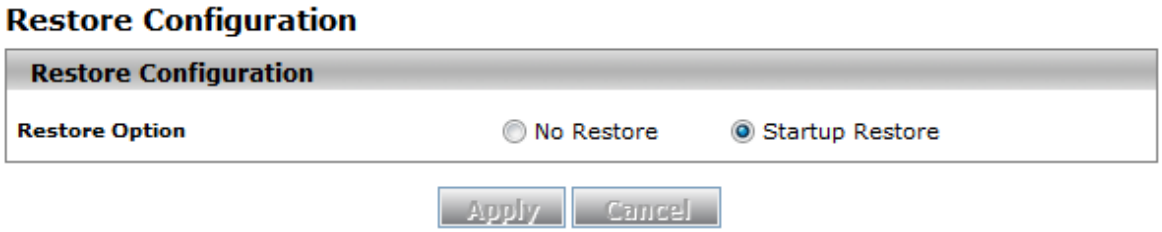
3.16.3 Configuration Copy

This feature support user to backup the configuration file.



Note:
Before you use the function, creat a backup file first so that the function can be configured. You can refer to the Chapter 3.1.7.2 Upload file.

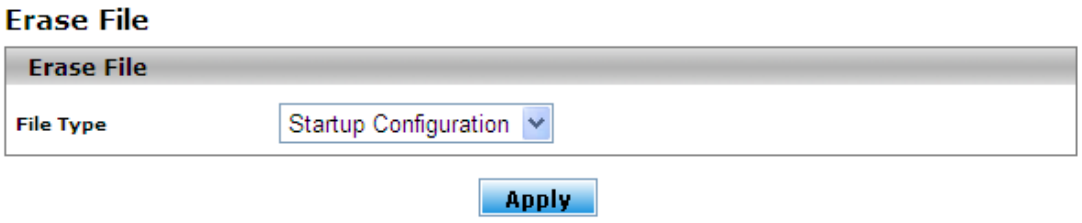
3.16.4 Restore



Restore Configuration

Item	Description
No Restore	After the switch reboots, it will load default configuration.
Startup Restore	After the switch reboots, it will load startup configuration. **Note:** Please make sure that you have saved the settings on the switch before restart the switch.

3.16.5 Erase



There are three file types which can be erased:

- Startup Configuration
- Backup Configuration
- Log

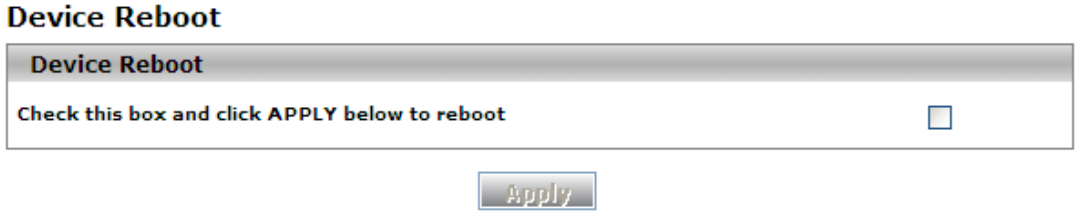
Note:
When you erase the startup configuration file (for example, because there are problems with the file) and then restart the switch, the factory default startup configuration is used. However, note that erasing the startup configuration file is not the same as resetting the switch to the factory default settings. Resetting the switch to the factory default deletes not only the startup configuration file but also all other configuration files such as the SSL key, the log files, the backup configuration, and so on.

3.17 Reset

The Reset function provides the function of rebooting a switch for users.

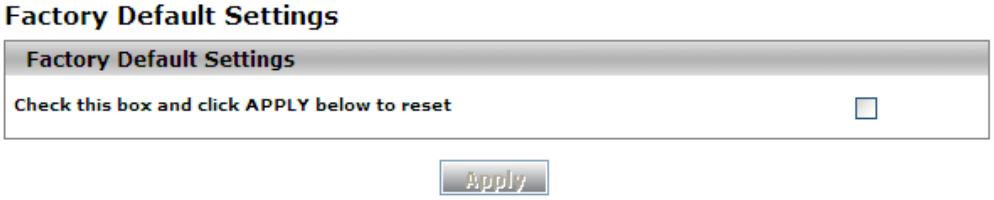
3.17.1 Device Reboot

After you select the box and click the **Apply** button, GUI will not be available until the switch completes the boot cycle. After the switch is reset, you need to re-login again.



3.17.2 Factory Default Settings

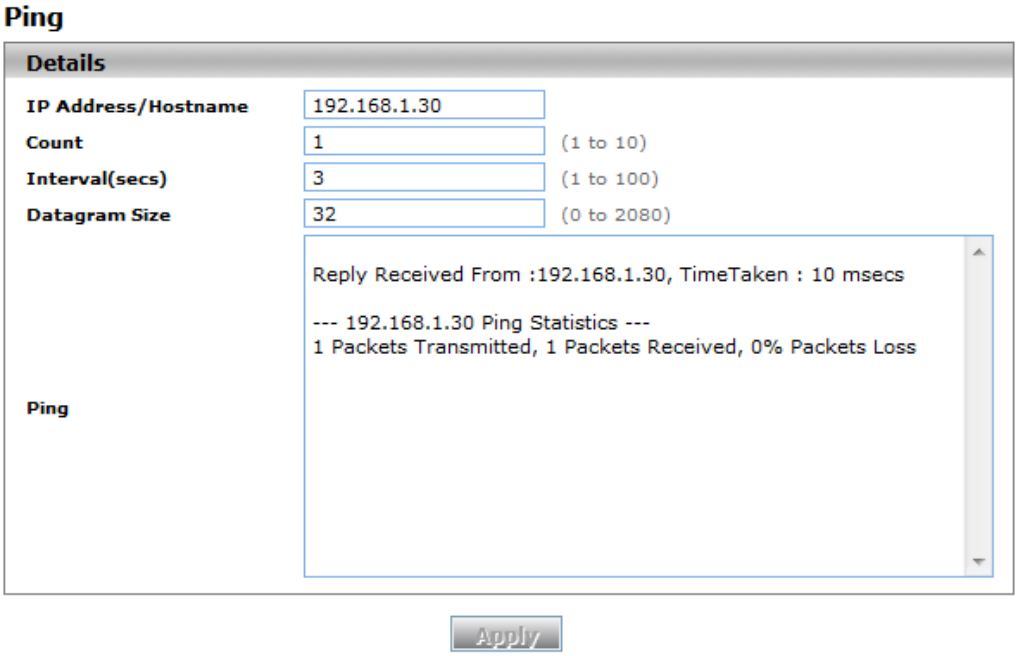
After you select the box and click the **Apply** button, the Delta switch will be reset to the factory default values. The IP address reverts to 192.168.1.5, the user login name reverts to the admin, and the password is blank.



3.18 Troubleshooting

Sometimes there is disconnection or unstable connection in the network. So the Troubleshooting function provides the ping function which checks the connection situation between the Delta switch and the other devices or clients. It also provides the traceroute function which traces the packet's path to a remote destination.

3.18.1 Ping IPv4



Ping

Description	Factory default
IP Address/Hostname	
Specify the IP address or the host name that you want to ping. Enter an IPv4 address or a host name.	None
Count	
Specify the number of echo requests to be sent. Enter a number between 1 and 10.	3
Interval(secs)	
Specify the ping request interval between the ping packets if the IP address/Hostname doesn't reply. Enter a number between 1 and 100 seconds.	3
Datagram Size	
Specify the size of the ping packet in bytes. Enter a payload size between 0 and 2080 bytes.	32

- An unsuccessful ping is displayed in the way described below:
  Reply Not Received From : <ipv4 address>, Timeout : <number> secs
  --- <ipv4 address> Ping Statistics ---
  <count> Packets Transmitted, 0 Packets Received, 100% Packets Loss
- A successful ping is displayed in the way described below:
  Reply Received From : <ipv4 address>, TimeTaken : <number> msecs
  --- 192.168.1.5 Ping Statistics ---
  <count> Packets Transmitted, <number> Packets Received, 0% Packets Loss

Note:
Make sure that the IP Address/Hostname you want to ping really exists and normally works in the same segment as the switch.

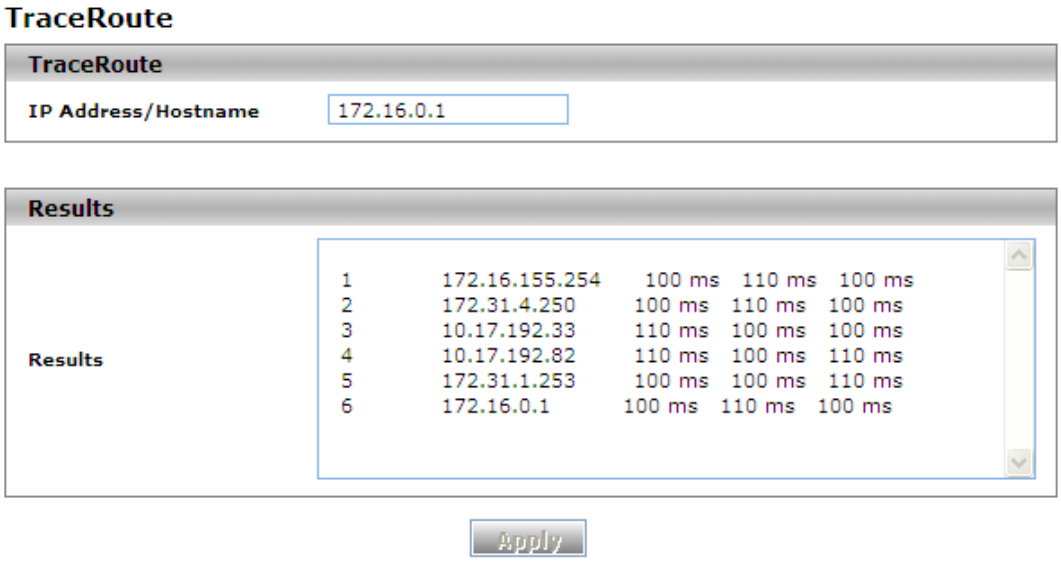
3.18.2 Ping IPv6

Ping IPv6

Description	Factory default
Ping	
Specify a type of IP address. • **Global:** The global IP address • **Link Local:** The link local IP address. They are assigned with the fe80::/64 prefix.	Global
IPv6 Address/Host Name	
Specify the IPv6 address or the host name that you want to ping. Enter an address in the xxxx:xxxx:xxxx:xxxxx:xxxx:xxxx:xxxx:xxxx format.	None
Datagram Size	
Specify the size of the ping packet in bytes. Enter a payload size between 48 and 2048 bytes.	100

- An unsuccessful ping is displayed in the way described below:
  ping6 <IPv6 address> Destination Unreachable
- A successful ping is displayed in the way described below:
  count=3, Receive count=<number> from <IPv6 address>. Average round trip time = <number> ms

3.18.3 Traceroute IPv4



Traceroute IPv4

Item	Description
IP Address/Hostname	Specify the IP address or the host name that you want to ping. Enter an IPv4 address or a host name.

After you click **Apply** to trace the route, the results are displayed in the Results field. If the switch can not trace the route, the Results field displays asterisk characters (***).

3.18.4 Traceroute IPv6

After you click **Apply** to trace the route, the results are displayed in the Results field. If the switch can not trace the route, the Results field displays asterisk characters (***) and the following text: “Destination unreachable Error in receiving the packet.”

Traceroute IPv6

Item	Description
IPv6 Address/Host Name	Specify the IPv6 address or the host name that you want to ping. Enter an address in the xxxx:xxxx:xxxx:xxxxx:xxxx:xxxx:xxxx:xxxx format.

3.19 Logout

Logout will disconnect the HTTP session. After you finish the configuration, we recommend that you log out for security reasons.

MEMO

Chapter 4 IEXplorer Utility Introduction

Table of Contents

Delta has many kinds of industrial products and network devices. If you have many Delta network products, the IEXplorer utility can help you search them via one interface. The IEXplorer utility can search for IES series products, DVP series products and some Delta products which have extension communication cards. It can help you know the IP address of a device, modify the configuration, and upgrade the firmware.

The IEXplorer utility supports the following models:

- DVS-108W02-2SFP
- DVS-109W02-1GE
- DVS-110W02-3SFP
- DVW-W02W2-E2 / DVW-W02W2-E2-CN / DVW-W02W2-E2-EU
- DVS-328R02-8SFP
- DVS-G512W01-4GF
- IFD9506
- IFD9507
- RTU-EN01
- DVPEN01-SL
- DVP12SE
- DVP-FEN01
- DVPSCM12-SL
- DVPSCM52-SL
- ASDA-M
- CMC-MOD01
- CMC-EIP01

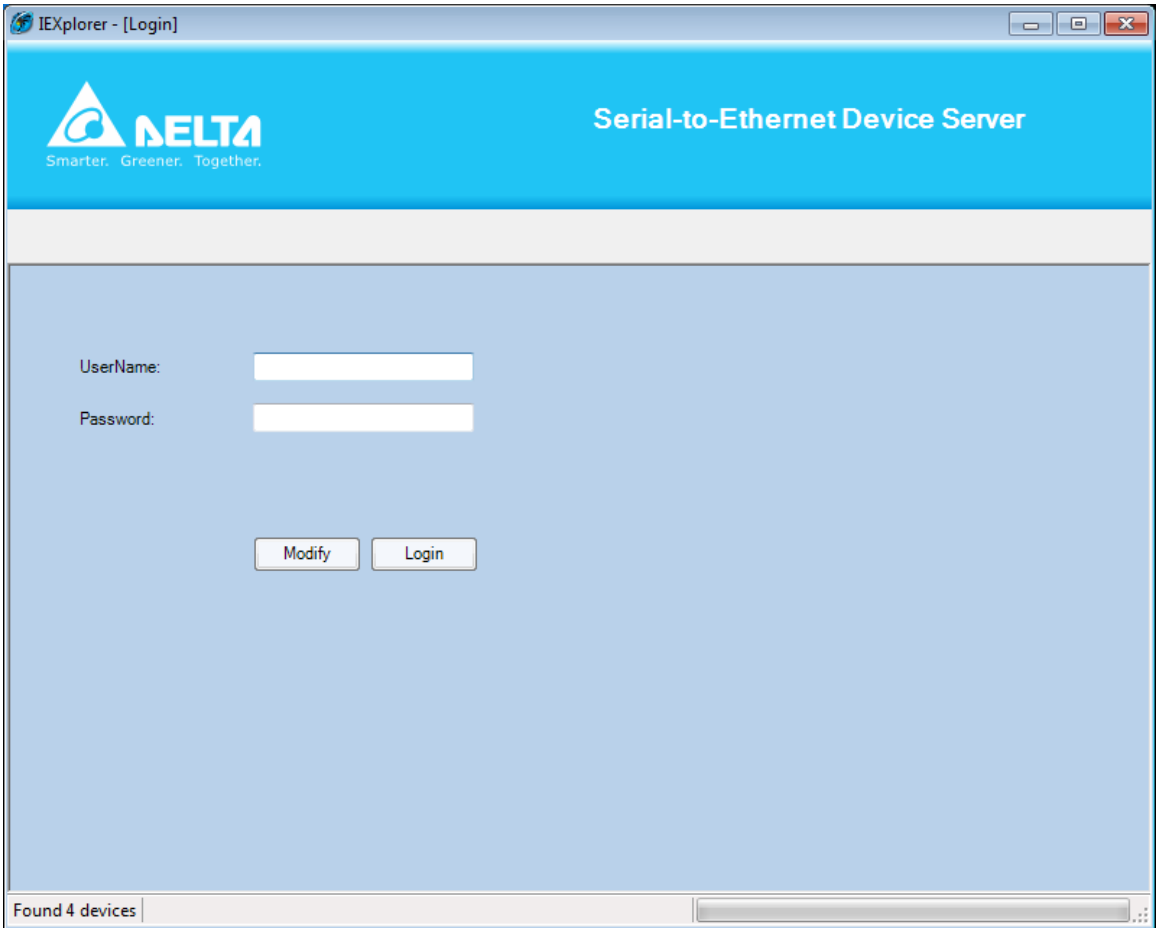
More models are coming soon.

Compatible OS: Windows XP SP2, Windows 7 (32/64 bits), Windows 8(64 bits)or Windows 10 (32/64 bits)

4.1 Starting the Configuration

After you finish the installation, you can find the IEXplorer icon on the desktop. Double-click the icon to run the program.

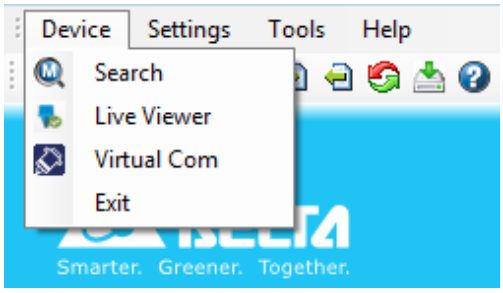
1. After double-clicking the icon, you can see the IEXplorer interface shown below:



2. Enter the username “**admin**” and the password is “**admin1234**”, click Login button to start the configuration.
3. IEXPlorer also provides an admin user can be able to make modification of password. Passwords are 1–20 alphanumeric characters in length and are case sensitive. The password is displayed as asterisks (*).

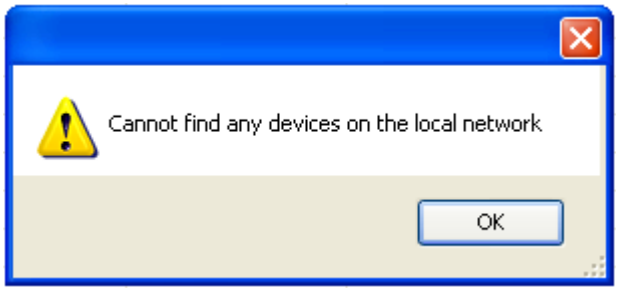
4.2 Device

There are four items on the **Devices** menu: Search, Live Viewer, Virtual COM and Exit.



4.2.1 Search

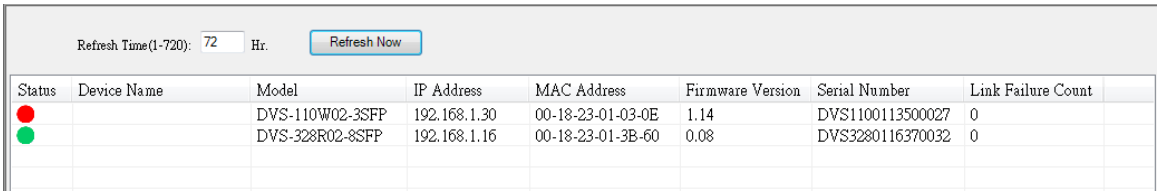
If the utility can not find any devices, the message box will pop up.



The automatic search function performs every 1 minute. If the device does not exist anymore, it will be moved from the list view.
You can specify the refresh interval from the device search window

4.2.2 Live Viewer

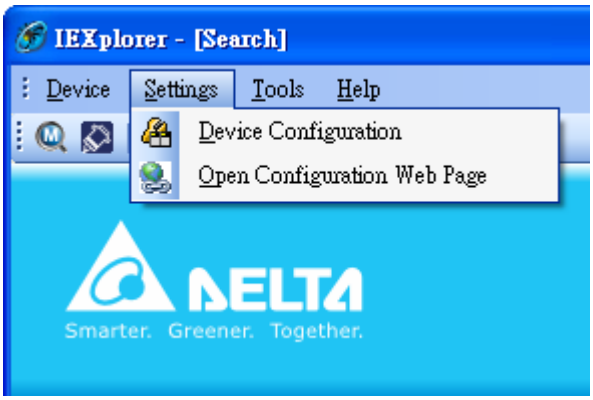
IEXplorer provides the user monitor the connectivity. The default refresh interval is 72 hours, and the range is 1 to 720 hours. The status of RED is meaning disconnection and the status of GREEN is meaning connection.
If the user needs to check current on-line status, please click the **Refresh Now** button.



Status	Device Name	Model	IP Address	MAC Address	Firmware Version	Serial Number	Link Failure Count
		DVS-110W02-3SFP	192.168.1.30	00-18-23-01-03-0E	1.14	DVS1100113500027	0
		DVS-328R02-8SFP	192.168.1.16	00-18-23-01-3B-60	0.08	DVS3280116370032	0

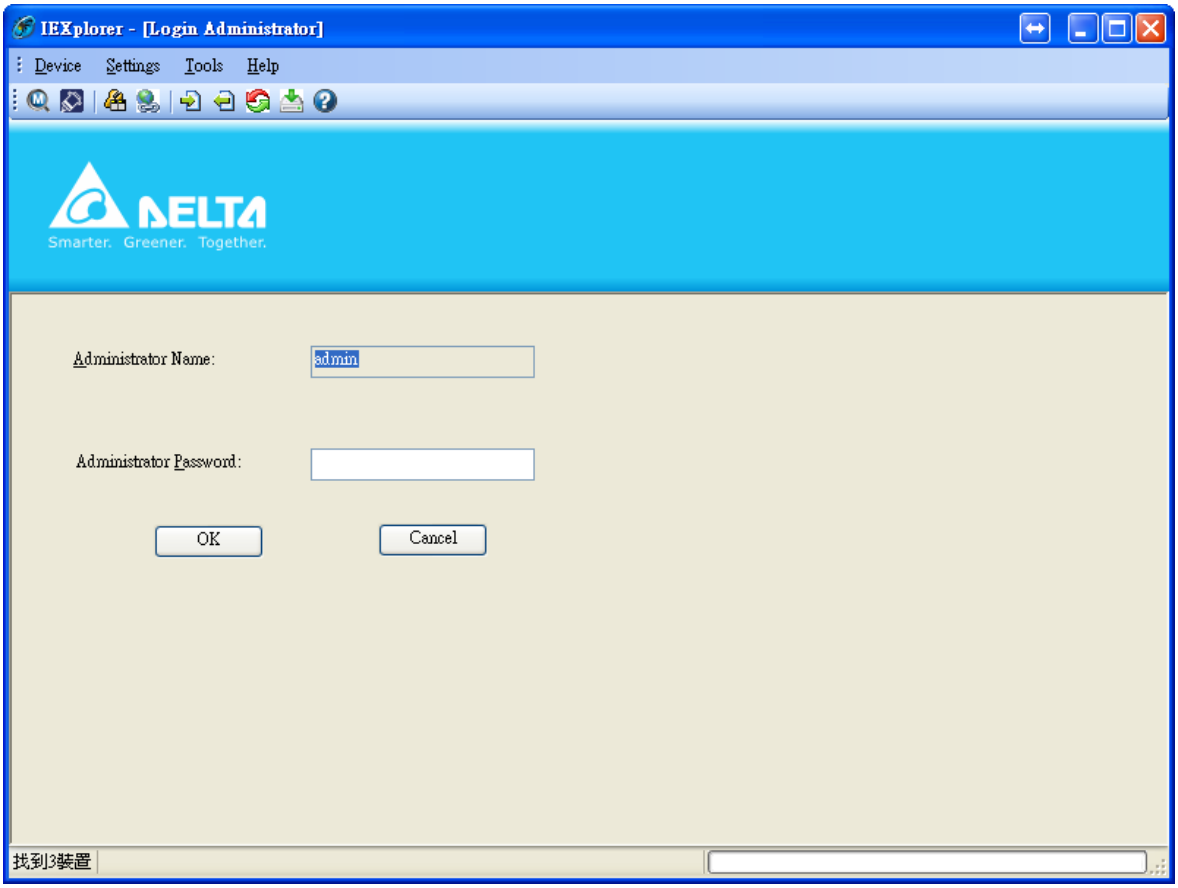
4.3 Settings

The IEXplorer utility provides two ways for users to configure the devices. You can configure the basic settings via **Device Configuration** or configure completely settings via **Open Configuration Web Page**. The **Settings** menu can be clicked only when you select DVS or DVW series products in the list view.

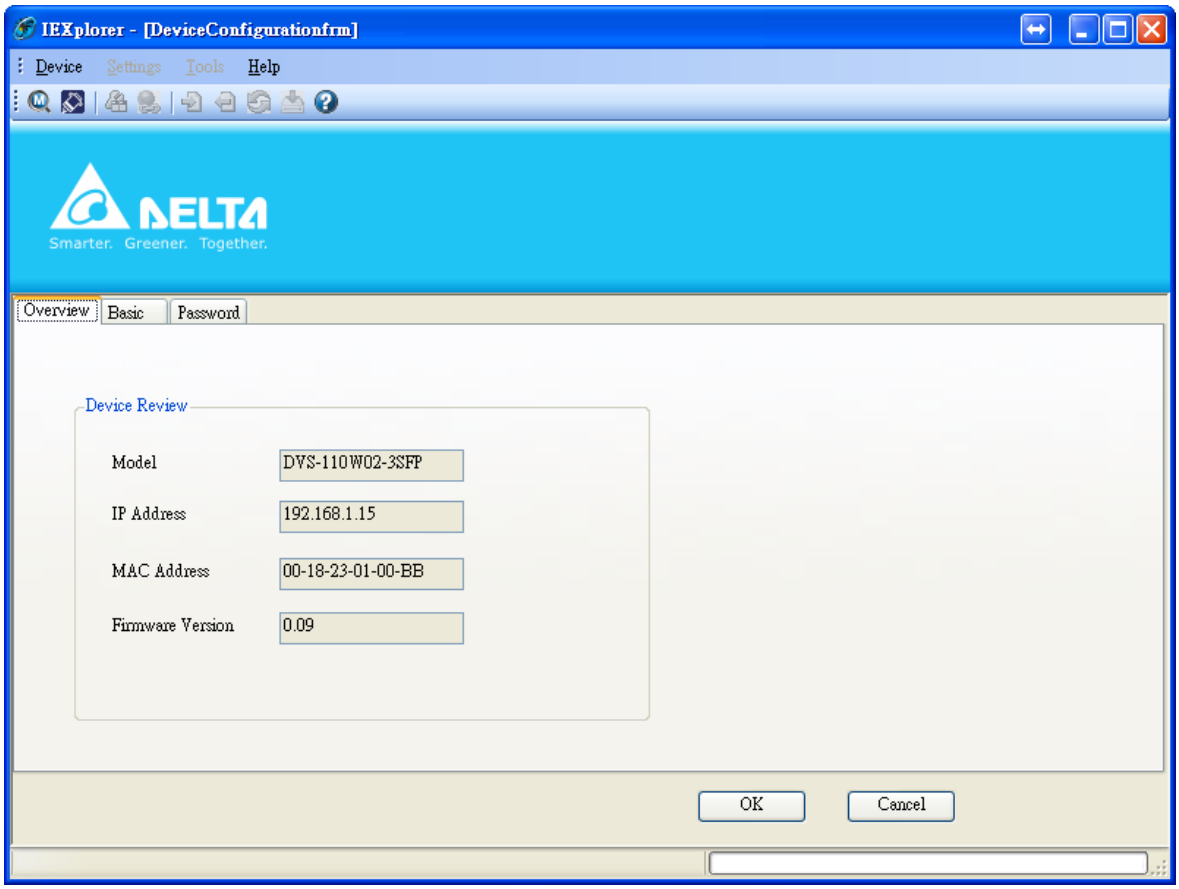


4.3.1 Device Configuration

The login ID and the password are the same as the web interface.



After the authentication progresses, the basic setting interface will display information, as shown below:

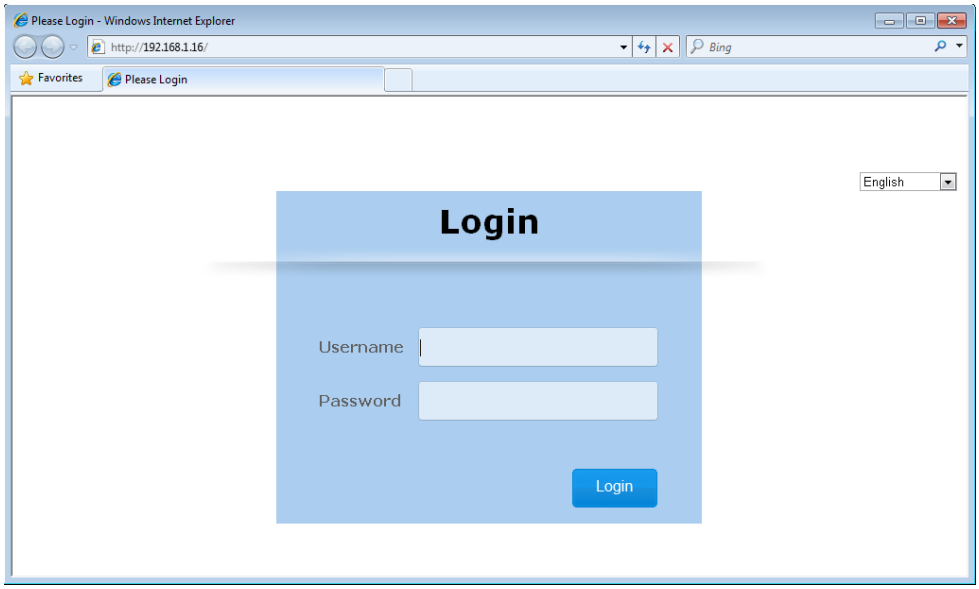


4

You can configure the device name and the IP information, modify the password, and reset the password to the factory default setting in this interface.

4.3.2 Configuration Web Page

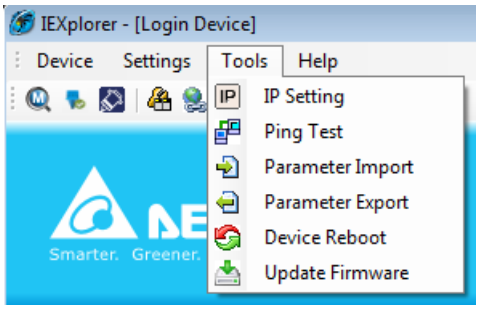
If you click **Open Configuration Web Page**, the web interface will be displayed.



Note:
You can double-click the device in the list view to open the configuration web page. If the device which you select is not a DVS or DVW series device, the utility will start **DCISoft** for you to configure the device.

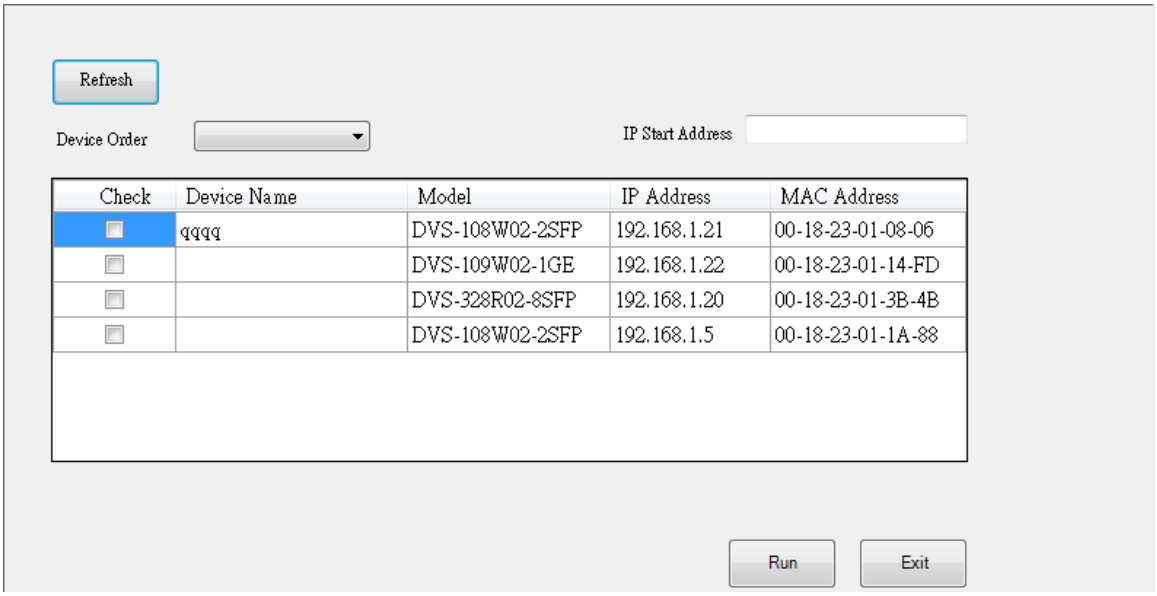
4.4 Tools

Please select the device before using the functions on the **Tools** menu.



4.4.1 IP Setting

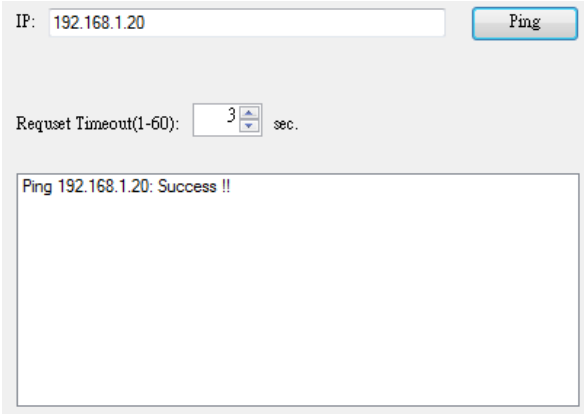
After IP Setting is clicked, it will display the device list and you can select one device to configure a static IP address, or entering the start IP address to configure multiple devices which you select from the device list.



Note:
If you need to keep the IP address, please remember to save the configuration from any managed interface

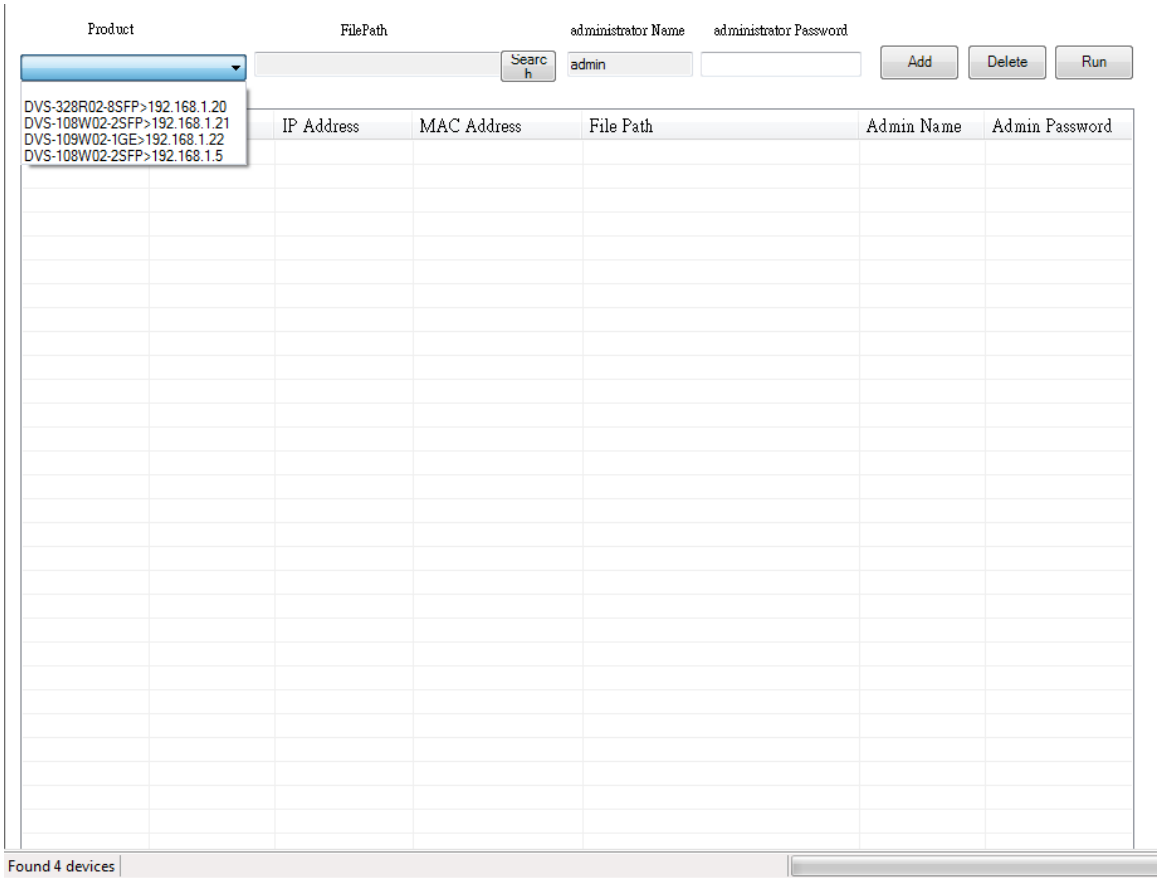
4.4.2 Ping Test

After Ping Test is clicked, you can specify the IP address that you want to ping.



4.4.3 Parameter Import

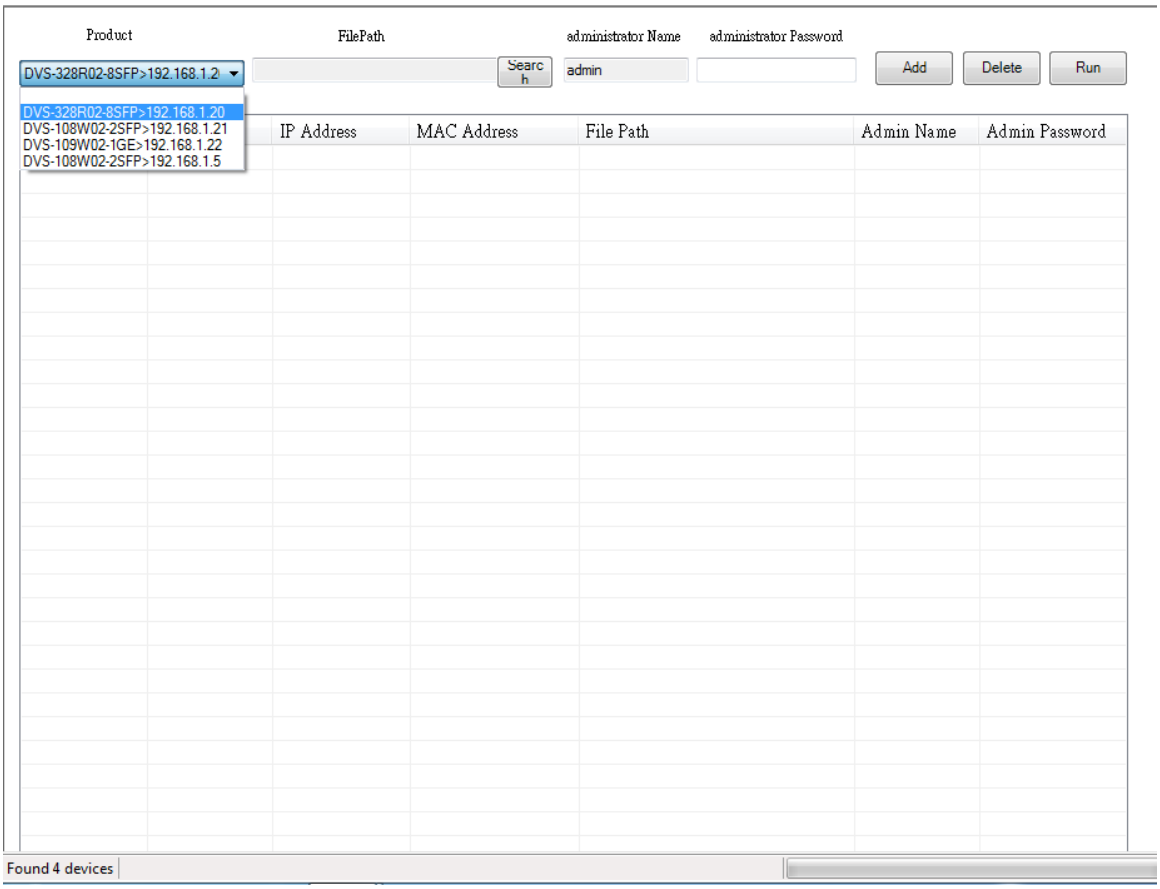
After **Parameter Import** is clicked, the drop-down list of Product will display the product list, and you can select one device to import the parameter file.
When you select the product and the path is specified, entering administrator name and password to starting import the parameter file.



Note:
Make sure the parameter file and the product you selected is matched.

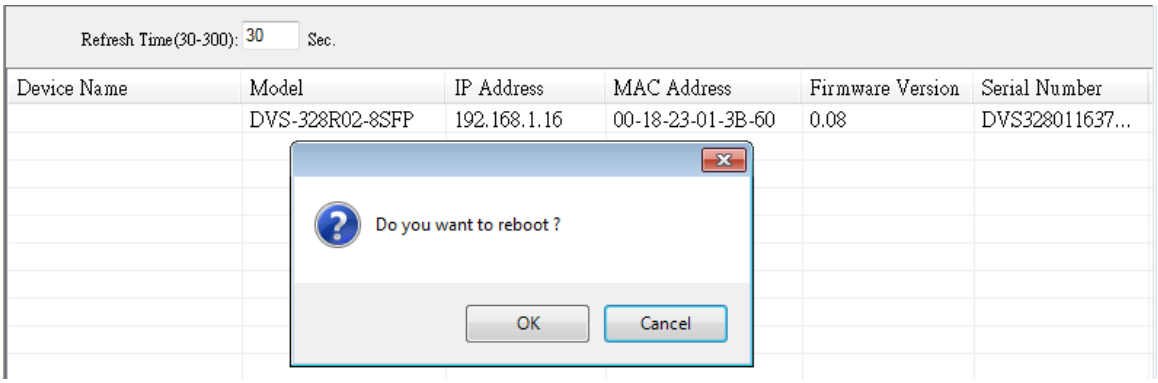
4.4.4 Parameter Export

After **Parameter Export** is clicked, the drop-down list of Product will display the product list, and you can select one device to export the parameter file.
When you select the product and the path is specified, entering administrator name and password to starting export the parameter file.



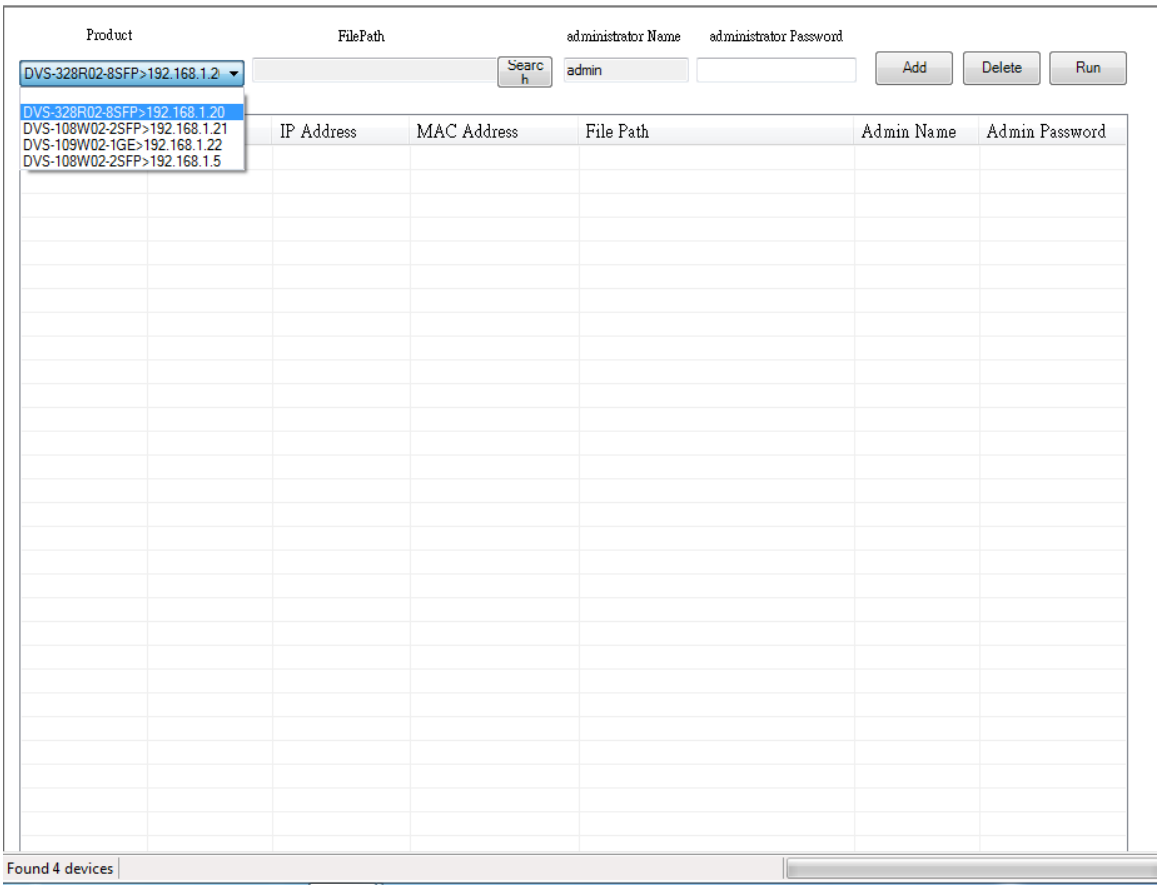
4.4.5 Device Reboot

IEXplorer allows you to reboot the device via the utility.



4.4.6 Update Firmware

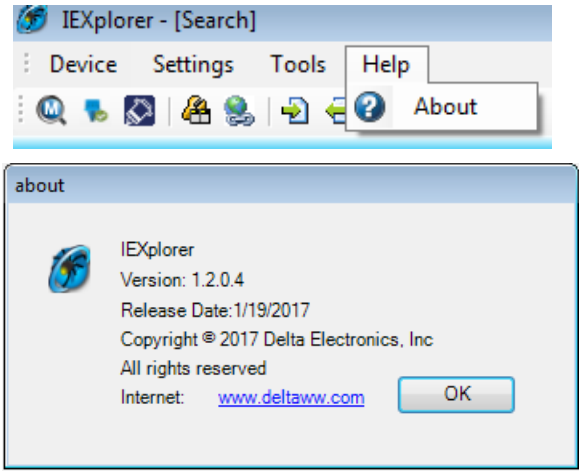
After **Update Firmware** is clicked, the drop-down list of Product will display the product list, and you can select one device to update the firmware.
When you select the product and the path is specified, entering administrator name and password to starting update firmware.



Note:
If it is updated successfully, please wait for 3 minutes to log in again.

4.5 Help

After **About** on the **Help** menu is clicked, an information message window of IEXplorer will pop up.



Appendix A Private MIB Group

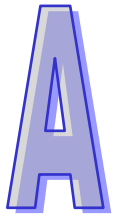
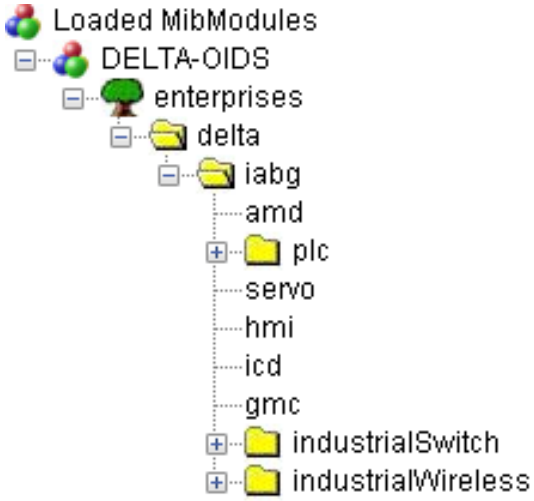


Table of Contents

A.1 Private MIB Group

Delta switch not only supports standard MIBs, but also provides private MIBs. You can use the SNMP tool to configure or monitor the switch's configuration. The private MIBs are the same as standard MIBs. It is displayed like a web tree. It's easily to be understood and used, so you don't need to learn or find where the OIDs of the commands are.
A private MIB can be found in the product CD if you need to use it.



We also support standard MIB Groups. For example, Interfaces Group, IP Group, TCP Group, UDP Group, and SNMP Group.

Appendix B MODBUS TCP Map

Table of Contents

B.1 DVS-108W02-2SFP

Address Offset	Data Type	Description
System Information		
0x0000	1 word	Reserved
0x0001	1 word	Reserved
0x0002	1 word	Reserved
0x0003	1 word	Firmware Version Hi byte = major Lo byte = minor
0x0004	2 word	Firmware Release Date Word 0 Hi byte = day Word 0 Lo byte = clock Word 1 Hi byte = year Word 1 Lo byte = month Ex: 20120918, PM9:00 Word 0 = 0x1215, Word 1 = 0x0C09
0x0010	20 words	Vendor Name = "Delta Electronics, Inc." Word 0 Hi byte = 'D' Word 0 Lo byte = 'e' Word 1 Hi byte = 'l' Word 1 Lo byte = 't' Word 2 Hi byte = 'a' Word 2 Lo byte = ' ' Word 3 Hi byte = 'E' Word 3 Lo byte = 'l' Word 4 Hi byte = 'e' Word 4 Lo byte = 'c' Word 5 Hi byte = 't' Word 5 Lo byte = 'r' Word 6 Hi byte = 'o' Word 6 Lo byte = 'n' Word 7 Hi byte = 'i' Word 7 Lo byte = 'c' Word 8 Hi byte = 's' Word 8 Lo byte = ', ' Word 9 Hi byte = ' ' Word 9 Lo byte = 'I' Word 10 Hi byte = 'n' Word 10 Lo byte = 'c' Word 11 Hi byte = '.' Word 11 Lo byte = '\0'

Address Offset	Data Type	Description
0x0030	20 words	Product Name = "DVS-108W02-2SFP" Word 0 Hi byte = 'D' Word 0 Lo byte = 'V' Word 1 Hi byte = 'S' Word 1 Lo byte = '-' Word 2 Hi byte = '1' Word 2 Lo byte = '0' Word 3 Hi byte = '8' Word 3 Lo byte = 'W' Word 4 Hi byte = '0' Word 4 Lo byte = '2' Word 5 Hi byte = '-' Word 5 Lo byte = '2' Word 6 Hi byte = 'S' Word 6 Lo byte = 'F' Word 7 Hi byte = 'P' Word 7 Lo byte ='\0'
0x0050	20 words	Serial No.
0x0070	3 words	Ethernet MAC Address Ex: MAC = 00:11:22:33:44:55 Word 0 Hi byte = 0x00 Word 0 Lo byte = '0x11 Word 1 Hi byte = 0x22 Word 1 Lo byte = 0x33 Word 2 Hi byte = 0x44 Word 2 Lo byte = '0x55
0x0073	2 words	Ethernet IP Address Ex: IP = 192.168.1.5 Word 0 = 0xC0A8 Word 1 = 0x0105
0x0075	2 words	Ethernet Netmask Ex: Mask = 255.255.255.0 Word 0 = 0xFFFF Word 1 = 0xFF00
0x0077	2 words	Ethernet Gateway IP Address Ex: IP = 192.168.1.1 Word 0 = 0xC0A8 Word 1 = 0x0101
0x0080	1 word	Power 1 Status 0x0000: OFF 0x0001: ON
0x0081	1 word	Power 2 Status 0x0000: OFF 0x0001: ON
0x0090	1 word	DO 1 Status 0x0000: OFF 0x0001: ON
0x0091	1 word	DO 2 Status 0x0000: OFF 0x0001: ON
0x00A0	1 word	DI 1 Status 0x0000: OFF 0x0001: ON

Address Offset	Data Type	Description
0x00A1	1 word	DI 2 Status 0x0000: OFF 0x0001: ON
Port Information		
0x1000 ~ 0x1007	1 word	Port 1 to 8 Status 0x0000: Link down 0x0001: Link up 0x0002: Disable
0x1100 ~ 0x1107	1 word	Port 1 to 8 Communication Format 0x0000: 10M,Half 0x0001: 10M,Full 0x0002: 100M,Half 0x0003: 100M,Full 0x0004: 1G,Full
0x1200 ~ 0x1207	1 word	Port 1 to 8 Flow Control 0x0000: OFF 0x0001: ON
0x1300 ~ 0x1307	1 word	Port 1 to 8 MDI/MDIX Setting 0x0000: Auto 0x0001: MDI 0x0002: MDIX
0x1400 ~ 0x148B	20 words	Port 1 to 8 Description EX: 10/100/1000TX,RJ45 Word 0 Hi byte = '1' Word 0 Lo byte = '0' Word 1 Hi byte = '/' Word 1 Lo byte = '1' Word 2 Hi byte = '0' Word 2 Lo byte = '0' Word 3 Hi byte = '/' Word 3 Lo byte = '1' Word 4 Hi byte = '0' Word 4 Lo byte = '0' Word 5 Hi byte = '0' Word 5 Lo byte = 'T' Word 6 Hi byte = 'X' Word 6 Lo byte = ',' Word 7 Hi byte = 'R' Word 7 Lo byte = 'J' Word 8 Hi byte = '4' Word 8 Lo byte = '5' Word 9 Hi byte = '\0' Word 9 Lo byte = '\0'
0x1500 ~ 0x1507	1 word	Port 1 to 8 bandwidth overload 0x0000: OFF 0x0001: Port X bandwidth overload
0x1600 ~ 0x1607	1 word	Port 1 to 8 loopback detection port status 0x0000: OFF 0x0001: loopback detected
Packet Information		
0x2000 ~ 0x200F	2 words	Port 1 to 8 Tx Packets Ex: Port 1 Tx Packet Amount = 0x33221100 0x2000 = 0x3322 0x2001 = 0x1100

Address Offset	Data Type	Description
0x2100 ~ 0x210F	2 words	Port 1 to 8 Rx Packets Ex: Port 1 Rx Packet Amount = 0x33221100 0x2100 = 0x3322 0x2101 = 0x1100
0x2200 ~ 0x220F	2 words	Port 1 to 8 Tx Error Packets Ex: Port 1 Tx Packet Amount = 0x33221100 0x2200 = 0x3322 0x2201 = 0x1100
0x2300 ~ 0x230F	2 words	Port 1 to 8 Rx Error Packets Ex: Port 1 Rx Packet Amount = 0x33221100 0x2300 = 0x3322 0x2301 = 0x1100
Redundancy Information		
0x3000	1 word	Redundancy Protocol 0x0000: None 0x0001: RSTP/STP
0x3001	1 word	RSTP Root 0x0000: Not Root 0x0001: Root
0x3100	1 word	RSTP Port 1 to 8 Status 0x0000: Port Disable 0x0001: Not RSTP Port 0x0002: Link Down 0x0003: Discarding 0x0004: Learning 0x0005: Forwarding
SPF DDM Information		
0x4000 ~ 0x4001	1 word	Port 7 to Port 8 Port No.
0x4100 ~ 0x4127	20 words	Port 1 to Port 2 Model Name Example: LCP-1250B4QDRH Word 0 Hi byte = 'L' Word 0 Lo byte = 'C' Word 1 Hi byte = 'P' Word 1 Lo byte = '-' Word 2 Hi byte = '1' Word 2 Lo byte = '2' Word 3 Hi byte = '5' Word 3 Lo byte = '0' Word 4 Hi byte = 'B' Word 4 Lo byte = '4' Word 5 Hi byte = 'Q' Word 5 Lo byte = 'D' Word 6 Hi byte = 'R' Word 6 Lo byte = 'H' Word 7 Hi byte = '\0' Word 7 Lo byte ='\0'
0x4200 ~ 0x4203	2 words	Port 7 to Port 8 Temperature Word 0 = Temperature MSB Word 1 = Temperature LSB
0x4300 ~ 0x4303	2 words	Port 7 to Port 8 Voltage Word 0 = Vcc MSB Word 1 = Vcc LSB
0x4400 ~ 0x4403	2 words	Port 7 to Port 8 TX Power Word 0 = TX Power MSB Word 1 = TX Power LSB

Address Offset	Data Type	Description
0x4500 ~ 0x4503	2 words	Port 7 to Port 8 RX Power Word 0 = RX Power MSB Word 1 = RX Power LSB
0x4600 ~ 0x4601	1 words	Port 7 to Port 8 Link Status 0x0000: Link down 0x0001: Link up
Alarm		
0x5000	1 word	Switch cold start alarm 0x0000: OFF 0x0001: ON 0xFFFF: Disable
0x5001	1 word	Switch warm start alarm 0x0000: OFF 0x0001: ON
0x5004	1 word	Power state on alarm 0x0000: OFF 0x0001: ON
0x5005	1 word	Power state off alarm 0x0000: OFF 0x0001: ON
0x5006	1 word	DI on alarm 0x0000: OFF 0x0001: ON
0x5007	1 word	DI off alarm 0x0000: OFF 0x0001: ON
0x5008	1 word	authentication failure alarm 0x0000: OFF 0x0001: ON
0x5009	1 word	dot1d Bridge New Root alarm 0x0000: OFF 0x0001: ON
0x500A	1 word	dot1d Bridge Topology Changed alarm 0x0000: OFF 0x0001: ON
0x500B	1 word	LLDP Remote Tables Change alarm 0x0000: OFF 0x0001: ON
0x500C	1 word	Configuration Changed alarm 0x0000: OFF 0x0001: ON
0x500D	1 word	Firmware update alarm 0x0000: OFF 0x0001: ON
0x500E	1 word	IP changed alarm 0x0000: OFF 0x0001: ON
0x500F	1 word	Password changed alarm 0x0000: OFF 0x0001: ON
0x5100 ~ 0x5102	1 word	SFP Port 7 to Port 8 DDM Failure - Temp alarm 0x0000: OFF 0x0001: ON

Address Offset	Data Type	Description
0x5110 ~ 0x5112	1 word	SFP Port 7 to Port 8 DDM Failure – Voltage 0x0000: OFF 0x0001: ON
0x5120 ~ 0x5122	1 word	SFP Port 7 to Port 8 DDM Failure – Bias 0x0000: OFF 0x0001: ON
0x5130 ~ 0x5132	1 word	SFP Port 7 to Port 8 DDM Failure - TX Power 0x0000: OFF 0x0001: ON
0x5140 ~ 0x5142	1 word	SFP Port 7 to Port 8 DDM Failure - RX Power 0x0000: OFF 0x0001: ON
IABU Internal Data (0x2B)		
Device ID Code	**Object ID**	**Description**
0x01	0x00	Vendor Name "Delta Electronics, Inc."
	0x01	Product Code "DVS-108W02-2SFP"
	0x02	Firmware Version Major.Minor Example: Major = 1, Minor = 2, Length = 4 Data byte 0: "31" Data byte 1: "." Data byte 2: "30" Data byte 3: "32"

B.2 DVS-109W02-1GE

Address Offset	Data Type	Description
System Information		
0x0000	1 word	Reserved
0x0001	1 word	Product Code
0x0002	1 word	Reserved
0x0003	1 word	Firmware Version Hi byte = major Lo byte = minor
0x0004	2 word	Firmware Release Date Word 0 Hi byte = day Word 0 Lo byte = clock Word 1 Hi byte = year Word 1 Lo byte = month Ex: 20120918, PM9:00 Word 0 = 0x1215, Word 1 = 0x0C09
0x0010	20 words	Vendor Name = "Delta Electronics, Inc." Word 0 Hi byte = 'D' Word 0 Lo byte = 'e' Word 1 Hi byte = 'l' Word 1 Lo byte = 't' Word 2 Hi byte = 'a' Word 2 Lo byte = ' ' Word 3 Hi byte = 'E' Word 3 Lo byte = 'l' Word 4 Hi byte = 'e' Word 4 Lo byte = 'c' Word 5 Hi byte = 't' Word 5 Lo byte = 'r' Word 6 Hi byte = 'o' Word 6 Lo byte = 'n' Word 7 Hi byte = 'i' Word 7 Lo byte = 'c' Word 8 Hi byte = 's' Word 8 Lo byte = ', ' Word 9 Hi byte = ' ' Word 9 Lo byte = 'l' Word 10 Hi byte = 'n' Word 10 Lo byte = 'c' Word 11 Hi byte = '.' Word 11 Lo byte = '\0'

Address Offset	Data Type	Description
0x0030	20 words	Product Name = "DVS-109W02-1GE" Word 0 Hi byte = 'D' Word 0 Lo byte = 'V' Word 1 Hi byte = 'S' Word 1 Lo byte = '-' Word 2 Hi byte = '1' Word 2 Lo byte = '0' Word 3 Hi byte = '9' Word 3 Lo byte = 'W' Word 4 Hi byte = '0' Word 4 Lo byte = '2' Word 5 Hi byte = '-' Word 5 Lo byte = '1' Word 6 Hi byte = 'G' Word 6 Lo byte = 'E' Word 7 Hi byte = '\0' Word 7 Lo byte ='\0'
0x0050	20 words	Serial No.
0x0070	3 words	Ethernet MAC Address Ex: MAC = 00:11:22:33:44:55 Word 0 Hi byte = 0x00 Word 0 Lo byte = '0x11 Word 1 Hi byte = 0x22 Word 1 Lo byte = 0x33 Word 2 Hi byte = 0x44 Word 2 Lo byte = '0x55
0x0073	2 words	Ethernet IP Address Ex: IP = 192.168.1.5 Word 0 = 0xC0A8 Word 1 = 0x0105
0x0075	2 words	Ethernet Netmask Ex: Mask = 255.255.255.0 Word 0 = 0xFFFF Word 1 = 0xFF00
0x0077	2 words	Ethernet Gateway IP Address Ex: IP = 192.168.1.1 Word 0 = 0xC0A8 Word 1 = 0x0101
0x0080	1 word	Power 1 Status 0x0000: OFF 0x0001: ON
0x0081	1 word	Power 2 Status 0x0000: OFF 0x0001: ON
0x0090	1 word	DO 1 Status 0x0000: OFF 0x0001: ON
0x00A0	1 word	DI 1 Status 0x0000: OFF 0x0001: ON

Address Offset	Data Type	Description
Port Information		
0x1000 ~ 0x1008	1 word	Port 1 to 9 Status 0x0000: Link down 0x0001: Link up 0x0002: Disable
0x1100 ~ 0x1108	1 word	Port 1 to 9 Communication Format 0x0000: 10M,Half 0x0001: 10M,Full 0x0002: 100M,Half 0x0003: 100M,Full 0x0004: 1G,Full
0x1200 ~ 0x1208	1 word	Port 1 to 9 Flow Control 0x0000: OFF 0x0001: ON
0x1300 ~ 0x1308	1 word	Port 1 to 9 MDI/MDIX Setting 0x0000: Auto 0x0001: MDI 0x0002: MDIX
0x1400 ~ 0x14B3	20 words	Port 1 to 9 Description EX: 10/100/1000TX,RJ45 Word 0 Hi byte = '1' Word 0 Lo byte = '0' Word 1 Hi byte = '/' Word 1 Lo byte = '1' Word 2 Hi byte = '0' Word 2 Lo byte = '0' Word 3 Hi byte = '/' Word 3 Lo byte = '1' Word 4 Hi byte = '0' Word 4 Lo byte = '0' Word 5 Hi byte = '0' Word 5 Lo byte = 'T' Word 6 Hi byte = 'X' Word 6 Lo byte = ',' Word 7 Hi byte = 'R' Word 7 Lo byte = 'J' Word 8 Hi byte = '4' Word 8 Lo byte = '5' Word 9 Hi byte = '\0' Word 9 Lo byte = '\0'
0x1500 ~ 0x1508	1 word	Port 1 to 9 bandwidth overload 0x0000: OFF 0x0001: Port X bandwidth overload
0x1600 ~ 0x1608	1 word	Port 1 to 9 loopback detection port status 0x0000: OFF 0x0001: loopback detected
Packet Information		
0x2000 ~ 0x2011	2 words	Port 1 to 9 Tx Packets Ex: Port 1 Tx Packet Amount = 0x33221100 0x2000 = 0x3322

Address Offset	Data Type	Description
		0x2001 = 0x1100
0x2100 ~ 0x2111	2 words	Port 1 to 9 Rx Packets Ex: Port 1 Rx Packet Amount = 0x33221100 0x2100 = 0x3322 0x2101 = 0x1100
0x2200 ~ 0x2211	2 words	Port 1 to 9 Tx Error Packets Ex: Port 1 Tx Packet Amount = 0x33221100 0x2200 = 0x3322 0x2201 = 0x1100
0x2300 ~ 0x2311	2 words	Port 1 to 9 Rx Error Packets Ex: Port 1 Rx Packet Amount = 0x33221100 0x2300 = 0x3322 0x2301 = 0x1100
Redundancy Information		
0x3000	1 word	Redundancy Protocol 0x0000: None 0x0001: RSTP/STP
0x3001	1 word	RSTP Root 0x0000: Not Root 0x0001: Root
0x3108	1 word	RSTP Port 1 to 9 Status 0x0000: Port Disable 0x0001: Not RSTP Port 0x0002: Link Down 0x0003: Discarding 0x0004: Learning 0x0005: Forwarding
Alarm		
0x5000	1 word	Switch cold start alarm 0x0000: OFF 0x0001: ON 0xFFFF: Disable
0x5001	1 word	Switch warm start alarm 0x0000: OFF 0x0001: ON
0x5004	1 word	Power state on alarm 0x0000: OFF 0x0001: ON
0x5005	1 word	Power state off alarm 0x0000: OFF 0x0001: ON
0x5006	1 word	DI on alarm 0x0000: OFF 0x0001: ON
0x5007	1 word	DI off alarm 0x0000: OFF 0x0001: ON

Address Offset	Data Type	Description
0x5008	1 word	authentication failure alarm 0x0000: OFF 0x0001: ON
0x5009	1 word	dot1d Bridge New Root alarm 0x0000: OFF 0x0001: ON
0x500A	1 word	dot1d Bridge Topology Changed alarm 0x0000: OFF 0x0001: ON
0x500B	1 word	LLDP Remote Tables Change alarm 0x0000: OFF 0x0001: ON
0x500C	1 word	Configuration Changed alarm 0x0000: OFF 0x0001: ON
0x500D	1 word	Firmware update alarm 0x0000: OFF 0x0001: ON
0x500E	1 word	IP changed alarm 0x0000: OFF 0x0001: ON
0x500F	1 word	Password changed alarm 0x0000: OFF 0x0001: ON
IABU Internal Data (0x2B)		
Device ID Code	**Object ID**	**Description**
0x01	0x00	Vendor Name "Delta Electronics, Inc."
	0x01	Product Code "DVS-109W02-1GE"
	0x02	Firmware Version Major.Minor Example: Major = 1, Minor = 2, Length = 4 Data byte 0: "31" Data byte 1: "." Data byte 2: "30" Data byte 3: "32"

B.3 DVS-110W02-3SFP

Address Offset	Data Type	Description
System Information		
0x0000	1 word	Reserved
0x0001	1 word	Reserved
0x0002	1 word	Reserved
0x0003	1 word	Firmware Version Hi byte = major Lo byte = minor
0x0004	2 word	Firmware Release Date Word 0 Hi byte = day Word 0 Lo byte = clock Word 1 Hi byte = year Word 1 Lo byte = month Ex: 20120918, PM9:00 Word 0 = 0x1215, Word 1 = 0x0C09
0x0010	20 words	Vendor Name = "Delta Electronics, Inc." Word 0 Hi byte = 'D' Word 0 Lo byte = 'e' Word 1 Hi byte = 'l' Word 1 Lo byte = 't' Word 2 Hi byte = 'a' Word 2 Lo byte = ' ' Word 3 Hi byte = 'E' Word 3 Lo byte = 'l' Word 4 Hi byte = 'e' Word 4 Lo byte = 'c' Word 5 Hi byte = 't' Word 5 Lo byte = 'r' Word 6 Hi byte = 'o' Word 6 Lo byte = 'n' Word 7 Hi byte = 'i' Word 7 Lo byte = 'c' Word 8 Hi byte = 's' Word 8 Lo byte = ', ' Word 9 Hi byte = ' ' Word 9 Lo byte = 'I' Word 10 Hi byte = 'n' Word 10 Lo byte = 'c' Word 11 Hi byte = '.' Word 11 Lo byte = '\0'

Address Offset	Data Type	Description
0x0030	20 words	Product Name = "DVS-110W02-3SFP" Word 0 Hi byte = 'D' Word 0 Lo byte = 'V' Word 1 Hi byte = 'S' Word 1 Lo byte = '-' Word 2 Hi byte = '1' Word 2 Lo byte = '1' Word 3 Hi byte = '0' Word 3 Lo byte = 'W' Word 4 Hi byte = '0' Word 4 Lo byte = '2' Word 5 Hi byte = '-' Word 5 Lo byte = '3' Word 6 Hi byte = 'S' Word 6 Lo byte = 'F' Word 7 Hi byte = 'P' Word 7 Lo byte ='\0'
0x0050	20 words	Serial No.
0x0070	3 words	Ethernet MAC Address Ex: MAC = 00:11:22:33:44:55 Word 0 Hi byte = 0x00 Word 0 Lo byte = '0x11 Word 1 Hi byte = 0x22 Word 1 Lo byte = 0x33 Word 2 Hi byte = 0x44 Word 2 Lo byte = '0x55
0x0073	2 words	Ethernet IP Address Ex: IP = 192.168.1.5 Word 0 = 0xC0A8 Word 1 = 0x0105
0x0075	2 words	Ethernet Netmask Ex: Mask = 255.255.255.0 Word 0 = 0xFFFF Word 1 = 0xFF00
0x0077	2 words	Ethernet Gateway IP Address Ex: IP = 192.168.1.1 Word 0 = 0xC0A8 Word 1 = 0x0101
0x0080	1 word	Power 1 Status 0x0000: OFF 0x0001: ON
0x0081	1 word	Power 2 Status 0x0000: OFF 0x0001: ON
0x0090	1 word	DO 1 Status 0x0000: OFF 0x0001: ON
0x0091	1 word	DO 2 Status 0x0000: OFF 0x0001: ON

Address Offset	Data Type	Description
0x00A0	1 word	DI 1 Status 0x0000: OFF 0x0001: ON
0x00A1	1 word	DI 2 Status 0x0000: OFF 0x0001: ON
Port Information		
0x1000 ~ 0x1009	1 word	Port 1 to 10 Status 0x0000: Link down 0x0001: Link up 0x0002: Disable
0x1100 ~ 0x1109	1 word	Port 1 to 10 Communication Format 0x0000: 10M,Half 0x0001: 10M,Full 0x0002: 100M,Half 0x0003: 100M,Full 0x0004: 1G,Full
0x1200 ~ 0x1209	1 word	Port 1 to 10 Flow Control 0x0000: OFF 0x0001: ON
0x1300 ~ 0x1309	1 word	Port 1 to 10 MDI/MDIX Setting 0x0000: Auto 0x0001: MDI 0x0002: MDIX
0x1400 ~ 0x14C7	20 words	Port 1 to 10 Description EX: 10/100/1000TX,RJ45 Word 0 Hi byte = '1' Word 0 Lo byte = '0' Word 1 Hi byte = '/' Word 1 Lo byte = '1' Word 2 Hi byte = '0' Word 2 Lo byte = '0' Word 3 Hi byte = '/' Word 3 Lo byte = '1' Word 4 Hi byte = '0' Word 4 Lo byte = '0' Word 5 Hi byte = '0' Word 5 Lo byte = 'T' Word 6 Hi byte = 'X' Word 6 Lo byte = ',' Word 7 Hi byte = 'R' Word 7 Lo byte = 'J' Word 8 Hi byte = '4' Word 8 Lo byte = '5' Word 9 Hi byte = '\0' Word 9 Lo byte = '\0'
0x1500 ~ 0x1509	1 word	Port 1 to 10 bandwidth overload 0x0000: OFF 0x0001: Port X bandwidth overload

Address Offset	Data Type	Description
Packet Information		
0x2000 ~ 0x2013	2 words	Port 1 to 10 Tx Packets Ex: Port 1 Tx Packet Amount = 0x33221100 0x2000 = 0x3322 0x2001 = 0x1100
0x2100 ~ 0x2113	2 words	Port 1 to 10 Rx Packets Ex: Port 1 Rx Packet Amount = 0x33221100 0x2100 = 0x3322 0x2101 = 0x1100
0x2200 ~ 0x2213	2 words	Port 1 to 10 Tx Error Packets Ex: Port 1 Tx Packet Amount = 0x33221100 0x2200 = 0x3322 0x2201 = 0x1100
0x2300 ~ 0x2313	2 words	Port 1 to 10 Rx Error Packets Ex: Port 1 Rx Packet Amount = 0x33221100 0x2300 = 0x3322 0x2301 = 0x1100
Redundancy Information		
0x3000	1 word	Redundancy Protocol 0x0000: None 0x0001: RSTP/STP
0x3001	1 word	RSTP Root 0x0000: Not Root 0x0001: Root
0x3100	1 word	RSTP Port 1 to 10 Status 0x0000: Port Disable 0x0001: Not RSTP Port 0x0002: Link Down 0x0003: Discarding 0x0004: Learning 0x0005: Forwarding
SPF DDM Information		
0x4000	1 word	Port 1 to Port 3 Port No.

Address Offset	Data Type	Description
0x4100	20 words	Port 8 to Port 10 Model Name Example: LCP-1250B4QDRH Word 0 Hi byte = 'L' Word 0 Lo byte = 'C' Word 1 Hi byte = 'P' Word 1 Lo byte = '-' Word 2 Hi byte = '1' Word 2 Lo byte = '2' Word 3 Hi byte = '5' Word 3 Lo byte = '0' Word 4 Hi byte = 'B' Word 4 Lo byte = '4' Word 5 Hi byte = 'Q' Word 5 Lo byte = 'D' Word 6 Hi byte = 'R' Word 6 Lo byte = 'H' Word 7 Hi byte = '\0' Word 7 Lo byte ='\0'
0x4200	2 words	Port 8 to Port 10 Temperature Word 0 = Temperature MSB Word 1 = Temperature LSB
0x4300	2 words	Port 8 to Port 10 Voltage Word 0 = Vcc MSB Word 1 = Vcc LSB
0x4400	2 words	Port 8 to Port 10 TX Power Word 0 = TX Power MSB Word 1 = TX Power LSB
0x4500	2 words	Port 8 to Port 10 RX Power Word 0 = RX Power MSB Word 1 = RX Power LSB
0x4600	1 words	Port 8 to Port 1 Link Status 0x0000: Link down 0x0001: Link up
Alarm		
0x5000	1 word	Switch cold start alarm 0x0000: OFF 0x0001: ON 0xFFFF: Disable
0x5001	1 word	Switch warm start alarm 0x0000: OFF 0x0001: ON
0x5004	1 word	Power state on alarm 0x0000: OFF 0x0001: ON
0x5005	1 word	Power state off alarm 0x0000: OFF 0x0001: ON
0x5006	1 word	DI on alarm 0x0000: OFF 0x0001: ON

Address Offset	Data Type	Description
0x5007	1 word	DI off alarm 0x0000: OFF 0x0001: ON
0x5008	1 word	authentication failure alarm 0x0000: OFF 0x0001: ON
0x5009	1 word	dot1d Bridge New Root alarm 0x0000: OFF 0x0001: ON
0x500A	1 word	dot1d Bridge Topology Changed alarm 0x0000: OFF 0x0001: ON
0x500B	1 word	LLDP Remote Tables Change alarm 0x0000: OFF 0x0001: ON
0x500C	1 word	Configuration Changed alarm 0x0000: OFF 0x0001: ON
0x500D	1 word	Firmware update alarm 0x0000: OFF 0x0001: ON
0x500E	1 word	IP changed alarm 0x0000: OFF 0x0001: ON
0x500F	1 word	Password changed alarm 0x0000: OFF 0x0001: ON
0x5100 ~ 0x5102	1 word	SFP Port 8 to Port 10 DDM Failure - Temp alarm 0x0000: OFF 0x0001: ON
0x5110 ~ 0x5112	1 word	SFP Port 8 to Port 10 DDM Failure – Voltage 0x0000: OFF 0x0001: ON
0x5120 ~ 0x5122	1 word	SFP Port 8 to Port 10 DDM Failure – Bias 0x0000: OFF 0x0001: ON
0x5130 ~ 0x5132	1 word	SFP Port 8 to Port 10 DDM Failure - TX Power 0x0000: OFF 0x0001: ON
0x5140 ~ 0x5142	1 word	SFP Port 8 to Port 10 DDM Failure - RX Power 0x0000: OFF 0x0001: ON

IABU Internal Data (0x2B)		
Device ID Code	**Object ID**	**Description**
0x01	0x00	Vendor Name "Delta Electronics, Inc."
	0x01	Product Code "DVS-110W02-3SFP"
	0x02	Firmware Version Major.Minor Example: Major = 1, Minor = 2, Length = 4 Data byte 0: "31" Data byte 1: "." Data byte 2: "30" Data byte 3: "32"

B.4 DVS-328R02-8SFP

Address Offset	Data Type	Description
System Information		
0x0000	1 word	Reserved
0x0001	1 word	Reserved
0x0002	1 word	Reserved
0x0003	1 word	Firmware Version Hi byte = major Lo byte = minor
0x0004	2 word	Firmware Release Date Word 0 Hi byte = day Word 0 Lo byte = clock Word 1 Hi byte = year Word 1 Lo byte = month Ex: 20120918, PM9:00 Word 0 = 0x1215, Word 1 = 0x0C09
0x0010	20 words	Vendor Name = "Delta Electronics, Inc." Word 0 Hi byte = 'D' Word 0 Lo byte = 'e' Word 1 Hi byte = 'l' Word 1 Lo byte = 't' Word 2 Hi byte = 'a' Word 2 Lo byte = ' ' Word 3 Hi byte = 'E' Word 3 Lo byte = 'l' Word 4 Hi byte = 'e' Word 4 Lo byte = 'c' Word 5 Hi byte = 't' Word 5 Lo byte = 'r' Word 6 Hi byte = 'o' Word 6 Lo byte = 'n' Word 7 Hi byte = 'i' Word 7 Lo byte = 'c' Word 8 Hi byte = 's' Word 8 Lo byte = ', ' Word 9 Hi byte = ' ' Word 9 Lo byte = 'l' Word 10 Hi byte = 'n' Word 10 Lo byte = 'c' Word 11 Hi byte = '.' Word 11 Lo byte = '\0'

Address Offset	Data Type	Description
0x0030	20 words	Product Name = "DVS-328R02-8SFP" Word 0 Hi byte = 'D' Word 0 Lo byte = 'V' Word 1 Hi byte = 'S' Word 1 Lo byte = '-' Word 2 Hi byte = '3' Word 2 Lo byte = '2' Word 3 Hi byte = '8' Word 3 Lo byte = 'R' Word 4 Hi byte = '0' Word 4 Lo byte = '2' Word 5 Hi byte = '-' Word 5 Lo byte = '8' Word 6 Hi byte = 'S' Word 6 Lo byte = 'F' Word 7 Hi byte = 'P' Word 7 Lo byte ='\0'
0x0050	20 words	Serial No.
0x0070	3 words	Ethernet MAC Address Ex: MAC = 00:11:22:33:44:55 Word 0 Hi byte = 0x00 Word 0 Lo byte = '0x11 Word 1 Hi byte = 0x22 Word 1 Lo byte = 0x33 Word 2 Hi byte = 0x44 Word 2 Lo byte = '0x55
0x0073	2 words	Ethernet IP Address Ex: IP = 192.168.1.5 Word 0 = 0xC0A8 Word 1 = 0x0105
0x0075	2 words	Ethernet Netmask Ex: Mask = 255.255.255.0 Word 0 = 0xFFFF Word 1 = 0xFF00
0x0077	2 words	Ethernet Gateway IP Address Ex: IP = 192.168.1.1 Word 0 = 0xC0A8 Word 1 = 0x0101
0x0080	1 word	Power 1 Status 0x0000: OFF 0x0001: ON
0x0081	1 word	Power 2 Status 0x0000: OFF 0x0001: ON
0x0082	1 word	Power 3 Status 0x0000: OFF 0x0001: ON
0x00A0	1 word	DI Status 0x0000: OFF 0x0001: ON

Address Offset	Data Type	Description
Port Information		
0x1000 ~ 0x101B	1 word	Port 1 to 28 Status 0x0000: Link down 0x0001: Link up 0x0002: Disable
0x1100 ~ 0x111B	1 word	Port 1 to 28 Communication Format 0x0000: 10M,Half 0x0001: 10M,Full 0x0002: 100M,Half 0x0003: 100M,Full 0x0004: 1G,Full
0x1200 ~ 0x121B	1 word	Port 1 to 28 Flow Control 0x0000: OFF 0x0001: ON
0x1300 ~ 0x131B	1 word	Port 1 to 28 MDI/MDIX Setting 0x0000: Auto 0x0001: MDI 0x0002: MDIX
0x1500 ~ 0x151B	1 word	Port 1 to 28 bandwidth overload 0x0000: OFF 0x0001: Port X bandwidth overload
0x1600 ~ 0x161B	1 word	Port 1 to 28 loopback detection port status 0x0000: OFF 0x0001: Port X bandwidth overload
0x1A00 ~ 0x1C30	20 words	Port 1 to 28 Description EX: 10/100/1000TX,RJ45 Word 0 Hi byte = '1' Word 0 Lo byte = '0' Word 1 Hi byte = '/' Word 1 Lo byte = '1' Word 2 Hi byte = '0' Word 2 Lo byte = '0' Word 3 Hi byte = '/' Word 3 Lo byte = '1' Word 4 Hi byte = '0' Word 4 Lo byte = '0' Word 5 Hi byte = '0' Word 5 Lo byte = 'T' Word 6 Hi byte = 'X' Word 6 Lo byte = ',' Word 7 Hi byte = 'R' Word 7 Lo byte = 'J' Word 8 Hi byte = '4' Word 8 Lo byte = '5' Word 9 Hi byte = '\0' Word 9 Lo byte = '\0'
Packet Information		
0x2000 ~ 0x2037	2 words	Port 1 to 28 Tx Packets Ex: Port 1 Tx Packet Amount = 0x33221100 0x2000 = 0x3322

Address Offset	Data Type	Description
		0x2001 = 0x1100
0x2100 ~ 0x2137	2 words	Port 1 to 28 Rx Packets Ex: Port 1 Rx Packet Amount = 0x33221100 0x2100 = 0x3322 0x2101 = 0x1100
0x2200 ~ 0x2237	2 words	Port 1 to 28 Tx Error Packets Ex: Port 1 Tx Packet Amount = 0x33221100 0x2200 = 0x3322 0x2201 = 0x1100
0x2300 ~ 0x2337	2 words	Port 1 to 28 Rx Error Packets Ex: Port 1 Rx Packet Amount = 0x33221100 0x2300 = 0x3322 0x2301 = 0x1100
Redundancy Information		
0x3000	1 word	Redundancy Protocol 0x0000: None 0x0001: RSTP/STP
0x3001	1 word	RSTP Root 0x0000: Not Root 0x0001: Root
0x3100 ~ 0x311B	1 word	RSTP Port 1 to 28 Status 0x0000: Port Disable 0x0001: Not RSTP Port 0x0002: Link Down 0x0003: Discarding 0x0004: Learning 0x0005: Forwarding
0x3200	1 word	RING mode 0x00: None (Disable) 0x01: Master 0x02: Slave
0x3201	1 word	RING state RING function is disable: 0x00: None RING Mode is Master: 0x00: Discover 0x01: Monitor 0x02: Fault RING Mode is Slave: 0x00: Forwarding 0x01: Hold 0x02: Fault
0x3300	1 word	COUPLING mode 0x00: None (Disable) 0x01: Head 0x02: Tail
0x3301	1 word	COUPLING state COUPING mode is disable: 0x00: None

Address Offset	Data Type	Description
		COUPING mode is Head: 0x00: Monitor 0x01: Fault 0x02: Link-Up 0x03: Hold COUPING mode is Tail 0x00: Discover 0x01: Monitor 0x02: Fault
0x3400	1 word	CHAIN mode 0x00: None (Disable) 0x01: Head 0x02: Tail 0x03: Member
0x3401	1 word	CHAIN state CHAIN mode is disable: 00: None CHAIN mode is Head: 0x00: Discover 0x01: Monitor 0x02: Fault 0x03: Holde CHAIN mode is Member: 0x00: Forwarding 0x01: Hold CHAIN mode is Tail: 0x00: Discover 0x01: Monitor 0x02: Fault
SPF DDM Information		
0x4000 ~ 0x4007	1 word	Port 21 to Port 28 Port No.
0x4100 ~ 0x419F	20 words	Port 1 to Port 3 Model Name Example: LCP-1250B4QDRH Word 0 Hi byte = 'L' Word 0 Lo byte = 'C' Word 1 Hi byte = 'P' Word 1 Lo byte = '-' Word 2 Hi byte = '1' Word 2 Lo byte = '2' Word 3 Hi byte = '5' Word 3 Lo byte = '0' Word 4 Hi byte = 'B' Word 4 Lo byte = '4' Word 5 Hi byte = 'Q' Word 5 Lo byte = 'D' Word 6 Hi byte = 'R' Word 6 Lo byte = 'H' Word 7 Hi byte = '\0' Word 7 Lo byte ='\0'

Address Offset	Data Type	Description
0x4200 ~ 0x420F	2 words	Port 21 to Port 28 Temperature Word 0 = Temperature MSB Word 1 = Temperature LSB
0x4300 ~ 0x430F	2 words	Port 21 to Port 28 Voltage Word 0 = Vcc MSB Word 1 = Vcc LSB
0x4400 ~ 0x440F	2 words	Port 21 to Port 28 TX Power Word 0 = TX Power MSB Word 1 = TX Power LSB
0x4500 ~ 0x450F	2 words	Port 21 to Port 28 RX Power Word 0 = RX Power MSB Word 1 = RX Power LSB
0x4600 ~ 0x460F	1 words	Port 21 to Port 28 Link Status 0x0000: Link down 0x0001: Link up
Alarm		
0x5000	1 word	Switch cold start alarm 0x0000: OFF 0x0001: ON 0xFFFF: Disable
0x5001	1 word	Switch warm start alarm 0x0000: OFF 0x0001: ON
0x5004	1 word	Power state on alarm 0x0000: OFF 0x0001: ON
0x5005	1 word	Power state off alarm 0x0000: OFF 0x0001: ON
0x5006	1 word	DI on alarm 0x0000: OFF 0x0001: ON
0x5007	1 word	DI off alarm 0x0000: OFF 0x0001: ON
0x5008	1 word	authentication failure alarm 0x0000: OFF 0x0001: ON
0x5009	1 word	dot1d Bridge New Root alarm 0x0000: OFF 0x0001: ON
0x500A	1 word	dot1d Bridge Topology Changed alarm 0x0000: OFF 0x0001: ON
0x500B	1 word	LLDP Remote Tables Change alarm 0x0000: OFF 0x0001: ON

Address Offset	Data Type	Description
0x500C	1 word	Configuration Changed alarm 0x0000: OFF 0x0001: ON
0x500D	1 word	Firmware update alarm 0x0000: OFF 0x0001: ON
0x500E	1 word	IP changed alarm 0x0000: OFF 0x0001: ON
0x500F	1 word	Password changed alarm 0x0000: OFF 0x0001: ON
0x5010	1 word	RING failure 0x0000: OFF 0x0001: ON
0x5011	1 word	RING backup path is activated 0x0000: OFF 0x0001: ON
0x5012	1 word	RING returns to health status 0x0000: OFF 0x0001: ON
0x5013	1 word	CHAIN failure 0x0000: OFF 0x0001: ON
0x5014	1 word	CHAIN backup path is activated 0x0000: OFF 0x0001: ON
0x5015	1 word	CHAIN returns to health status 0x0000: OFF 0x0001: ON
0x5016	1 word	COUPLING failure 0x0000: OFF 0x0001: ON
0x5017	1 word	COUPLING backup path is activated 0x0000: OFF 0x0001: ON
0x5018	1 word	COUPLING returns to health status 0x0000: OFF 0x0001: ON
0x5100 ~ 0x5107	1 word	SFP Port 21 to Port 28 DDM Failure - Temp alarm 0x0000: OFF 0x0001: ON
0x5110 ~ 0x5117	1 word	SFP Port 21 to Port 28 DDM Failure – Voltage 0x0000: OFF 0x0001: ON
0x5120 ~ 0x5127	1 word	SFP Port 21 to Port 28 DDM Failure – Bias 0x0000: OFF 0x0001: ON

Address Offset	Data Type	Description
0x5130 ~ 0x5137	1 word	SFP Port 21 to Port 28 DDM Failure - TX Power 0x0000: OFF 0x0001: ON
0x5140 ~ 0x5147	1 word	SFP Port 21 to Port 28 DDM Failure - RX Power 0x0000: OFF 0x0001: ON
IABU Internal Data (0x2B)		
Device ID Code	**Object ID**	**Description**
0x01	0x00	Vendor Name "Delta Electronics, Inc."
	0x01	Product Code "DVS-328R02-8SFP"
	0x02	Firmware Version Major.Minor Example: Major = 1, Minor = 2, Length = 4 Data byte 0: "31" Data byte 1: "." Data byte 2: "30" Data byte 3: "32"

Appendix C EtherNet/IP

Table of Contents

C.1 DVS-108W02-2SFP

Identity Object (0x01)

Class Attributes				
Attr ID	**Access rule**	**Name**	**Data type**	**Description of attribute**
1	Get	Revision	UINT	Revision of this object
2	Get	Max Instance	UINT	Maximum instance number of this object
Instance Attributes				
Attr ID	**Access rule**	**Name**	**Data type**	**Description of attribute**
1	Get	Vendor ID	UINT	799, Vendor ID of "Delta Electronics, Inc."
2	Get	Device Type	UINT	0x2C, "Managed Ethernet Switch Device".
3	Get	Product Code	UINT	Product code of device.
4	Get	Revision	STRUCT of:	Revision of the Identity Object
		Major	USINT	
		Minor	USINT	
5	Get	Status	WORD	0, Not used
6	Get	Serial Number	UDINT	Serial number of device
7	Get	Product Name	STRING	"DVS-108W02-2SFP", Product name of device.
Common Services				
Service Code	**Need in Implementation**		**Service name**	**Description of Service**
	Class	**Instance**		
0x01		V	Get_Attribute_All	Returns a predefined listing of this objects attributes.
0x05		V	Reset	Invokes the reset service for the device.
0x0E	V	V	Get_Attribute_Single	Returns the contents of the specified attribute.

Message Router Object (0x02)

Class Attributes				
Attr ID	**Access rule**	**Name**	**Data type**	**Description of attribute**
1	Get	Revision	UINT	Revision of this object
Instance Attributes				
Attr ID	**Access rule**	**Name**	**Data type**	**Description of attribute**
2	Get	Number Available	UINT	Maximum number of CIP connections supported
3	Get	Number Active	UINT	Number of CIP connections currently used by system components
Common Services				
Service Code	**Need in Implementation**		**Service name**	**Description of Service**
	Class	**Instance**		
0x0E	V	V	Get_Attribute_Single	Returns the contents of the specified attribute.

Assembly Object (0x04)

Class Attributes				
Attr ID	**Access rule**	**Name**	**Data type**	**Description of attribute**
1	Get	Revision	UINT	Revision of this object
Instance Attributes				
Attr ID	**Access rule**	**Name**	**Data type**	**Description of attribute**
3	Get/Set	Data	ARRAY of BYTE	
4	Get	Size	UINT	
Instance				
Instance Number	**Size (bytes)**	**Name**	**Type**	**Description of attribute**
1	18	Power Source and Link Status	Inupt	Refer to Base Switch Object Attr ID 4 Byte 0: Power Source Status (Least Significant Byte) Byte 1: Power Source Status (Most Significant Byte) Refer to Base Switch Object Attr ID 8 Byte 2-5: Global Link Status DWORD 0 Byte 6-9: Global Link Status DWORD 1 Byte 10-13: Global Link Status DWORD 2 Byte 14-17: Global Link Status DWORD 3
2	16	Global Admin State	Input	Refer to Base Switch Object Attr ID 7 Byte 0-3: Global Admin Status DWORD 0 Byte 4-7: Global Admin Status DWORD 1 Byte 8-11: Global Admin Status DWORD 2 Byte 12-15: Global Admin Status DWORD 3
3	2	Contact Status	Input	Refer to Base Switch Object Attr ID 10 Byte 0: Contact Status (Least Significant Byte) Byte 1: Contact Status (Most Significant Byte)
50	16	Port Admin State	Output	Refer to Base Switch Object Attr ID 7 Byte 0-3: Global Admin Status DWORD 0 Byte 4-7: Global Admin Status DWORD 1 Byte 8-11: Global Admin Status DWORD 2 Byte 12-15: Global Admin Status DWORD 3
64	75	Device Status	Input	Refer to I/O Assembly Connection 4 - Input

Common Services				
Service Code	**Need in Implementation**		**Service name**	**Description of Service**
	Class	**Instance**		
0x0E	V	V	Get_Attribute_Single	Returns the contents of the specified attribute.
0x10		V	Set_Attribute_Single	Modifies an attribute value.
I/O Assembly				
Connection1				
	Instance	**Size(SINT)**	**Description**	
Input	1	18	Please refer to Assembly Object Attr ID 1.	
Output	50	16	Please refer to Assembly Object Attr ID 50.	
Configuration	64	0		
Connection2				
	Instance	**Size(SINT)**	**Description**	
Input	2	16	Please refer to Assembly Object Attr ID 2.	
Output	50	16	Please refer to Assembly Object Attr ID 50.	
Configuration	64	0		
Connection3				
	Instance	**Size(SINT)**	**Description**	
Input	3	2	Please refer to Assembly Object Attr ID 2.	
Output	50	16	Please refer to Assembly Object Attr ID 50	
configuration	64	0		
Connection4				
	Instance	**Size(SINT)**	**Description**	
Input	64	2	Please refer to Assembly Object Attr ID 3	
Output	50	16	Please refer to Assembly Object Attr ID 50	
configuration	80	0		
Direction	**Name**	**Size(SINT)**	**Description**	
Input	Power Source Status	WORD	Refer to Base Switch Object Attr ID 4 Power Source Status (Least Significant Byte) Power Source Status (Most Significant Byte)	
	Global Link Status	ARRAY OF DWORD	Refer to Base Switch Object Attr ID 8 Global Link Status DWORD 0 Global Link Status DWORD 1 Global Link Stauts DWORD 2 Global Link Status DWORD 3	
	Global Admin State	ARRAY OF DWORD	Refer to Base Switch Object Attr ID 7 Global Admin Status DWORD 0 Global Admin Status DWORD 1 Global Admin Stauts DWORD 2 Global Admin Status DWORD 3	
	Contact Status	WORD	Refer to Base Switch Object Attr ID 10	
	AlarmStatus	ULINT	Refer to Delta IES Object Attr 11	
	Bandwidth overload	ULINT	Refer to Delta IES Object Attr 12	
	Loopback detection port status	ULINT	Refer to Delta IES Object Attr 13	
	SFP Failure	ARRAY OF USINT	Refer to Delta IES Object Attr 14	
	Redundancy Protocol	USINT	Refer to Delta IES Object Attr 15	
	RSTP Root	USINT	Refer to Delta IES Object Attr 16	
	Redundancy - RING Mode	USINT	Refer to Delta IES Object Attr 17	

Direction	Name	Size(SINT)	Description
Input	Redundancy - Ring State	USINT	Refer to Delta IES Object Attr 18
Input	Redundancy - CHAIN State	USINT	Refer to Delta IES Object Attr 19
	Redundancy - COUPING Mode	USINT	Refer to Delta IES Object Attr 20
	Redundancy - COUPING State	USINT	Refer to Delta IES Object Attr 21
Output	Port Admin State	ARRAY OF DWORD	Refer to Base Switch Object Attr ID 7 Global Admin Status DWORD 0 Global Admin Status DWORD 1 Global Admin Stauts DWORD 2 Global Admin Status DWORD 3

Connection Manager Object (0x06)

Class Attributes				
Attr ID	**Access rule**	**Name**	**Data type**	**Description of attribute**
1	Get	Revision	UINT	Revision of this object
Instance Attributes				
Attr ID	**Access rule**	**Name**	**Data type**	**Description of attribute**
Common Services				
Service Code	**Need in Implementation**		**Service name**	**Description of Service**
	Class	**Instance**		
0x0E	V	V	Get_Attribute_Single	Returns the contents of the specified attribute.
0x4E		V	Forward_Close	Closes a connection
0x54		V	Forward_Open	Open a connection

Port Object (0xF4)

Class Attributes				
Attr ID	**Access rule**	**Name**	**Data type**	**Description of attribute**
1	Get	Revision	UINT	Revision of this object
2	Get	Max Instance	UINT	Maximum instance number.
3	Get	Num Instances	UINT	Number of port currently instantiated.
8	Get	Entry Port	UINT	Returns the port through which this request entered the device.
9	Get	Port Instance Info	ARRAY of STRUCT of	
		Port Type	UINT	Enumerates the type of port.
		Port Number	UINT	CIP port number associated with this port
Instance Attributes				
Attr ID	**Access rule**	**Name**	**Data type**	**Description of attribute**
1	Get	Port Type	UINT	Enumerates the type. (4=EthetNet/IP)
2	Get	Port Number	UINT	CIP port number associated with this port.
3	Get	Link Object	STRUCT of	
		Path Length	UINT	Number of 16 bit words in the following path.
		Link Path	Padded EPATH	Logical path segments that identify the object for this port.
4	Get	Port Name	SHORT_STRING	String which names the physical network port
7	Get	Node Address	Padded EPATH	Node number of this device on port.

Common Services				
Service Code	**Need in Implementation**		**Service name**	**Description of Service**
	Class	**Instance**		
0x0E	V	V	Get_Attribute_Single	Returns the contents of the specified attribute.

TCP/IP Interface Object (0xF5)

Class Attributes				
Attr ID	**Access rule**	**Name**	**Data type**	**Description of attribute**
1	Get	Revision	UINT	Revision of this object
Instance Attributes				
Attr ID	**Access rule**	**Name**	**Data type**	**Description of attribute**
1	Get	Status	DWORD	Interface status 0=The Interface Configuration attribute has not been configured. 1=The Interface Configuration attribute contains configuration obtained from BOOTP, DHCP or non-volatile storage.
2	Get	Configuration Capability	DWORD	Interface capability Bit 0: BOOTP Client 1 (TRUE) shall indicate the device is capable of obtaining its network configuration via BOOTP. Bit 1: DNS Client 1 (TRUE) shall indicate the device is capable of resolving host names by querying a DNS server. Bit 2: DHCP Client 1 (TRUE) shall indicate the device is capable of obtaining its network configuration via DHCP. Bit 3: DHCP-DNS Update Shall be 0 Bit 4: Configuration Settable 1 (TRUE) shall indicate the Interface Configuration attribute is settable.
3	Get/Set	Configuration Control	DWORD	Interface control flags Bit 0-3: Configuration Method 0=The device shall use statically-assigned IP configuration values. 1=The device shall obtain its interface configuration values via BOOTP. 2=The device shall obtain its interface configuration values via DHCP. 3-15=Reserved for future use. Bit 4: DNS Enable If 1 (TRUE), the device shall resolve host names by querying a DNS server.
4	Get	Physical Link Object	STRUCT of	Path to physical link object.
		Path size	UINT	Size of Path.
		Path	Padded EPATH	Logical segments identifying the physical link object.

Attr ID	Access rule	Name	Data type	Description of attribute
5	Get/Set	Interface Configuration	STRUCT of	TCP/IP network interface configuration.
		IP Address	UDINT	The device's IP address.
		Network Mask	UDINT	The device's network mask
		Gateway Address	UDINT	Default gateway address
		Name Server	UDINT	Primary name server
		Name Server 2	UDINT	Secondary name server
		Domain Name	STRING	Default domain name Note: ASCII characters. Maximum length is 48 characters. Shall be padded to an even number of characters (pad not included in length).
6	Get/Set	Host Name	STRING	Host Name (Note: ASCII characters. Maximum length is 64 characters. Shall be padded to an even number of characters (pad not included in length).

Common Services				
Service Code	**Need in Implementation**		**Service name**	**Description of Service**
	Class	**Instance**		
0x0E	V	V	Get_Attribute_Single	Returns the contents of the specified attribute.
0x10		V	Set_Attribute_Single	Modifies an attribute value.

Ethernet Link Object (0xF6)

Class Attributes				
Attr ID	**Access rule**	**Name**	**Data type**	**Description of attribute**
1	Get	Revision	UINT	Revision of this object
2	Get	Max Instance	UINT	Maximum instance number of an object currently created in this class level of the device.
3	Get	Number of Instances	UINT	Number of object instances currently created at this class level of the device. (The value is mapping the number of ports in Switch device)
Instance Attributes				
Attr ID	**Access rule**	**Name**	**Data type**	**Description of attribute**
1	Get	Interface Speed	UDINT	Interface speed currently in use Speed in Mbps (e.g., 0, 10, 100, 1000, etc.)
2	Get	Interface Flags	DWORD	Interface status flags
3	Get	Physical Address	ARRAY of 6 USINTs	MAC layer address
4	Get	Interface Counters	STRUCT of:	
		In Octets	UDINT	Octets received on the interface
		In Ucast Packets	UDINT	Unicast packets received on the interface
		In Nucast Packets	UDINT	Non-unicast packets received on the interface
		In Discards	UDINT	Inbound packets received on the interface but discarded
		In Errors	UDINT	Inbound packets that contain errors (does not include In Discards)

Attr ID	Access rule	Name	Data type	Description of attribute
4	Get	In Unknown Protos	UDINT	Inbound packets with unknown protocol
		Out Octets	UDINT	Octets sent on the interface
		Out Ucast Packets	UDINT	Unicast packets sent on the interface
		Out Nucast Packets	UDINT	Non-unicast packets sent on the interface
		Out Discards	UDINT	Outbound packets discarded
		Out Errors	UDINT	Outbound packets that contain errors
5	Get	Media Counters	STRUCT of:	Media-specific counters
		Alignment Errors	UDINT	Frames received that are not an integral number of octets in length
		FCS Errors	UDINT	Frames received that do not pass the FCS check
		Single Collisions	UDINT	Successfully transmitted frames which experienced exactly one collision
		Multiple Collisions	UDINT	Successfully transmitted frames which experienced more than one collision
		SQE Test Errors	UDINT	Number of times SQE test error message is generated
		Deferred Transmissions	UDINT	Frames for which first transmission attempt is delayed because the medium is busy
		Late Collisions	UDINT	Number of times a collision is detected later than 512 bit-times into the transmission of a packet
		Excessive Collisions	UDINT	Frames for which transmission fails due to excessive collisions
		MAC Transmit Errors	UDINT	Frames for which transmission fails due to an internal MAC sublayer transmit error
		Carrier Sense Errors	UDINT	Times that the carrier sense condition was lost or never asserted when attempting to transmit a frame
		Frame Too Long	UDINT	Frames received that exceed the maximum permitted frame size
		MAC Receive Errors	UDINT	Frames for which reception on an interface fails due to an internal MAC sublayer receive error
10	Get	Interface Label	SHORT_STRING	Human readable identification
Common Services				

Service Code	Need in Implementation		Service name	Description of Service
	Class	Instance		
0x0E	V	V	Get_Attribute_Single	Returns the contents of the specified attribute.

Base Switch Object (0x51)

Class Attributes				
Attr ID	**Access rule**	**Name**	**Data type**	**Description of attribute**
1	Get	Revision	UINT	Revision of this object. The current value assigned to this values is 1

Instance Attributes				
Attr ID	**Access rule**	**Name**	**Data type**	**Description of attribute**
1	Get	Device Up Time	UDINT	Time since device was powered up (s) (Note: the value is 32-bit)
2	Get	Total port count	UDINT	Number of physical ports
3	Get	System Firmware Version	SHORT_STRING	Human readable representation of System Firmware Version (Note: ASCII characters, max length is 32 bytes)
4	Get	Power Source	WORD	Status of switch power source Bit 0-1: Power Source 1 Bit 2-3: Power Source 2…. Bit 14-15: Power Source 8 00=Not Present (power source not present in switch) 01=Not Powered (power source present but not powered) 10=Faulted (power source present but faulted) 11=Powered and ok (power source present, powered and OK)
5	Get	Port Mask Size	UINT	Number of DWORDs in port array attributes (Minimum=4, supporting 128 ports)
7	Get / Set	Global Port Admin State	ARRAY OF DWORD	Port Admin Status (Note: Size of array=attribute 5) DWORD[0]: Port 0 - 31 admin status DWORD[1]: Port 32 - 63 admin status DWORD[2]: Port 64 - 95 admin status DWORD[3]: Port 96 - 127 admin status 0=Port (or Interface) Enabled 1=Port (or Interface) Disabled
8	Get	Global Port Link Status	ARRAY OF DWORD	Port Link Status (Note: Size of array=attribute 5) DWORD[0]: Port 0 - 31 link status DWORD[1]: Port 32 - 63 link status DWORD[2]: Port 64 - 95 link status DWORD[3]: Port 96 - 127 link status 0=Link inactive (Down) 1=Link Active (UP)
10	Get	Contact Status	WORD	Switch Contact Closure (DI) Bit 0-1: Switch Contact 1 (DI 1) Bit 2-3: Switch Contact 2 (DI 2) Other Reserved (should be 0) 00=Switch Contact not support/pressed 01=Switch Contact is OPEN (OFF) 10=Switch Contact is CLOSED (ON) 11=Reserved

Common Services				
Service Code	**Need in Implementation**		**Service name**	**Description of Service**
	Class	**Instance**		
0x0E	V	V	Get_Attribute_Single	Returns the contents of the specified attribute.
0x10		V	Set_Attribute_Single	Modifies an attribute value.

Delta IES Object (0x64)

Class Attributes				
Attr ID	**Access rule**	**Name**	**Data type**	**Description of attribute**
1	Get	Revision	UINT	Revision of this object
Instance Attributes				
Attr ID	**Access rule**	**Name**	**Data type**	**Description of attribute**
1	Get/Set	Reboot Device	USINT	Reboot device Set 0x0001 to reboot device, and return to 0x0000 if reboot is completed.
2	Get/Set	Reset Device	USINT	Reset to default Set 0x0001 to reset configuration, and return to 0x0000 if reset is completed.
3	Get	Firmware Release Date	UDINT	Ex: 20120918, PM9:00 Word 0=0x1215, Word 1=0x0C09
4	Get	Relay Output Status	WORD	Relay Output Status Bit 0-1: Relay Output 1 status Bit 2-3: Relay Output 2 status Other Reserved (should be 0) 00=Digital output not support/pressed 01=Switch Contact is OPEN (OFF) 10=Switch Contact is CLOSED (ON) 11=Reserved
11	Get	Alarm Status	ULINT	Alarm Status (0 is ON, 1 is OFF) Bit 0: switch code start Bit 1: switch warm start Bit 2: power1 state on->off Bit 3: power1 state off->on Bit 4: power2 state on->off Bit 5: power2 state off->on Bit 6: DI1 state on->off Bit 7: DI1 state off->on Bit 8: DI2 state on->off Bit 9: DI2 state off->on Bit 10: authentication failure Bit 11: dot1d Bridge New Root Bit 12: dot1d Bridge Topology Changed Bit 13: LLDP Remote Tables Changed Bit 14: configuration changed Bit 15: firmware update Bit 16: IP changed Bit 17: password changed
12	Get	Bandwidth overload	ULINT	Bit 0: Port 0 state Bit 1: Port 1 state…. Bit 63: Port 63 state 0=OFF or not support 1=Bandwidth overload
13	Get	Loopback detection port status	ULINT	Bit 0: Port 0 state Bit 1: Port 1 state…. Bit 63: Port 63 state 0=OFF or not support 1=Loopback detected
15	Get	Redundancy Protocol	USINT	0x0000: None x0001: RSTP/STP

16	Get	RSTP Root	USINT	0x0000: Not Root 0x0001: Root
17	Get	Redundancy - RING Mode	USINT	0x00: None (Disable) 0x01: Master 0x02: Slave
18	Get	Redundancy - Ring State	USINT	RING function is disable: 0x00: None RING Mode is Master: 0x00: Discover 0x01: Monitor 0x02: Fault RING Mode is Slave: 0x00: Forwarding 0x01: Hold 0x02: Fault
19	Get	Redundancy - CHAIN State	USINT	0x00: None 0x01: The chain failure is happened.
20	Get	Redundancy - COUPING Mode	USINT	0x00: None (Disable) 0x01: Head 0x02: Tail
21	Get	Redundancy - COUPING State	USINT	COUPING mode is Head: 0x00: Monitor 0x01: Fault 0x02: Link-Up 0x03: Hold COUPING mode is Tail 0x00: Discover 0x01: Monitor 0x02: Fault

Common Services

Service Code	Need in Implementation		Service name	Description of Service
	Class	Instance		
0x0E	V	V	Get_Attribute_Single	Returns the contents of the specified attribute.
0x10		V	Set_Attribute_Single	Modifies an attribute value.

C.2 DVS-109W02-1GE

Identity Object (0x01)

Class Attributes				
Attr ID	Access Rule	Name	Data Type	Description of Attribute
1	Get	Revision	UINT	Revision of this object
2	Get	Max Instance	UINT	Maximum instance number of this object

Instance Attributes				
Attr ID	Access Rule	Name	Data Type	Description of Attribute
1	Get	Vendor ID	UINT	799, Vendor ID of "Delta Electronics, Inc. "
2	Get	Device Type	UINT	0x2C, "Managed Ethernet Switch Device".
3	Get	Product Code	UINT	Product code of device.
4	Get	Revision	STRUCT of:	Revision of the Identity Object
		Major	USINT	
		Minor	USINT	
5	Get	Status	WORD	0, Not used
6	Get	Serial Number	UDINT	Serial number of device
7	Get	Product Name	STRING	"DVS-109W02-1GE", Product name of device.

Common Services				
Service Code	Need in Implementation		Service Name	Description of Service
	Class	Instance		
0x05		V	Reset	Invokes the reset service for the device.
0x0E	V	V	Get_Attribute_Single	Returns the contents of the specified attribute.

Message Router Object (0x02)

Class Attributes				
Attr ID	Access Rule	Name	Data Type	Description of Attribute
1	Get	Revision	UINT	Revision of this object

Instance Attributes				
Attr ID	Access Rule	Name	Data Type	Description of Attribute
2	Get	Number Available	UINT	Maximum number of CIP connections supported
3	Get	Number Active	UINT	Number of CIP connections currently used by system components

Common Services				
Service Code	Need in Implementation		Service Name	Description of Service
	Class	Instance		

0x0E	V	V	Get_Attribute_Single	Returns the contents of the specified attribute.

Assembly Object (0x04)

Class Attributes				
Attr ID	Access Rule	Name	Data Type	Description of Attribute
1	Get	Revision	UINT	Revision of this object
Instance Attributes				
Attr ID	Access Rule	Name	Data Type	Description of Attribute
3	Get/Set	Data	ARRAY of BYTE	
4	Get	Size	UINT	
Instance				
Instance Number	Size (bytes)	Name	Type	Description of Attribute
1	18	Power Source and Link Status	Inupt	Refer to Base Switch Object Attr ID 4 Byte 0: Power Source Status (Least Significant Byte) Byte 1: Power Source Status (Most Significant Byte) Refer to Base Switch Object Attr ID 8 Byte 2-5: Global Link Status DWORD 0 Byte 6-9: Global Link Status DWORD 1 Byte 10-13: Global Link Stauts DWORD 2 Byte 14-17: Global Link Status DWORD 3
2	16	Global Admin State	Input	Refer to Base Switch Object Attr ID 7 Byte 0-3: Global Admin Status DWORD 0 Byte 4-7: Global Admin Status DWORD 1 Byte 8-11: Global Admin Stauts DWORD 2 Byte 12-15: Global Admin Status DWORD 3
3	2	Contact Status	Input	Refer to Base Switch Object Attr ID 10 Byte 0: Contact Status (Least Signifcant Byte) Byte 1: Contact Status (Most Signifcant Byte)

Instance Number	Size (bytes)	Name	Type	Description of Attribute
50	16	Port Admin State	Output	Refer to Base Switch Object Attr ID 7 Byte 0-3: Global Admin Status DWORD 0 Byte 4-7: Global Admin Status DWORD 1 Byte 8-11: Global Admin Stauts DWORD 2 Byte 12-15: Global Admin Status DWORD 3
64	75	Device Status	Input	Refer to I/O Assembly Connection 4 - Input

Common Services

Service Code	Need in Implementation		Service Name	Description of Service
	Class	Instance		
0x0E	V	V	Get_Attribute_Single	Returns the contents of the specified attribute.
0x10		V	Set_Attribute_Single	Modifies an attribute value.

I/O Assembly

Connection1

	Instance	Size(SINT)	Description
Input	1	18	Please refer to Assembly Object Attr ID 1.
Output	50	16	Please refer to Assembly Object Attr ID 50.
Configuration	64	0	

Connection2

	Instance	Size(SINT)	Description
Input	2	16	Please refer to Assembly Object Attr ID 2.
Output	50	16	Please refer to Assembly Object Attr ID 50.
Configuration	64	0	

Connection3

	Instance	Size(SINT)	Description
Input	3	2	Please refer to Assembly Object Attr ID 2.
Output	50	16	Please refer to Assembly Object Attr ID 50
configuration	64	0	

Connection4

	Instance	Size(SINT)	Description
Input	64	2	Please refer to Assembly Object Attr ID 2.
Output	50	16	Please refer to Assembly Object Attr ID 50
configuration	80	0	

Direction	Name	Size(SINT)	Description
Input	Power Source Status	WORD	Refer to Base Switch Object Attr ID 4 Power Source Status (Least Significant Byte) Power Source Status (Most Significant Byte)
	Global Link Status	ARRAY OF DWORD	Refer to Base Switch Object Attr ID 8 Global Link Status DWORD 0 Global Link Status DWORD 1 Global Link Stauts DWORD 2 Global Link Status DWORD 3
	Global Admin State	ARRAY OF DWORD	Refer to Base Switch Object Attr ID 7 Global Admin Status DWORD 0 Global Admin Status DWORD 1 Global Admin Stauts DWORD 2 Global Admin Status DWORD 3
	Contact Status	WORD	Refer to Base Switch Object Attr ID 10
	AlarmStatus	ULINT	Refer to Delta IES Object Attr 11
	Bandwidth overload	ULINT	Refer to Delta IES Object Attr 12
	Loopback detection port status	ULINT	Refer to Delta IES Object Attr 13
	SFP Failure	ARRAY OF USINT	Refer to Delta IES Object Attr 14
	Redundancy Protocol	USINT	Refer to Delta IES Object Attr 15
	RSTP Root	USINT	Refer to Delta IES Object Attr 16
	Redundancy - RING Mode	USINT	Refer to Delta IES Object Attr 17
	Redundancy - Ring State	USINT	Refer to Delta IES Object Attr 18
	Redundancy - CHAIN State	USINT	Refer to Delta IES Object Attr 19
	Redundancy - COUPING Mode	USINT	Refer to Delta IES Object Attr 20
	Redundancy - COUPING State	USINT	Refer to Delta IES Object Attr 21
Output	Port Admin State	ARRAY OF DWORD	Refer to Base Switch Object Attr ID 7 Global Admin Status DWORD 0 Global Admin Status DWORD 1 Global Admin Stauts DWORD 2 Global Admin Status DWORD 3

Connection Manager Object (0x06)

Class Attributes				
Attr ID	Access Rule	Name	Data Type	Description of Attribute
1	Get	Revision	UINT	Revision of this object
Instance Attributes				
Attr ID	Access Rule	Name	Data Type	Description of Attribute
Common Services				
Service Code	Need in Implementation		Service Name	Description of Service
	Class	Instance		
0x0E	V	V	Get_Attribute_Single	Returns the contents of the specified attribute.

Service Code	Need in Implementation		Service Name	Description of Service
	Class	Instance		
0x4E		V	Forward_Close	Closes a connection
0x54		V	Forward_Open	Open a connection

Port Object (0xF4)

Class Attributes				
Attr ID	Access Rule	Name	Data Type	Description of Attribute
1	Get	Revision	UINT	Revision of this object
2	Get	Max Instance	UINT	Maximum instance number.
3	Get	Num Instances	UINT	Number of port currently instantiated.
8	Get	Entry Port	UINT	Returns the port through which this request entered the device.
9	Get	Port Instance Info	ARRAY of STRUCT of	
		Port Type	UINT	Enumerateds the type of port.
		Port Number	UINT	CIP port number associated with this port
Instance Attributes				
Attr ID	Access Rule	Name	Data Type	Description of Attribute
1	Get	Port Type	UINT	Enumerates the type. (4 = EthetNet/IP)
2	Get	Port Number	UINT	CIP port number associated with this port.
3	Get	Link Object	STRUCT of	
		Path Length	UINT	Number of 16 bit words in the following path.
		Link Path	Padded EPATH	Logical path segments that identify the object for this port.
4	Get	Port Name	SHORT_STRING	String which names the physical network port
7	Get	Node Address	Padded EPATH	Node number of this device on port.
Common Services				
Service Code	Need in Implementation		Service Name	Description of Service
	Class	Instance		
0x0E	V	V	Get_Attribute_Single	Returns the contents of the specified attribute.

TCP/IP Interface Object (0xF5)

Class Attributes				
Attr ID	Access Rule	Name	Data Type	Description of Attribute
1	Get	Revision	UINT	Revision of this object

Instance Attributes				
Attr ID	Access Rule	Name	Data Type	Description of Attribute
1	Get	Status	DWORD	Interface status 0 = The Interface Configuration attribute has not been configured. 1 = The Interface Configuration attribute contains configuration obtained from BOOTP, DHCP or non-volatile storage.
2	Get	Configuration Capability	DWORD	Interface capability Bit 0: BOOTP Clinet 1 (TRUE) shall indicate the device is capable of obtaining its network configuration via BOOTP. Bit 1: DNS Client 1 (TRUE) shall indicate the device is capable of resolving host names by querying a DNS server. Bit 2: DHCP Client 1 (TRUE) shall indicate the device is capable of obtaining its network configuration via DHCP. Bit 3: DHCP-DNS Update Shall be 0 Bit 4: Configuration Settable 1 (TRUE) shall indicate the Interface Configuration attribute is settable.
3	Get/Set	Configuration Control	DWORD	Interface control flags Bit 0-3: Configuraiton Method 0 = The device shall use statically-assigned IP configuration values. 1 = The device shall obtain its interface configuration values via BOOTP. 2 = The device shall obtain its interface configuration values via DHCP. 3-15 = Reserved for future use. Bit 4: DNS Enable If 1 (TRUE), the device shall resolve host names

				by querying a DNS server.
4	Get	Physical Link Object	STRUCT of	Path to physical link object.
		Path size	UINT	Size of Path.
		Path	Padded EPATH	Logical segments identifying the physical link object.
5	Get/Set	Interface Configuration	STRUCT of	TCP/IP network interface configuration.
		IP Address	UDINT	The device's IP address.
		Network Mask	UDINT	The device's network mask
		Gateway Address	UDINT	Default gateway address
		Name Server	UDINT	Primary name server
		Namer Server 2	UDINT	Secondary name server
		Domain Name	STRING	Default domain name Note: ASCII characters. Maximum length is 48 characters. Shall be padded to an even number of characters (pad not included in length).
6	Get/Set	Host Name	STRING	Host Name (Note: ASCII characters. Maximum length is 64 characters. Shall be padded to an even number of characters (pad not included in length).
Common Services				
Service Code	Need in Implementation		Service Name	Description of Service
	Class	Instance		
0x0E	V	V	Get_Attribute_Single	Returns the contents of the specified attribute.
0x10		V	Set_Attribute_Single	Modifies an attribute value.

Ethernet Link Object (0xF6)

Class Attributes				
Attr ID	Access Rule	Name	Data Type	Description of Attribute
1	Get	Revision	UINT	Revision of this object
2	Get	Max Instance	UINT	Maximum instance number of an object currently created in this class level of the device.
3	Get	Number of Instances	UINT	Number of object instances currently created at this class level of the device.

				(The value is mapping the number of ports in Switch device)
Instance Attributes				
Attr ID	Access Rule	Name	Data Type	Description of Attribute
1	Get	Interface Speed	UDINT	Interface speed currently in use Speed in Mbps (e.g., 0, 10, 100, 1000, etc.)
2	Get	Interface Flags	DWORD	Interface status flags
3	Get	Physical Address	ARRAY of 6 USINTs	MAC layer address
4	Get	Interface Counters	STRUCT of:	
		In Octets	UDINT	Octets received on the interface
		In Ucast Packets	UDINT	Unicast packets received on the interface
		In Nucast Packets	UDINT	Non-unicast packets received on the interface
		In Discards	UDINT	Inbound packets received on the interface but discarded
		In Errors	UDINT	Inbound packets that contain errors (does not include In Discards)
		In Unknown Protos	UDINT	Inbound packets with unknown protocol
		Out Octets	UDINT	Octets sent on the interface
		Out Ucast Packets	UDINT	Unicast packets sent on the interface
		Out Nucast Packets	UDINT	Non-unicast packets sent on the interface
		Out Discards	UDINT	Outbound packets discarded
		Out Errors	UDINT	Outbound packets that contain errors
5	Get	Media Counters	STRUCT of:	Media-specific counters
		Alignmenet Errors	UDINT	Frames received that are not an integral number of octets in length
		FCS Errors	UDINT	Frames received that do not pass the FCS check
		Single Collisions	UDINT	Successfully transmitted frames which experienced exactly one collision
		Multiple Collisons	UDINT	Successfully transmitted frames which experienced more than one collision
		SQE Test Errors	UDINT	Number of times SQE test error message is generated

		Deferred Transmissions	UDINT	Frames for which first transmission attempt is delayed because the medium is busy
		Late Collisions	UDINT	Number of times a collision is detected later than 512 bit-times into the transmission of a packet
		Excessive Collisions	UDINT	Frames for which transmission fails due to excessive collisions
		MAC Transmit Errors	UDINT	Frames for which transmission fails due to an internal MAC sublayer transmit error
		Carrier Sense Errors	UDINT	Times that the carrier sense condition was lost or never asserted when attempting to transmit a frame
		Frame Too Long	UDINT	Frames received that exceed the maximum permitted frame size
		MAC Receive Errors	UDINT	Frames for which reception on an interface fails due to an internal MAC sublayer receive error
10	Get	Interface Label	SHORT_STRING	Human readable identification

Common Services				
Service Code	Need in Implementation		Service Name	Description of Service
	Class	Instance		
0x0E	V	V	Get_Attribute_Single	Returns the contents of the specified attribute.

Base Switch Object (0x51)

Class Attributes				
Attr ID	Access Rule	Name	Data Type	Description of Attribute
1	Get	Revision	UINT	Revision of this object. The current value assigned to this values is 1
Instance Attributes				
Attr ID	Access Rule	Name	Data Type	Description of Attribute
1	Get	Device Up Time	UDINT	Time since device was powered up (s) (Note: the value is 32-bit)
2	Get	Total port count	UDINT	Number of physical ports
3	Get	System Firmware Version	SHORT_STRING	Human readable representation of System Firmware Version (Note: ASCII characters, max

				length is 32 bytes)
4	Get	Power Source	WORD	Status of switch power source Bit 0-1: Power Source 1 Bit 2-3: Power Source 2…. Bit 14-15: Power Source 8 00 = Not Present (power source not present in switch) 01 = Not Powered (power source present but not powered) 10 = Faulted (power source present but faulted) 11 = Powered and ok (power source present, powered and OK)
5	Get	Port Mask Size	UINT	Number of DWORDs in port array attributes (Minimum = 4, supporting 128 ports)
7	Get / Set	Global Port Admin State	ARRAY OF DWORD	Port Admin Status (Note: Size of array = attribute 5) DWORD[0]: Port 0 - 31 admin status DWORD[1]: Port 32 - 63 admin status DWORD[2]: Port 64 - 95 admin status DWORD[3]: Port 96 - 127 admin status 0 = Port (or Interface) Enabled 1 = Port (or Interface) Disabled
8	Get	Global Port Link Status	ARRAY OF DWORD	Port Link Status (Note: Size of array = attribute 5) DWORD[0]: Port 0 - 31 link status DWORD[1]: Port 32 - 63 link status DWORD[2]: Port 64 - 95 link status DWORD[3]: Port 96 - 127 link status 0 = Link inactive (Down) 1 = Link Active (UP)

10	Get	Constact Status	WORD	Switch Contact Closure (DI) Bit 0-1: Switch Contact 1 (DI 1) Bit 2-3: Switch Contact 2 (DI 2) Other Reserved (should be 0) 00 = Switch Contact not support/presed 01 = Switch Contact is OPEN (OFF) 10 = Switch Contact is CLOSED (ON) 11 = Reserved

Common Services

Service Code	Need in Implementation		Service Name	Description of Service
	Class	Instance		
0x0E	V	V	Get_Attribute_Single	Returns the contents of the specified attribute.
0x10		V	Set_Attribute_Single	Modifies an attribute value.

Delta IES Object (0x64)

Class Attributes

Attr ID	Access Rule	Name	Data Type	Description of Attribute
1	Get	Revision	UINT	Revision of this object

Instance Attributes

Attr ID	Access Rule	Name	Data Type	Description of Attribute
1	Get/Set	Reboot Device	USINT	Reboot device Set 0x0001 to reboot device, and return to 0x0000 if reboot is completed.
2	Get/Set	Reset Device	USINT	Reset to default Set 0x0001 to reset configuration, and return to 0x0000 if reset is completed.
3	Get	Firmware Release Date	UDINT	Ex: 20120918, PM9:00 Word 0 = 0x1215, Word 1 = 0x0C09
4	Get	Relay Output Status	WORD	Relay Output Status Bit 0-1: Relay Output 1 status Bit 2-3: Relay Output 2 status Other Reserved (should be 0) 00 = Digital output not support/preset 01 = Switch Contact is

				OPEN (OFF) 10 = Switch Contact is CLOSED (ON) 11 = Reserved
11	Get	AlarmStauts	ULINT	Alarm Status (0 is ON, 1 is OFF) Bit 0: switch code start Bit 1: switch warm start Bit 2: power1 state on->off Bit 3: power1 state off->on Bit 4: power2 state on->off Bit 5: power2 state off->on Bit 6: DI1 state on->off Bit 7: DI1 state off->on Bit 8: DI2 state on->off Bit 9: DI2 state off->on Bit 10: authentication failure Bit 11: dot1d Bridge New Root Bit 12: dot1d Bridge Topology Changed Bit 13: LLDP Remote Tables Changed Bit 14: configuration changed Bit 15: firmware update Bit 16: IP changed Bit 17: password changed
12	Get	Bandwidth overload	ULINT	Bit 0: Port 0 state Bit 1: Port 1 state…. Bit 63: Port 63 state 0 = OFF or not support 1 = Bandwidth overload
13	Get	Loopback detection port status	ULINT	Bit 0: Port 0 state Bit 1: Port 1 state…. Bit 63: Port 63 state 0 = OFF or not support 1 = Loopback detected
15	Get	Redundancy Protocol	USINT	0x0000: None 0x0001: RSTP/STP
16	Get	RSTP Root	USINT	0x0000: Not Root 0x0001: Root
17	Get	Redundancy - RING Mode	USINT	0x00: None (Disable) 0x01: Master 0x02: Slave
18	Get	Redundancy - Ring State	USINT	
19	Get	Redundancy - CHAIN State	USINT	0x00: None 0x01: The chain failure is happened.

Attr ID	Access Rule	Name	Data Type	Description of Attribute
20	Get	Redundancy - COUPING Mode	USINT	0x00: None (Disable) 0x01: Head 0x02: Tail
21	Get	Redundancy - COUPING State	USINT	COUPING mode is Head: 0x00: Monitor 0x01: Fault 0x02: Link-Up 0x03: Hold COUPING mode is Tail 0x00: Discover 0x01: Monitor 0x02: Fault
Common Services				
Service Code	Need in Implementation		Service Name	Description of Service
	Class	Instance		
0x0E	V	V	Get_Attribute_Single	Returns the contents of the specified attribute.
0x10		V	Set_Attribute_Single	Modifies an attribute value.

C.3 DVS-110W02-3SFP

Identity Object (0x01)

Class Attributes				
Attr ID	**Access rule**	**Name**	**Data type**	**Description of attribute**
1	Get	Revision	UINT	Revision of this object
2	Get	Max Instance	UINT	Maximum instance number of this object
Instance Attributes				
Attr ID	**Access rule**	**Name**	**Data type**	**Description of attribute**
1	Get	Vendor ID	UINT	799, Vendor ID of "Delta Electronics, Inc."
2	Get	Device Type	UINT	0x2C, "Managed Ethernet Switch Device".
3	Get	Product Code	UINT	Product code of device.
4	Get	Revision	STRUCT of:	Revision of the Identity Object
		Major	USINT	
		Minor	USINT	
5	Get	Status	WORD	0, Not used
6	Get	Serial Number	UDINT	Serial number of device
7	Get	Product Name	STRING	"DVS-110W02-3SFP", Product name of device.
Common Services				
Service Code	**Need in Implementation**		**Service name**	**Description of Service**
	Class	**Instance**		
0x01		V	Get_Attribute_All	Returns a predefined listing of this objects attributes.
0x05		V	Reset	Invokes the reset service for the device.
0x0E	V	V	Get_Attribute_Single	Returns the contents of the specified attribute.

Message Router Object (0x02)

Class Attributes				
Attr ID	**Access rule**	**Name**	**Data type**	**Description of attribute**
1	Get	Revision	UINT	Revision of this object
Instance Attributes				
Attr ID	**Access rule**	**Name**	**Data type**	**Description of attribute**
2	Get	Number Available	UINT	Maximum number of CIP connections supported
3	Get	Number Active	UINT	Number of CIP connections currently used by system components
Common Services				
Service Code	**Need in Implementation**		**Service name**	**Description of Service**
	Class	**Instance**		
0x0E	V	V	Get_Attribute_Single	Returns the contents of the specified attribute.

Assembly Object (0x04)

Class Attributes				
Attr ID	**Access rule**	**Name**	**Data type**	**Description of attribute**
1	Get	Revision	UINT	Revision of this object
Instance Attributes				
Attr ID	**Access rule**	**Name**	**Data type**	**Description of attribute**
3	Get/Set	Data	ARRAY of BYTE	

Attr ID	Access rule	Name	Data type	Description of attribute
4	Get	Size	UINT	
Instance				
Instance Number	**Size (bytes)**	**Name**	**Type**	**Description of attribute**
1	18	Power Source and Link Status	Inupt	Refer to Base Switch Object Attr ID 4 Byte 0: Power Source Status (Least Significant Byte) Byte 1: Power Source Status (Most Significant Byte) Refer to Base Switch Object Attr ID 8 Byte 2-5: Global Link Status DWORD 0 Byte 6-9: Global Link Status DWORD 1 Byte 10-13: Global Link Status DWORD 2 Byte 14-17: Global Link Status DWORD 3
2	16	Global Admin State	Input	Refer to Base Switch Object Attr ID 7 Byte 0-3: Global Admin Status DWORD 0 Byte 4-7: Global Admin Status DWORD 1 Byte 8-11: Global Admin Status DWORD 2 Byte 12-15: Global Admin Status DWORD 3
3	2	Contact Status	Input	Refer to Base Switch Object Attr ID 10 Byte 0: Contact Status (Least Significant Byte) Byte 1: Contact Status (Most Significant Byte)
50	16	Port Admin State	Output	Refer to Base Switch Object Attr ID 7 Byte 0-3: Global Admin Status DWORD 0 Byte 4-7: Global Admin Status DWORD 1 Byte 8-11: Global Admin Status DWORD 2 Byte 12-15: Global Admin Status DWORD 3
64	75	Device Status	Input	Refer to I/O Assembly Connection 4 - Input
Common Services				
Service Code	**Need in Implementation**		**Service name**	**Description of Service**
	Class	**Instance**		
0x0E	V	V	Get_Attribute_Single	Returns the contents of the specified attribute.
0x10		V	Set_Attribute_Single	Modifies an attribute value.
I/O Assembly				

Connection1			
	Instance	**Size(SINT)**	**Description**
Input	1	18	Please refer to Assembly Object Attr ID 1.
Output	50	16	Please refer to Assembly Object Attr ID 50.
Configuration	64	0	
Connection2			
	Instance	**Size(SINT)**	**Description**
Input	2	16	Please refer to Assembly Object Attr ID 2.
Output	50	16	Please refer to Assembly Object Attr ID 50.
Configuration	64	0	
Connection3			
	Instance	**Size(SINT)**	**Description**
Input	3	2	Please refer to Assembly Object Attr ID 2.
Output	50	16	Please refer to Assembly Object Attr ID 50
configuration	64	0	
Connection4			
	Instance	**Size(SINT)**	**Description**
Input	64	2	Please refer to Assembly Object Attr ID 3
Output	50	16	Please refer to Assembly Object Attr ID 50
configuration	80	0	
Direction	**Name**	**Size(SINT)**	**Description**
Input	Power Source Status	WORD	Refer to Base Switch Object Attr ID 4 Power Source Status (Least Significant Byte) Power Source Status (Most Significant Byte)
	Global Link Status	ARRAY OF DWORD	Refer to Base Switch Object Attr ID 8 Global Link Status DWORD 0 Global Link Status DWORD 1 Global Link Stauts DWORD 2 Global Link Status DWORD 3
	Global Admin State	ARRAY OF DWORD	Refer to Base Switch Object Attr ID 7 Global Admin Status DWORD 0 Global Admin Status DWORD 1 Global Admin Stauts DWORD 2 Global Admin Status DWORD 3
	Contact Status	WORD	Refer to Base Switch Object Attr ID 10
	AlarmStatus	ULINT	Refer to Delta IES Object Attr 11
	Bandwidth overload	ULINT	Refer to Delta IES Object Attr 12
	Loopback detection port status	ULINT	Refer to Delta IES Object Attr 13
	SFP Failure	ARRAY OF USINT	Refer to Delta IES Object Attr 14
	Redundancy Protocol	USINT	Refer to Delta IES Object Attr 15
	RSTP Root	USINT	Refer to Delta IES Object Attr 16
	Redundancy - RING Mode	USINT	Refer to Delta IES Object Attr 17
Direction	**Name**	**Size(SINT)**	**Description**
Input	Redundancy - Ring State	USINT	Refer to Delta IES Object Attr 18
Input	Redundancy - CHAIN State	USINT	Refer to Delta IES Object Attr 19
	Redundancy - COUPING Mode	USINT	Refer to Delta IES Object Attr 20
	Redundancy - COUPING State	USINT	Refer to Delta IES Object Attr 21

Output	Port Admin State	ARRAY OF DWORD	Refer to Base Switch Object Attr ID 7 Global Admin Status DWORD 0 Global Admin Status DWORD 1 Global Admin Stauts DWORD 2 Global Admin Status DWORD 3

Connection Manager Object (0x06)

Class Attributes				
Attr ID	**Access rule**	**Name**	**Data type**	**Description of attribute**
1	Get	Revision	UINT	Revision of this object
Instance Attributes				
Attr ID	**Access rule**	**Name**	**Data type**	**Description of attribute**
Common Services				
Service Code	**Need in Implementation**		**Service name**	**Description of Service**
	Class	**Instance**		
0x0E	V	V	Get_Attribute_Single	Returns the contents of the specified attribute.
0x4E		V	Forward_Close	Closes a connection
0x54		V	Forward_Open	Open a connection

Port Object (0xF4)

Class Attributes				
Attr ID	**Access rule**	**Name**	**Data type**	**Description of attribute**
1	Get	Revision	UINT	Revision of this object
2	Get	Max Instance	UINT	Maximum instance number.
3	Get	Num Instances	UINT	Number of port currently instantiated.
8	Get	Entry Port	UINT	Returns the port through which this request entered the device.
9	Get	Port Instance Info	ARRAY of STRUCT of	
		Port Type	UINT	Enumerates the type of port.
		Port Number	UINT	CIP port number associated with this port
Instance Attributes				
Attr ID	**Access rule**	**Name**	**Data type**	**Description of attribute**
1	Get	Port Type	UINT	Enumerates the type. (4=EthetNet/IP)
2	Get	Port Number	UINT	CIP port number associated with this port.
3	Get	Link Object	STRUCT of	
		Path Length	UINT	Number of 16 bit words in the following path.
		Link Path	Padded EPATH	Logical path segments that identify the object for this port.
4	Get	Port Name	SHORT_STRING	String which names the physical network port
7	Get	Node Address	Padded EPATH	Node number of this device on port.
Common Services				
Service Code	**Need in Implementation**		**Service name**	**Description of Service**
	Class	**Instance**		
0x0E	V	V	Get_Attribute_Single	Returns the contents of the specified attribute.

TCP/IP Interface Object (0xF5)

Class Attributes				
Attr ID	**Access rule**	**Name**	**Data type**	**Description of attribute**
1	Get	Revision	UINT	Revision of this object

Instance Attributes				
Attr ID	**Access rule**	**Name**	**Data type**	**Description of attribute**
1	Get	Status	DWORD	Interface status 0=The Interface Configuration attribute has not been configured. 1=The Interface Configuration attribute contains configuration obtained from BOOTP, DHCP or non-volatile storage.
2	Get	Configuration Capability	DWORD	Interface capability Bit 0: BOOTP Client 1 (TRUE) shall indicate the device is capable of obtaining its network configuration via BOOTP. Bit 1: DNS Client 1 (TRUE) shall indicate the device is capable of resolving host names by querying a DNS server. Bit 2: DHCP Client 1 (TRUE) shall indicate the device is capable of obtaining its network configuration via DHCP. Bit 3: DHCP-DNS Update Shall be 0 Bit 4: Configuration Settable 1 (TRUE) shall indicate the Interface Configuration attribute is settable.
3	Get/Set	Configuration Control	DWORD	Interface control flags Bit 0-3: Configuration Method 0=The device shall use statically-assigned IP configuration values. 1=The device shall obtain its interface configuration values via BOOTP. 2=The device shall obtain its interface configuration values via DHCP. 3-15=Reserved for future use. Bit 4: DNS Enable If 1 (TRUE), the device shall resolve host names by querying a DNS server.
4	Get	Physical Link Object	STRUCT of	Path to physical link object.
		Path size	UINT	Size of Path.
		Path	Padded EPATH	Logical segments identifying the physical link object.

Attr ID	**Access rule**	**Name**	**Data type**	**Description of attribute**
5	Get/Set	Interface Configuration	STRUCT of	TCP/IP network interface configuration.
		IP Address	UDINT	The device's IP address.
		Network Mask	UDINT	The device's network mask
		Gateway Address	UDINT	Default gateway address
		Name Server	UDINT	Primary name server
		Name Server 2	UDINT	Secondary name server
		Domain Name	STRING	Default domain name Note: ASCII characters. Maximum

				length is 48 characters. Shall be padded to an even number of characters (pad not included in length).
6	Get/Set	Host Name	STRING	Host Name (Note: ASCII characters. Maximum length is 64 characters. Shall be padded to an even number of characters (pad not included in length).

Common Services

Service Code	Need in Implementation		Service name	Description of Service
	Class	Instance		
0x0E	V	V	Get_Attribute_Single	Returns the contents of the specified attribute.
0x10		V	Set_Attribute_Single	Modifies an attribute value.

Ethernet Link Object (0xF6)

Class Attributes

Attr ID	Access rule	Name	Data type	Description of attribute
1	Get	Revision	UINT	Revision of this object
2	Get	Max Instance	UINT	Maximum instance number of an object currently created in this class level of the device.
3	Get	Number of Instances	UINT	Number of object instances currently created at this class level of the device. (The value is mapping the number of ports in Switch device)

Instance Attributes

Attr ID	Access rule	Name	Data type	Description of attribute
1	Get	Interface Speed	UDINT	Interface speed currently in use Speed in Mbps (e.g., 0, 10, 100, 1000, etc.)
2	Get	Interface Flags	DWORD	Interface status flags
3	Get	Physical Address	ARRAY of 6 USINTs	MAC layer address
4	Get	Interface Counters	STRUCT of:	
		In Octets	UDINT	Octets received on the interface
		In Ucast Packets	UDINT	Unicast packets received on the interface
		In Nucast Packets	UDINT	Non-unicast packets received on the interface
		In Discards	UDINT	Inbound packets received on the interface but discarded
		In Errors	UDINT	Inbound packets that contain errors (does not include In Discards)
Attr ID	**Access rule**	**Name**	**Data type**	**Description of attribute**
4	Get	In Unknown Protos	UDINT	Inbound packets with unknown protocol
		Out Octets	UDINT	Octets sent on the interface
		Out Ucast Packets	UDINT	Unicast packets sent on the interface
		Out Nucast Packets	UDINT	Non-unicast packets sent on the interface
		Out Discards	UDINT	Outbound packets discarded
		Out Errors	UDINT	Outbound packets that contain errors
5	Get	Media Counters	STRUCT of:	Media-specific counters

		Alignment Errors	UDINT	Frames received that are not an integral number of octets in length
		FCS Errors	UDINT	Frames received that do not pass the FCS check
		Single Collisions	UDINT	Successfully transmitted frames which experienced exactly one collision
		Multiple Collisions	UDINT	Successfully transmitted frames which experienced more than one collision
		SQE Test Errors	UDINT	Number of times SQE test error message is generated
		Deferred Transmissions	UDINT	Frames for which first transmission attempt is delayed because the medium is busy
		Late Collisions	UDINT	Number of times a collision is detected later than 512 bit-times into the transmission of a packet
		Excessive Collisions	UDINT	Frames for which transmission fails due to excessive collisions
		MAC Transmit Errors	UDINT	Frames for which transmission fails due to an internal MAC sublayer transmit error
		Carrier Sense Errors	UDINT	Times that the carrier sense condition was lost or never asserted when attempting to transmit a frame
		Frame Too Long	UDINT	Frames received that exceed the maximum permitted frame size
		MAC Receive Errors	UDINT	Frames for which reception on an interface fails due to an internal MAC sublayer receive error
10	Get	Interface Label	SHORT_STRING	Human readable identification

Common Services

Service Code	Need in Implementation		Service name	Description of Service
	Class	Instance		
0x0E	V	V	Get_Attribute_Single	Returns the contents of the specified attribute.

Base Switch Object (0x51)

Class Attributes

Attr ID	Access rule	Name	Data type	Description of attribute
1	Get	Revision	UINT	Revision of this object. The current value assigned to this values is 1

Instance Attributes

Attr ID	Access rule	Name	Data type	Description of attribute
1	Get	Device Up Time	UDINT	Time since device was powered up (s) (Note: the value is 32-bit)
2	Get	Total port count	UDINT	Number of physical ports
3	Get	System Firmware Version	SHORT_STRING	Human readable representation of System Firmware Version (Note: ASCII characters, max length is 32 bytes)
4	Get	Power Source	WORD	Status of switch power source Bit 0-1: Power Source 1 Bit 2-3: Power Source 2…. Bit 14-15: Power Source 8

				00=Not Present (power source not present in switch) 01=Not Powered (power source present but not powered) 10=Faulted (power source present but faulted) 11=Powered and ok (power source present, powered and OK)
5	Get	Port Mask Size	UINT	Number of DWORDs in port array attributes (Minimum=4, supporting 128 ports)
7	Get / Set	Global Port Admin State	ARRAY OF DWORD	Port Admin Status (Note: Size of array=attribute 5) DWORD[0]: Port 0 - 31 admin status DWORD[1]: Port 32 - 63 admin status DWORD[2]: Port 64 - 95 admin status DWORD[3]: Port 96 - 127 admin status 0=Port (or Interface) Enabled 1=Port (or Interface) Disabled
8	Get	Global Port Link Status	ARRAY OF DWORD	Port Link Status (Note: Size of array=attribute 5) DWORD[0]: Port 0 - 31 link status DWORD[1]: Port 32 - 63 link status DWORD[2]: Port 64 - 95 link status DWORD[3]: Port 96 - 127 link status 0=Link inactive (Down) 1=Link Active (UP)
10	Get	Contact Status	WORD	Switch Contact Closure (DI) Bit 0-1: Switch Contact 1 (DI 1) Bit 2-3: Switch Contact 2 (DI 2) Other Reserved (should be 0) 00=Switch Contact not support/pressed 01=Switch Contact is OPEN (OFF) 10=Switch Contact is CLOSED (ON) 11=Reserved

Common Services

Service Code	Need in Implementation		Service name	Description of Service
	Class	Instance		
0x0E	V	V	Get_Attribute_Single	Returns the contents of the specified attribute.
0x10		V	Set_Attribute_Single	Modifies an attribute value.

Delta IES Object (0x64)

Class Attributes

Attr ID	Access rule	Name	Data type	Description of attribute
1	Get	Revision	UINT	Revision of this object

Instance Attributes

Attr ID	Access rule	Name	Data type	Description of attribute
1	Get/Set	Reboot Device	USINT	Reboot device Set 0x0001 to reboot device, and return to 0x0000 if reboot is completed.
2	Get/Set	Reset Device	USINT	Reset to default Set 0x0001 to reset configuration, and return to 0x0000 if reset is completed.

Attr ID	Access rule	Name	Data type	Description of attribute
3	Get	Firmware Release Date	UDINT	Ex: 20120918, PM9:00 Word 0=0x1215, Word 1=0x0C09
4	Get	Relay Output Status	WORD	Relay Output Status Bit 0-1: Relay Output 1 status Bit 2-3: Relay Output 2 status Other Reserved (should be 0) 00=Digital output not support/pressed 01=Switch Contact is OPEN (OFF) 10=Switch Contact is CLOSED (ON) 11=Reserved
11	Get	Alarm Status	ULINT	Alarm Status (0 is ON, 1 is OFF) Bit 0: switch code start Bit 1: switch warm start Bit 2: power1 state on->off Bit 3: power1 state off->on Bit 4: power2 state on->off Bit 5: power2 state off->on Bit 6: DI1 state on->off Bit 7: DI1 state off->on Bit 8: DI2 state on->off Bit 9: DI2 state off->on Bit 10: authentication failure Bit 11: dot1d Bridge New Root Bit 12: dot1d Bridge Topology Changed Bit 13: LLDP Remote Tables Changed Bit 14: configuration changed Bit 15: firmware update Bit 16: IP changed Bit 17: password changed
12	Get	Bandwidth overload	ULINT	Bit 0: Port 0 state Bit 1: Port 1 state…. Bit 63: Port 63 state 0=OFF or not support 1=Bandwidth overload
13	Get	Loopback detection port status	ULINT	Bit 0: Port 0 state Bit 1: Port 1 state…. Bit 63: Port 63 state 0=OFF or not support 1=Loopback detected
15	Get	Redundancy Protocol	USINT	0x0000: None x0001: RSTP/STP
16	Get	RSTP Root	USINT	0x0000: Not Root 0x0001: Root
17	Get	Redundancy - RING Mode	USINT	0x00: None (Disable) 0x01: Master 0x02: Slave
18	Get	Redundancy - Ring State	USINT	RING function is disable: 0x00: None RING Mode is Master: 0x00: Discover 0x01: Monitor 0x02: Fault RING Mode is Slave:

				0x00: Forwarding 0x01: Hold 0x02: Fault
19	Get	Redundancy - CHAIN State	USINT	0x00: None 0x01: The chain failure is happened.
20	Get	Redundancy - COUPING Mode	USINT	0x00: None (Disable) 0x01: Head 0x02: Tail
21	Get	Redundancy - COUPING State	USINT	COUPING mode is Head: 0x00: Monitor 0x01: Fault 0x02: Link-Up 0x03: Hold COUPING mode is Tail 0x00: Discover 0x01: Monitor 0x02: Fault

Common Services

Service Code	Need in Implementation		Service name	Description of Service
	Class	Instance		
0x0E	V	V	Get_Attribute_Single	Returns the contents of the specified attribute.
0x10		V	Set_Attribute_Single	Modifies an attribute value.

C.4 DVS-328R02-8SFP

Identity Object (0x01)

Class Attributes				
Attr ID	**Access rule**	**Name**	**Data type**	**Description of attribute**
1	Get	Revision	UINT	Revision of this object
2	Get	Max Instance	UINT	Maximum instance number of this object
Instance Attributes				
Attr ID	**Access rule**	**Name**	**Data type**	**Description of attribute**
1	Get	Vendor ID	UINT	799, Vendor ID of "Delta Electronics, Inc."
2	Get	Device Type	UINT	0x2C, "Managed Ethernet Switch Device".
3	Get	Product Code	UINT	Product code of device.
4	Get	Revision	STRUCT of:	Revision of the Identity Object
		Major	USINT	
		Minor	USINT	
5	Get	Status	WORD	0, Not used
6	Get	Serial Number	UDINT	Serial number of device
7	Get	Product Name	STRING	"DVS-328R02-8SFP", Product name of device.
Common Services				
Service Code	**Need in Implementation**		**Service name**	**Description of Service**
	Class	**Instance**		
0x01		V	Get_Attribute_All	Returns a predefined listing of this objects attributes.
0x05		V	Reset	Invokes the reset service for the device.
0x0E	V	V	Get_Attribute_Single	Returns the contents of the specified attribute.

Message Router Object (0x02)

Class Attributes				
Attr ID	**Access rule**	**Name**	**Data type**	**Description of attribute**
1	Get	Revision	UINT	Revision of this object
Instance Attributes				
Attr ID	**Access rule**	**Name**	**Data type**	**Description of attribute**
2	Get	Number Available	UINT	Maximum number of CIP connections supported
3	Get	Number Active	UINT	Number of CIP connections currently used by system components
Common Services				
Service Code	**Need in Implementation**		**Service name**	**Description of Service**
	Class	**Instance**		
0x0E	V	V	Get_Attribute_Single	Returns the contents of the specified attribute.

Assembly Object (0x04)

Class Attributes				
Attr ID	**Access rule**	**Name**	**Data type**	**Description of attribute**
1	Get	Revision	UINT	Revision of this object
Instance Attributes				
Attr ID	**Access rule**	**Name**	**Data type**	**Description of attribute**
3	Get/Set	Data	ARRAY of BYTE	
Attr ID	**Access rule**	**Name**	**Data type**	**Description of attribute**
4	Get	Size	UINT	
Instance				
Instance Number	**Size (bytes)**	**Name**	**Type**	**Description of attribute**
1	18	Power Source and Link Status	Input	Refer to Base Switch Object Attr ID 4 Byte 0: Power Source Status (Least Significant Byte) Byte 1: Power Source Status (Most Significant Byte) Refer to Base Switch Object Attr ID 8 Byte 2-5: Global Link Status DWORD 0 Byte 6-9: Global Link Status DWORD 1 Byte 10-13: Global Link Status DWORD 2 Byte 14-17: Global Link Status DWORD 3
2	16	Global Admin State	Input	Refer to Base Switch Object Attr ID 7 Byte 0-3: Global Admin Status DWORD 0 Byte 4-7: Global Admin Status DWORD 1 Byte 8-11: Global Admin Status DWORD 2 Byte 12-15: Global Admin Status DWORD 3
3	2	Contact Status	Input	Refer to Base Switch Object Attr ID 10 Byte 0: Contact Status (Least Significant Byte) Byte 1: Contact Status (Most Significant Byte)
50	16	Port Admin State	Output	Refer to Base Switch Object Attr ID 7 Byte 0-3: Global Admin Status DWORD 0 Byte 4-7: Global Admin Status DWORD 1 Byte 8-11: Global Admin Status DWORD 2 Byte 12-15: Global Admin Status DWORD 3
64	76	Device Status	Input	Refer to I/O Assembly Connection - Input

Common Services				
Service Code	**Need in Implementation**		**Service name**	**Description of Service**
	Class	**Instance**		
0x0E	V	V	Get_Attribute_Single	Returns the contents of the specified attribute.
0x10		V	Set_Attribute_Single	Modifies an attribute value.
I/O Assembly				
Connection1				
	Instance	**Size(SINT)**	**Description**	
Input	1	18	Please refer to Assembly Object Attr ID 1.	
Output	50	16	Please refer to Assembly Object Attr ID 50.	
Configuration	64	0		
Connection2				
	Instance	**Size(SINT)**	**Description**	
Input	2	16	Please refer to Assembly Object Attr ID 2.	
Output	50	16	Please refer to Assembly Object Attr ID 50.	
Configuration	64	0		
Connection3				
	Instance	**Size(SINT)**	**Description**	
Input	3	2	Please refer to Assembly Object Attr ID 2.	
Output	50	16	Please refer to Assembly Object Attr ID 50	
configuration	64	0		
Connection4				
	Instance	**Size(SINT)**	**Description**	
Input	64	76	Please refer to Assembly Object Attr ID 3	
Output	50	16	Please refer to Assembly Object Attr ID 50	
configuration	80	0		
Direction	**Name**	**Size(SINT)**	**Description**	
Input	Power Source Status	WORD	Refer to Base Switch Object Attr ID 4 Power Source Status (Least Significant Byte) Power Source Status (Most Significant Byte)	
	Global Link Status	ARRAY OF DWORD	Refer to Base Switch Object Attr ID 8 Global Link Status DWORD 0 Global Link Status DWORD 1 Global Link Stauts DWORD 2 Global Link Status DWORD 3	
	Global Admin State	ARRAY OF DWORD	Refer to Base Switch Object Attr ID 7 Global Admin Status DWORD 0 Global Admin Status DWORD 1 Global Admin Stauts DWORD 2 Global Admin Status DWORD 3	
	Contact Status	WORD	Refer to Base Switch Object Attr ID 10	
	AlarmStatus	ULINT	Refer to Delta IES Object Attr 11	
	Bandwidth overload	ULINT	Refer to Delta IES Object Attr 12	
	Loopback detection port status	ULINT	Refer to Delta IES Object Attr 13	
	SFP Failure	ARRAY OF USINT	Refer to Delta IES Object Attr 14	
	Redundancy Protocol	USINT	Refer to Delta IES Object Attr 15	
	RSTP Root	USINT	Refer to Delta IES Object Attr 16	
	Redundancy - RING Mode	USINT	Refer to Delta IES Object Attr 17	

Direction	Name	Size(SINT)	Description
Input	Redundancy - Ring State	USINT	Refer to Delta IES Object Attr 18
	Redundancy - CHAIN State	USINT	Refer to Delta IES Object Attr 19
	Redundancy - COUPING Mode	USINT	Refer to Delta IES Object Attr 20
	Redundancy - COUPING State	USINT	Refer to Delta IES Object Attr 21
Output	Port Admin State	ARRAY OF DWORD	Refer to Base Switch Object Attr ID 7 Global Admin Status DWORD 0 Global Admin Status DWORD 1 Global Admin Stauts DWORD 2 Global Admin Status DWORD 3

Connection Manager Object (0x06)

Class Attributes				
Attr ID	**Access rule**	**Name**	**Data type**	**Description of attribute**
1	Get	Revision	UINT	Revision of this object
Instance Attributes				
Attr ID	**Access rule**	**Name**	**Data type**	**Description of attribute**
Common Services				
Service Code	**Need in Implementation**		**Service name**	**Description of Service**
	Class	**Instance**		
0x0E	V	V	Get_Attribute_Single	Returns the contents of the specified attribute.
0x4E		V	Forward_Close	Closes a connection
0x54		V	Forward_Open	Open a connection

Port Object (0xF4)

Class Attributes				
Attr ID	**Access rule**	**Name**	**Data type**	**Description of attribute**
1	Get	Revision	UINT	Revision of this object
2	Get	Max Instance	UINT	Maximum instance number.
3	Get	Num Instances	UINT	Number of port currently instantiated.
8	Get	Entry Port	UINT	Returns the port through which this request entered the device.
9	Get	Port Instance Info	ARRAY of STRUCT of	
		Port Type	UINT	Enumerates the type of port.
		Port Number	UINT	CIP port number associated with this port
Instance Attributes				
Attr ID	**Access rule**	**Name**	**Data type**	**Description of attribute**
1	Get	Port Type	UINT	Enumerates the type. (4=EthetNet/IP)
2	Get	Port Number	UINT	CIP port number associated with this port.
3	Get	Link Object	STRUCT of	
		Path Length	UINT	Number of 16 bit words in the following path.
		Link Path	Padded EPATH	Logical path segments that identify the object for this port.
4	Get	Port Name	SHORT_STRING	String which names the physical network port
7	Get	Node Address	Padded EPATH	Node number of this device on port.

Common Services				
Service Code	**Need in Implementation**		**Service name**	**Description of Service**
	Class	**Instance**		
0x0E	V	V	Get_Attribute_Single	Returns the contents of the specified attribute.

TCP/IP Interface Object (0xF5)

Class Attributes				
Attr ID	**Access rule**	**Name**	**Data type**	**Description of attribute**
1	Get	Revision	UINT	Revision of this object
Instance Attributes				
Attr ID	**Access rule**	**Name**	**Data type**	**Description of attribute**
1	Get	Status	DWORD	Interface status 0=The Interface Configuration attribute has not been configured. 1=The Interface Configuration attribute contains configuration obtained from BOOTP, DHCP or non-volatile storage.
2	Get	Configuration Capability	DWORD	Interface capability Bit 0: BOOTP Client 1 (TRUE) shall indicate the device is capable of obtaining its network configuration via BOOTP. Bit 1: DNS Client 1 (TRUE) shall indicate the device is capable of resolving host names by querying a DNS server. Bit 2: DHCP Client 1 (TRUE) shall indicate the device is capable of obtaining its network configuration via DHCP. Bit 3: DHCP-DNS Update Shall be 0 Bit 4: Configuration Settable 1 (TRUE) shall indicate the Interface Configuration attribute is settable.
3	Get/Set	Configuration Control	DWORD	Interface control flags Bit 0-3: Configuration Method 0=The device shall use statically-assigned IP configuration values. 1=The device shall obtain its interface configuration values via BOOTP. 2=The device shall obtain its interface configuration values via DHCP. 3-15=Reserved for future use. Bit 4: DNS Enable If 1 (TRUE), the device shall resolve host names by querying a DNS server.
4	Get	Physical Link Object	STRUCT of	Path to physical link object.
		Path size	UINT	Size of Path.
		Path	Padded EPATH	Logical segments identifying the physical link object.

Attr ID	Access rule	Name	Data type	Description of attribute
5	Get/Set	Interface Configuration	STRUCT of	TCP/IP network interface configuration.
		IP Address	UDINT	The device's IP address.
		Network Mask	UDINT	The device's network mask
		Gateway Address	UDINT	Default gateway address
		Name Server	UDINT	Primary name server
		Name Server 2	UDINT	Secondary name server
		Domain Name	STRING	Default domain name Note: ASCII characters. Maximum length is 48 characters. Shall be padded to an even number of characters (pad not included in length).
6	Get/Set	Host Name	STRING	Host Name (Note: ASCII characters. Maximum length is 64 characters. Shall be padded to an even number of characters (pad not included in length).

Common Services

Service Code	Need in Implementation		Service name	Description of Service
	Class	Instance		
0x0E	V	V	Get_Attribute_Single	Returns the contents of the specified attribute.
0x10		V	Set_Attribute_Single	Modifies an attribute value.

Ethernet Link Object (0xF6)

Class Attributes

Attr ID	Access rule	Name	Data type	Description of attribute
1	Get	Revision	UINT	Revision of this object
2	Get	Max Instance	UINT	Maximum instance number of an object currently created in this class level of the device.
3	Get	Number of Instances	UINT	Number of object instances currently created at this class level of the device. (The value is mapping the number of ports in Switch device)

Instance Attributes

Attr ID	Access rule	Name	Data type	Description of attribute
1	Get	Interface Speed	UDINT	Interface speed currently in use Speed in Mbps (e.g., 0, 10, 100, 1000, etc.)
2	Get	Interface Flags	DWORD	Interface status flags
3	Get	Physical Address	ARRAY of 6 USINTs	MAC layer address
4	Get	Interface Counters	STRUCT of:	
		In Octets	UDINT	Octets received on the interface
		In Ucast Packets	UDINT	Unicast packets received on the interface
		In Nucast Packets	UDINT	Non-unicast packets received on the interface
		In Discards	UDINT	Inbound packets received on the interface but discarded
		In Errors	UDINT	Inbound packets that contain errors (does not include In Discards)

Attr ID	Access rule	Name	Data type	Description of attribute
4	Get	In Unknown Protos	UDINT	Inbound packets with unknown protocol
		Out Octets	UDINT	Octets sent on the interface
		Out Ucast Packets	UDINT	Unicast packets sent on the interface
		Out Nucast Packets	UDINT	Non-unicast packets sent on the interface
		Out Discards	UDINT	Outbound packets discarded
		Out Errors	UDINT	Outbound packets that contain errors
5	Get	Media Counters	STRUCT of:	Media-specific counters
		Alignment Errors	UDINT	Frames received that are not an integral number of octets in length
		FCS Errors	UDINT	Frames received that do not pass the FCS check
		Single Collisions	UDINT	Successfully transmitted frames which experienced exactly one collision
		Multiple Collisions	UDINT	Successfully transmitted frames which experienced more than one collision
		SQE Test Errors	UDINT	Number of times SQE test error message is generated
		Deferred Transmissions	UDINT	Frames for which first transmission attempt is delayed because the medium is busy
		Late Collisions	UDINT	Number of times a collision is detected later than 512 bit-times into the transmission of a packet
		Excessive Collisions	UDINT	Frames for which transmission fails due to excessive collisions
		MAC Transmit Errors	UDINT	Frames for which transmission fails due to an internal MAC sublayer transmit error
		Carrier Sense Errors	UDINT	Times that the carrier sense condition was lost or never asserted when attempting to transmit a frame
		Frame Too Long	UDINT	Frames received that exceed the maximum permitted frame size
		MAC Receive Errors	UDINT	Frames for which reception on an interface fails due to an internal MAC sublayer receive error
10	Get	Interface Label	SHORT_STRING	Human readable identification

Common Services

Service Code	Need in Implementation		Service name	Description of Service
	Class	Instance		
0x0E	V	V	Get_Attribute_Single	Returns the contents of the specified attribute.

Base Switch Object (0x51)

Class Attributes				
Attr ID	**Access rule**	**Name**	**Data type**	**Description of attribute**
1	Get	Revision	UINT	Revision of this object. The current value assigned to this values is 1
Instance Attributes				
Attr ID	**Access rule**	**Name**	**Data type**	**Description of attribute**
1	Get	Device Up Time	UDINT	Time since device was powered up (s) (Note: the value is 32-bit)
2	Get	Total port count	UDINT	Number of physical ports
3	Get	System Firmware Version	SHORT_STRING	Human readable representation of System Firmware Version (Note: ASCII characters, max length is 32 bytes)
4	Get	Power Source	WORD	Status of switch power source Bit 0-1: Power Source 1 Bit 2-3: Power Source 2…. Bit 14-15: Power Source 8 00=Not Present (power source not present in switch) 01=Not Powered (power source present but not powered) 10=Faulted (power source present but faulted) 11=Powered and ok (power source present, powered and OK)
5	Get	Port Mask Size	UINT	Number of DWORDs in port array attributes (Minimum=4, supporting 128 ports)
7	Get / Set	Global Port Admin State	ARRAY OF DWORD	Port Admin Status (Note: Size of array=attribute 5) DWORD[0]: Port 0 - 31 admin status DWORD[1]: Port 32 - 63 admin status DWORD[2]: Port 64 - 95 admin status DWORD[3]: Port 96 - 127 admin status 0=Port (or Interface) Enabled 1=Port (or Interface) Disabled
8	Get	Global Port Link Status	ARRAY OF DWORD	Port Link Status (Note: Size of array=attribute 5) DWORD[0]: Port 0 - 31 link status DWORD[1]: Port 32 - 63 link status DWORD[2]: Port 64 - 95 link status DWORD[3]: Port 96 - 127 link status 0=Link inactive (Down) 1=Link Active (UP)
10	Get	Contact Status	WORD	Switch Contact Closure (DI) Bit 0-1: Switch Contact 1 (DI 1) Bit 2-3: Switch Contact 2 (DI 2) Other Reserved (should be 0) 00=Switch Contact not support/pressed 01=Switch Contact is OPEN (OFF) 10=Switch Contact is CLOSED (ON) 11=Reserved

Common Services				
Service Code	**Need in Implementation**		**Service name**	**Description of Service**
	Class	**Instance**		
0x0E	V	V	Get_Attribute_Single	Returns the contents of the specified attribute.
0x10		V	Set_Attribute_Single	Modifies an attribute value.

Delta IES Object (0x64)

Class Attributes				
Attr ID	**Access rule**	**Name**	**Data type**	**Description of attribute**
1	Get	Revision	UINT	Revision of this object
Instance Attributes				
Attr ID	**Access rule**	**Name**	**Data type**	**Description of attribute**
1	Get/Set	Reboot Device	USINT	Reboot device Set 0x0001 to reboot device, and return to 0x0000 if reboot is completed.
2	Get/Set	Reset Device	USINT	Reset to default Set 0x0001 to reset configuration, and return to 0x0000 if reset is completed.
Attr ID	**Access rule**	**Name**	**Data type**	**Description of attribute**
3	Get	Firmware Release Date	UDINT	Ex: 20120918, PM9:00 Word 0=0x1215, Word 1=0x0C09
4	Get	Relay Output Status	WORD	Relay Output Status Bit 0-1: Relay Output 1 status Bit 2-3: Relay Output 2 status Other Reserved (should be 0) 00=Digital output not support/pressed 01=Switch Contact is OPEN (OFF) 10=Switch Contact is CLOSED (ON) 11=Reserved
11	Get	Alarm Status	ULINT	Alarm Status (0 is ON, 1 is OFF) Bit 0: switch code start Bit 1: switch warm start Bit 2: power1 state on->off Bit 3: power1 state off->on Bit 4: power2 state on->off Bit 5: power2 state off->on Bit 6: DI1 state on->off Bit 7: DI1 state off->on Bit 8: DI2 state on->off Bit 9: DI2 state off->on Bit 10: authentication failure Bit 11: dot1d Bridge New Root Bit 12: dot1d Bridge Topology Changed Bit 13: LLDP Remote Tables Changed Bit 14: configuration changed Bit 15: firmware update Bit 16: IP changed Bit 17: password changed
12	Get	Bandwidth overload	ULINT	Bit 0: Port 0 state Bit 1: Port 1 state…. Bit 63: Port 63 state 0=OFF or not support 1=Bandwidth overload

13	Get	Loopback detection port status	ULINT	Bit 0: Port 0 state Bit 1: Port 1 state…. Bit 63: Port 63 state 0=OFF or not support 1=Loopback detected
15	Get	Redundancy Protocol	USINT	0x0000: None x0001: RSTP/STP
16	Get	RSTP Root	USINT	0x0000: Not Root 0x0001: Root
17	Get	Redundancy - RING Mode	USINT	0x00: None (Disable) 0x01: Master 0x02: Slave
18	Get	Redundancy - Ring State	USINT	RING function is disable: 0x00: None RING Mode is Master: 0x00: Discover 0x01: Monitor 0x02: Fault RING Mode is Slave: 0x00: Forwarding 0x01: Hold 0x02: Fault
19	Get	Redundancy - CHAIN State	USINT	0x00: None 0x01: The chain failure is happened.
20	Get	Redundancy - COUPING Mode	USINT	0x00: None (Disable) 0x01: Head 0x02: Tail
21	Get	Redundancy - COUPING State	USINT	COUPING mode is Head: 0x00: Monitor 0x01: Fault 0x02: Link-Up 0x03: Hold COUPING mode is Tail 0x00: Discover 0x01: Monitor 0x02: Fault

Common Services

Service Code	Need in Implementation		Service name	Description of Service
	Class	Instance		
0x0E	V	V	Get_Attribute_Single	Returns the contents of the specified attribute.
0x10		V	Set_Attribute_Single	Modifies an attribute value.

Appendix D EDS File

Table of Contents

D.1 EDS (Electronic Data Sheet) File

The EDS file is used to specify and describe the communication data of an EtherNet/IP switch. We provide the EDS file to help you identify the communication data or objects of the Delta managed switch, and you can use the notepad or the text editor to open the EDS file.
The EDS file list is shown below:

- File
- Device
- Device Classification
- Params
- Connection Manager
- Port
- Ethernet Link Class

An EDS file can be found in the product CD if you need to use it.