



## Industrial Automation Headquarters

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

### Asia

**Delta Electronics (Shanghai) Co., Ltd.**  
No.182 Minyu Rd., Pudong Shanghai, P.R.C.  
Post code : 201209  
TEL: 86-21-6872-3988 / FAX: 86-21-6872-3996  
Customer Service: 400-820-9595

**Delta Electronics (Japan), Inc.**  
Tokyo Office  
Industrial Automation Sales Department  
2-1-14 Shibadaimon, Minato-ku  
Tokyo, Japan 105-0012  
TEL: 81-3-5733-1155 / FAX: 81-3-5733-1255

**Delta Electronics (Korea), Inc.**  
Seoul Office  
1511, 219, Gasan Digital 1-Ro., Geumcheon-gu,  
Seoul, 08501 South Korea  
TEL: 82-2-515-5305 / FAX: 82-2-515-5302

**Delta Energy Systems (Singapore) Pte Ltd.**  
4 Kaki Bukit Avenue 1, #05-04, Singapore 417939  
TEL: 65-6747-5155 / FAX: 65-6744-9228

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

**Delta Electronics (Thailand) PCL.**  
909 Soi 9, Moo 4, Bangpoo Industrial Estate (E.P.Z),  
Pattana 1 Rd., T.Phraksa, A.Muang,  
Samutprakarn 10280, Thailand  
TEL: 66-2709-2800 / FAX : 662-709-2827

**Delta Energy Systems (Australia) Pty Ltd.**  
Unit 20-21/45 Normanby Rd., Notting Hill Vic 3168, Australia  
TEL: 61-3-9543-3720

### Americas

**Delta Electronics (Americas) Ltd.**  
Raleigh Office  
P.O. Box 12173, 5101 Davis Drive,  
Research Triangle Park, NC 27709, U.S.A.  
TEL: 1-919-767-3813 / FAX: 1-919-767-3969

**Delta Greentech (Brasil) S/A**  
São Paulo Office  
Rua Itapeva, 26 - 3º Andar - Bela Vista  
CEP: 01332-000 - São Paulo - SP - Brasil  
TEL: 55-11-3530-8642 / 55-11-3530-8640

**Delta Electronics International Mexico S.A. de C.V.**  
Mexico Office  
Vía Dr. Gustavo Baz No. 2160, Colonia La Loma,  
54060 TlalnepanTla Estado de Mexico  
TEL: 52-55-2628-3015 #3050/3052

### EMEA

**Headquarters: Delta Electronics (Netherlands) B.V.**  
Sales: Sales.IA.EMEA@deltaww.com  
Marketing: Marketing.IA.EMEA@deltaww.com  
Technical Support: iatechnicalsupport@deltaww.com  
Customer Support: Customer-Support@deltaww.com  
Service: Service.IA.emea@deltaww.com  
TEL: +31(0)40 800 3800

**BENELUX: Delta Electronics (Netherlands) B.V.**  
De Witbogt 20, 5652 AG Eindhoven, The Netherlands  
Mail: Sales.IA.Benelux@deltaww.com  
TEL: +31(0)40 800 3800

**DACH: Delta Electronics (Netherlands) B.V.**  
Coesterweg 45, D-59494 Soest, Germany  
Mail: Sales.IA.DACH@deltaww.com  
TEL: +49(0)2921 987 0

**France: Delta Electronics (France) S.A.**  
ZI du bois Challand 2, 15 rue des Pyrénées,  
Lisses, 91090 Evry Cedex, France  
Mail: Sales.IA.FR@deltaww.com  
TEL: +33(0)1 69 77 82 60

**Iberia: Delta Electronics Solutions (Spain) S.L.U**  
Ctra. De Villaverde a Vallecas, 265 1º Dcha Ed.  
Hormigueras - P.I. de Vallecas 28031 Madrid  
TEL: +34(0)91 223 74 20  
C/Lluïa, 321-329 (Edifici CINC) | 22@Barcelona, 08019 Barcelona  
Mail: Sales.IA.Iberia@deltaww.com  
TEL: +34 93 303 00 60

**Italy: Delta Electronics (Italy) S.r.l.**  
Ufficio di Milano Via Senigallia 18/2 20161 Milano (MI)  
Piazza Grazioli 18 00186 Roma Italy  
Mail: Sales.IA.Italy@deltaww.com  
TEL: +39 02 64672538

**Russia: Delta Energy System LLC**  
Vereyskaya Plaza II, office 112 Vereyskaya str.  
17 121357 Moscow Russia  
Mail: Sales.IA.RU@deltaww.com  
TEL: +7 495 644 3240

**Turkey: Delta Greentech Elektronik San. Ltd. Sti. (Turkey)**  
Şerifali Mah. Hendem Cad. Kule Sok. No:16-A  
34775 Ümraniye - Istanbul  
Mail: Sales.IA.Turkey@deltaww.com  
TEL: + 90 216 499 9910

**GCC: Delta Energy Systems AG (Dubai BR)**  
P.O. Box 185668, Gate 7, 3rd Floor, Hamarain Centre  
Dubai, United Arab Emirates  
Mail: Sales.IA.MEA@deltaww.com  
TEL: +971(0)4 2690148

**Egypt + North Africa: Delta Electronics**  
511 Cairo Business Plaza, North 90 street,  
New Cairo, Cairo, Egypt  
Mail: Sales.IA.MEA@deltaww.com



# Managed Industrial GbE DIN-Rail Ethernet Switch DVS-G100 Series User Manual

DVS-G106 | DVS-G112 | DVS-G116

# DVS Managed Industrial

## GbE DIN-Rail Ethernet Switch User Manual

### Table of Contents

#### Chapter 1 Introduction

1.1	Product Overview.....	1-3
1.1.1	High Performance Network Technology.....	1-3
1.1.2	Industrial Grade Reliability .....	1-3
1.1.3	Robust Design .....	1-3
1.1.4	Dimensions(mm) & Product Profile .....	1-4
1.1.5	LED Indicators .....	1-7
1.2	Installation.....	1-8
1.2.1	DIN-Rail Mounting.....	1-8
1.2.2	Wall-Mounting.....	1-9
1.2.3	SFP installation .....	1-9
1.2.4	Wiring the Redundant Power Input .....	1-10
1.2.5	Wiring the Alarm Contact .....	1-11
1.2.6	Wiring the Digital Input.....	1-11
1.3	Package Checklist .....	1-12
1.4	MTBF (Mean Time Between Failures) .....	1-12

#### Chapter 2 User Interface Introduction

2.1	RJ45 Console Configuration.....	2-2
2.2	Telnet Console Configuration .....	2-4
2.3	Web Browser Configuration .....	2-5

#### Chapter 3 Featured Functions

3.1	Basic Setting .....	3-5
3.1.1	System Information.....	3-5
3.1.2	Network Interface .....	3-6

3.1.2.1	IPv4 Network Configuration .....	3-6
3.1.2.2	IPv6 Network Configuration .....	3-7
3.1.2.3	IPv6 Network Neighbor .....	3-8
3.1.3	Port Setting .....	3-9
3.1.3.1	Port Settings .....	3-9
3.1.3.2	LAG Settings .....	3-10
3.1.4	Time .....	3-10
3.1.4.1	SNTP Scalars Configuration .....	3-11
3.1.4.2	SNTP Unicast Server Configuration .....	3-12
3.1.5	DHCP/BOOTP Settings .....	3-12
3.1.5.1	DHCP Server .....	3-12
3.1.5.2	DHCP Relay .....	3-17
3.1.5.3	DHCP L2 Relay .....	3-19
3.1.6	DNS .....	3-22
3.1.6.1	DNS Configuration .....	3-22
3.1.6.2	Host Configuration .....	3-23
3.1.7	System File Update .....	3-24
3.1.7.1	Download File .....	3-24
3.1.7.2	Upload File .....	3-25
3.1.8	Management Access .....	3-27
3.1.8.1	HTTP Configuration .....	3-27
3.1.8.2	HTTPS .....	3-28
3.1.8.3	SSH Configuration .....	3-30
3.1.8.4	Telnet Configuration .....	3-31
3.1.8.5	Console Port .....	3-32
3.1.9	Loopback-Detection .....	3-32
3.1.9.1	Global Configuration .....	3-32
3.1.9.2	Port Configuration .....	3-32
3.1.10	EtherNet/IP .....	3-33
3.2	SNMP Manager .....	3-34
3.2.1	SNMP v1/v2c .....	3-34
3.2.1.1	Community Configuration .....	3-34
3.2.1.2	Trap Configuration .....	3-35
3.2.1.3	Trap Flags .....	3-36
3.2.2	SNMP v3 .....	3-37
3.2.2.1	User Configuration .....	3-37
3.3	Network Redundancy .....	3-38

3.3.1	STP .....	3-38
3.3.1.1	STP Configuration .....	3-42
3.3.1.2	CST Configuration.....	3-43
3.3.1.3	CST Port Configuration .....	3-46
3.3.1.4	CST Port Status .....	3-48
3.3.1.5	MST Configuration .....	3-50
3.3.1.6	MST Port Status .....	3-51
3.3.1.7	STP Statistics .....	3-53
3.3.2	Redundancy.....	3-54
3.3.2.1	ONE RING Configuration.....	3-54
3.3.2.2	ONE CHAIN Configuration .....	3-55
3.3.2.3	ONE COUPLING Configuration .....	3-55
3.3.2.4	Redundancy Cruiser .....	3-56
3.3.3	Redundancy Application Setting .....	3-58
3.4	Virtual LANs .....	3-64
3.4.1	VLAN Mode Configuration .....	3-65
3.4.2	VLAN Configuration .....	3-65
3.4.3	VLAN Membership .....	3-66
3.4.4	VLAN Status .....	3-67
3.4.5	Port PVID Configuration .....	3-67
3.4.6	GVRP Configuration .....	3-68
3.4.7	QinQ VLAN Configuration.....	3-69
3.4.8	MAC Based VLAN.....	3-70
3.4.9	IP Subnet Based VLAN .....	3-71
3.5	Multicast Filtering.....	3-71
3.5.1	IGMP Snooping Configuration .....	3-73
3.5.2	IGMP VLAN Configuration .....	3-74
3.5.3	IGMP Snooping Multicast Forwarding Table .....	3-74
3.5.4	Multicast MAC Address Configuration .....	3-75
3.5.5	GMRP Configuration.....	3-75
3.5.6	Multicast Forwarding Table.....	3-76
3.6	Traffic Prioritization .....	3-77
3.6.1	QoS .....	3-77
3.6.1.1	QoS Setting .....	3-77
3.6.1.2	CoS Queue Mapping.....	3-78
3.6.1.3	DSCP Queue Mapping.....	3-78

3.7	Traffic Control.....	3-80
3.7.1	Port Isolation Configuration .....	3-80
3.8	Port Bandwidth.....	3-81
3.8.1	Storm Control.....	3-81
3.8.1.1	Storm Control Setting .....	3-81
3.8.1.2	Rate Limiting .....	3-82
3.9	Port Trunking.....	3-82
3.9.1	LAG .....	3-83
3.9.1.1	LAG Membership .....	3-83
3.9.1.2	LAG Information.....	3-84
3.10	Access Control List.....	3-84
3.10.1	MAC ACL .....	3-84
3.10.1.1	MAC Rules .....	3-85
3.10.1.2	MAC Binding Configuration.....	3-87
3.10.1.3	MAC Binding Table .....	3-88
3.10.2	ARP ACL.....	3-88
3.10.2.1	ARP Rules.....	3-89
3.10.2.2	ARP Binding Configuration .....	3-90
3.10.2.3	ARP Binding Table.....	3-91
3.11	Security Settings .....	3-91
3.11.1	Security .....	3-91
3.11.1.1	Port Security.....	3-91
3.11.1.2	IP Source .....	3-93
3.11.1.3	802.1X.....	3-94
3.11.2	Management Security .....	3-99
3.11.2.1	Local Users Management .....	3-99
3.11.2.2	RADIUS Server Config.....	3-100
3.11.2.3	RADIUS Statistics .....	3-101
3.11.2.4	TACACS+ Server .....	3-102
3.11.2.5	TACACS+ AS.....	3-102
3.11.2.6	Login Authentication .....	3-103
3.11.2.7	Login User Sessions .....	3-103
3.11.3	Denial of Service .....	3-104
3.12	Monitoring Settings .....	3-104
3.12.1	MAC Address Table .....	3-105
3.12.2	SFP DDM (Only for SFP Module) .....	3-106

3.12.3	System CPU Status.....	3-106
3.12.4	Interface Statistics .....	3-107
3.12.5	ARP Configure.....	3-107
3.12.5.1	Basic.....	3-107
3.12.6	RMON .....	3-108
3.12.6.1	Basic Settings .....	3-108
3.12.6.2	Alarms .....	3-108
3.12.6.3	Events.....	3-109
3.12.6.4	Event Log .....	3-110
3.12.6.5	History .....	3-110
3.12.6.6	RMON Ethernet Statistics.....	3-111
3.12.6.7	Ethernet History Statistics .....	3-113
3.12.7	SYSLOG .....	3-115
3.12.7.1	Show Logs .....	3-115
3.12.7.2	Logs Configuration.....	3-115
3.12.7.3	Syslog Fwd Table .....	3-117
3.12.7.4	Syslog Email Configuration .....	3-118
3.12.7.5	Syslog Email Alarm Table.....	3-118
3.13	Diagnostic Settings .....	3-120
3.13.1	LLDP.....	3-120
3.13.1.1	LLDP Basic Settings .....	3-120
3.13.1.2	LLDP Interface Configuration.....	3-121
3.13.1.3	LLDP TLV Options .....	3-122
3.13.1.4	LLDP Local Information .....	3-123
3.13.1.5	LLDP Neighbor Information .....	3-124
3.13.1.6	LLDP Traffic.....	3-126
3.13.1.7	LLDP-MED Global Configuration.....	3-126
3.13.1.8	LLDP-MED Interface Configuration .....	3-127
3.13.2	Port Mirroring .....	3-128
3.13.2.1	Multiple Port Mirroring.....	3-128
3.14	Auto Warning .....	3-129
3.14.1	Relay Alarm.....	3-129
3.14.1.1	Relay Alarm Setting .....	3-129
3.14.1.2	Relay Alarm Table .....	3-132
3.15	Dual Image .....	3-132
3.15.1	Copy.....	3-132
3.15.2	Configuration.....	3-133

3.16	Save Config.....	3-133
3.16.1	Save Configuration .....	3-133
3.16.2	Auto-Save Configuration .....	3-133
3.16.3	Configuration Copy .....	3-133
3.16.4	Restore .....	3-134
3.16.5	Erase.....	3-134
3.17	Reset .....	3-134
3.17.1	Device Reboot.....	3-134
3.17.2	Factory Default Settings .....	3-135
3.18	Troubleshooting .....	3-135
3.18.1	Ping IPv4 .....	3-135
3.18.2	Ping IPv6 .....	3-136
3.18.3	Traceroute IPv4.....	3-137
3.18.4	Traceroute IPv6.....	3-137
3.19	Logout.....	3-138

## Chapter 4 IEXplorer Utility Introduction

4.1	Starting the Configuration .....	4-3
4.2	Device .....	4-4
4.2.1	Search .....	4-4
4.2.2	Live Viewer.....	4-4
4.3	Settings.....	4-5
4.3.1	Device Configuration.....	4-5
4.3.2	Configuration Web Page .....	4-6
4.4	Tools .....	4-7
4.4.1	IP Setting.....	4-7
4.4.2	Ping Test .....	4-7
4.4.3	Parameter Import.....	4-8
4.4.4	Parameter Export .....	4-8
4.4.5	Device Reboot.....	4-9
4.4.6	Update Firmware.....	4-9
4.5	Help .....	4-10

Appendix A Private MIB Group

A.1 Private MIB Group..... A-2

Appendix B MODBUS TCP Map

B.1 DVS-G106W02-2GF ..... B-2

B.2 DVS-G112W02-4GF ..... B-8

B.3 DVS-G116W02-4GF ..... B-14

Appendix C EtherNet/IP

C.1 DVS-G106W02-2GF ..... C-2

C.2 DVS-G112W02-4GF ..... C-13

C.3 DVS-G116W02-4GF ..... C-23

Appendix D EDS File

D.1 EDS(Electronic Data Sheet) File .....D-2

---

# Chapter 1 Product Introduction

## Table of Contents

- 1.1 Product Overview ..... 1-3**
  - 1.1.1 High Performance Network Technology ..... 1-3
  - 1.1.2 Industrial Grade Reliability ..... 1-3
  - 1.1.3 Robust Design ..... 1-3
  - 1.1.4 Dimensions(mm) & Product Profile ..... 1-4
  - 1.1.5 LED Indicators ..... 1-7
- 1.2 Installation ..... 1-8**
  - 1.2.1 DIN-Rail Mounting ..... 1-8
  - 1.2.2 Wall-Mounting ..... 1-9
  - 1.2.3 SFP installation ..... 1-9
  - 1.2.4 Wiring the Redundant Power Input ..... 1-10
  - 1.2.5 Wiring the Alarm Contact ..... 1-11
  - 1.2.6 Wiring the Digital Input ..... 1-11
- 1.3 Package Checklist ..... 1-12**
- 1.4 MTBF (Mean Time Between Failures) ..... 1-12**

## **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 Product Overview

Thank you for purchasing the DVS Managed Industrial Ethernet Switches. The DVS series switches including Unmanaged and Managed switches. Except the DVS-G100 Series, the DVS series switches are equipped with the intelligent alarm function, and allow the wide range of operating temperature (-40 to 75°C or -20 to 70°C). 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

- 10/100/1000Base-T(X) (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

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

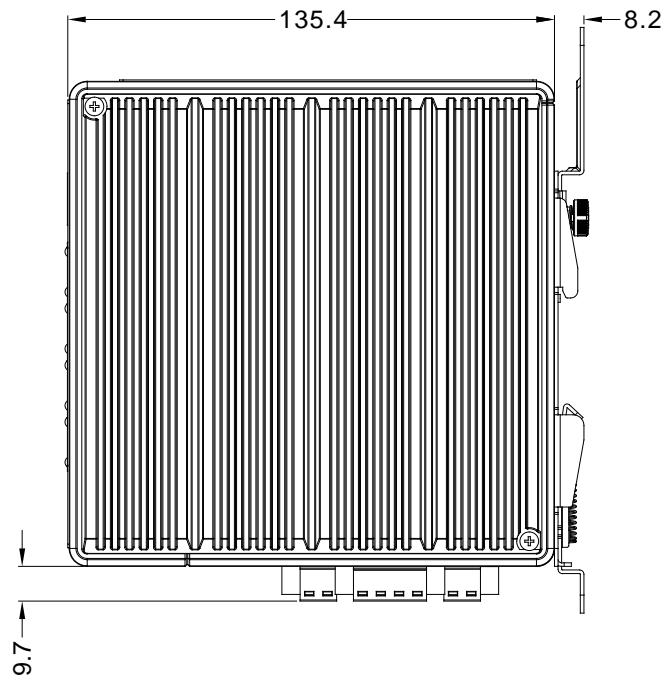
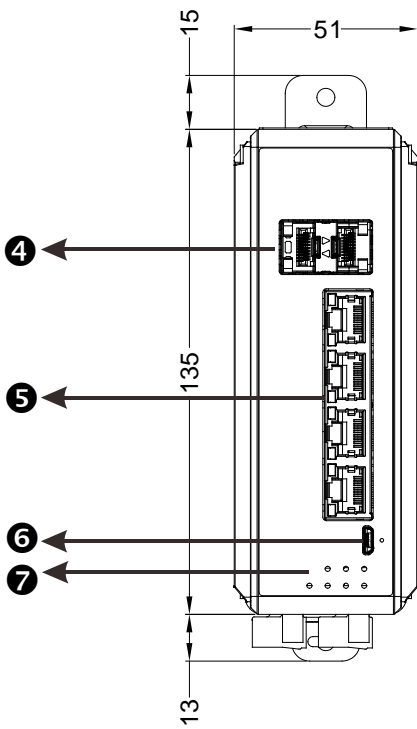
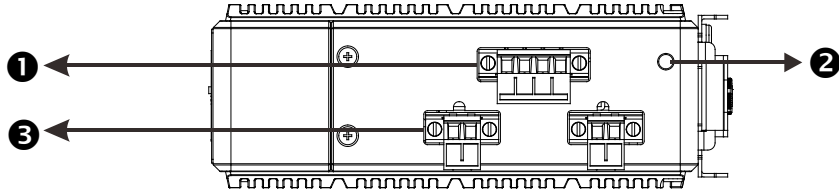
### 1.1.3 Robust Design

- Operating temperature: -40~75°C
- Storage temperature: -40~85°C
- Humidity: 0%~95% (non-condensing)
- Protection: IP40

1

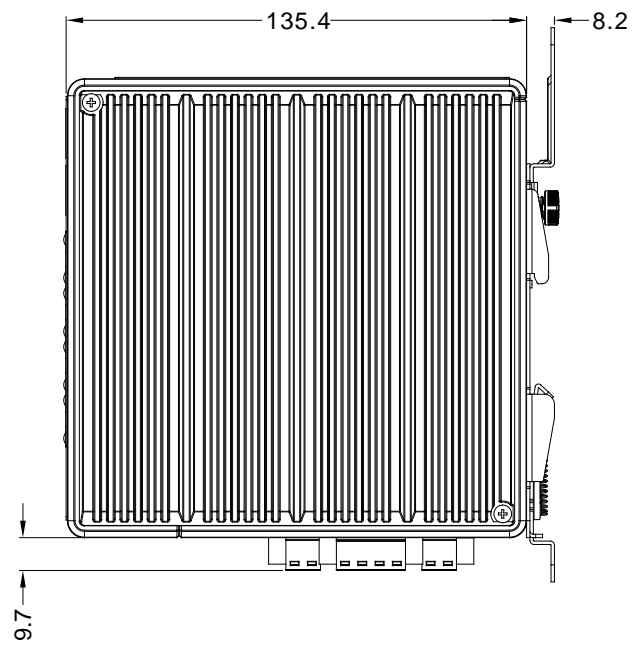
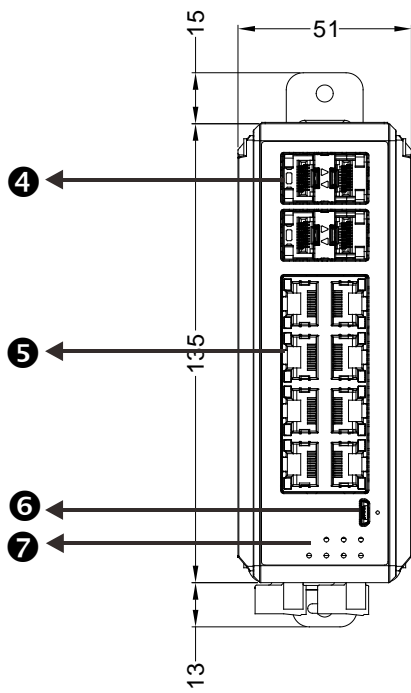
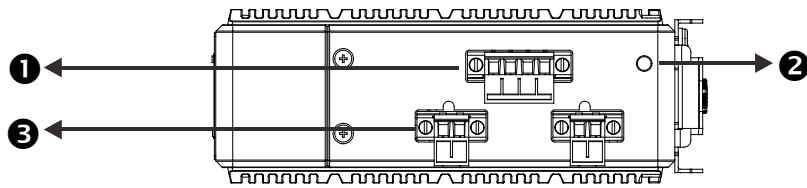
### 1.1.4 Dimensions(mm) & Product Profile

- DVS-G106W02-2GF



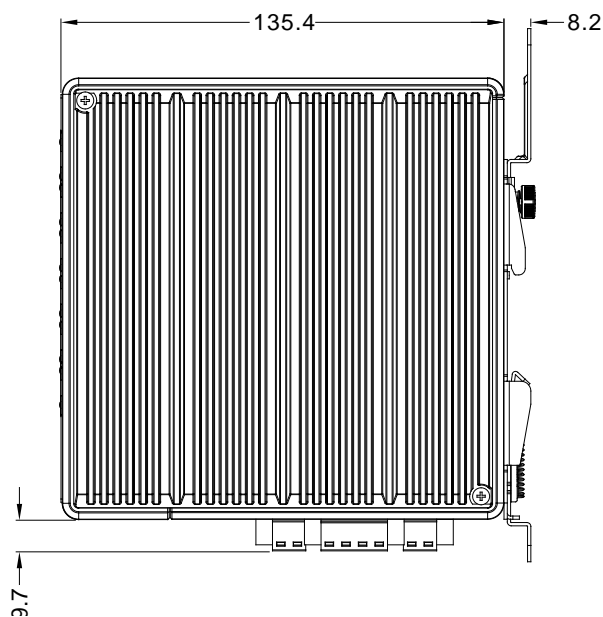
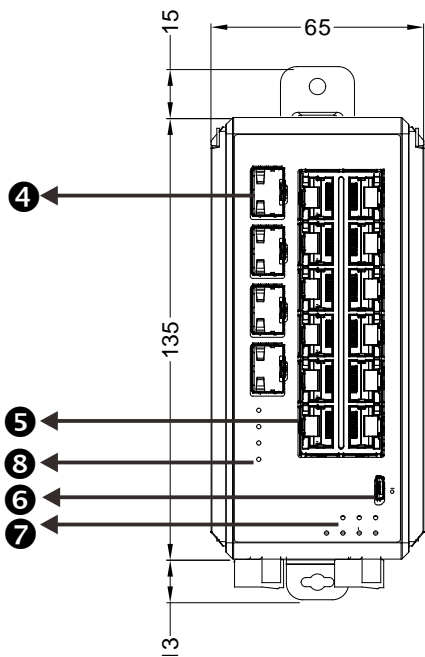
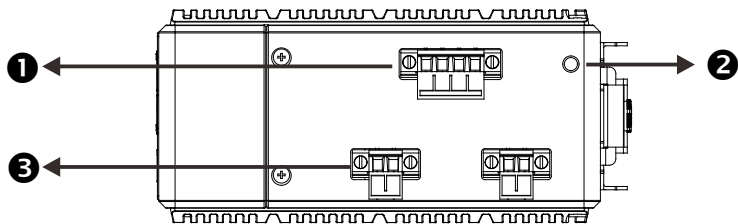
● DVS-G112W02-4GF

1



1

● **DVS-G116W02-4GF**



No	Description
1	DI/DO port
2	Ground screw
3	Power terminal
4	SFP port
5	Ethernet communication port
6	Micro USB CONSOLE port
7	LED indicator
8	Reset button

	DVS-G106W02-2GF	DVS-G112W02-1GF	DVS-116W02-4GF
<b>Case</b>	IP40 Metal Case		
<b>Dimension(mm)</b>	135H x 51W x 135D	135H x 51W x 135D	135H x 65W x 135D
<b>Weight(g)</b>	520	500	564

### 1.1.5 LED Indicators

LED		Color	Status	Description
SYS	Green	ON	The system is normal.	
		Blinking	The system is booting.	
	Red	OFF	The system is abnormal.	
ALARM	Red	ON	The communication is interrupted, power failure, or alarm event which has been configured happened.	
		OFF	The communication is NOT interrupted, power failure, or alarm event which has been configured doesn't happen.	
PWR1/ PWR2	Green	ON	The power is supplied normally.	
		OFF	The power is not supplied.	
DI	Green	ON	The DI is triggered.	
		OFF	The DI is not triggered.	
RJ45 (Copper)	10/100/1000M	Green	ON	Ethernet ports capable of are 1000Mbps
			OFF	Ethernet port is inactive
		Amber	ON	Ethernet ports capable of are 100/10Mbps
			OFF	Ethernet port is inactive
	LINK/ACT	Amber	ON	The Network communication connection has been established.
			Blinking	Data is transmitting
OFF			Ethernet port is inactive	
SFP (Fiber)	100/1000M	Green	ON	SPF ports capable of are 1000Mbps
			Blinking	Data is transmitting at 1000Mbps
			OFF	SPF port is inactive
		Amber	ON	SPF ports capable of are 100Mbps
			Blinking	Data is transmitting at 100Mbps
			OFF	SPF port is inactive
R.M/CPLG.R	Amber	ON	As a master of ONE RING, or a forwarding path of Coupling Ring.	
		Blinking	Any node disconnection is occurred in ONE RING or Coupling Ring.	
		OFF	A slave of ONE RING, or ONE RING or Coupling Ring is not available.	
C.HD/C.TL	Green	ON	As a head or a tail of ONE CHAIN.	
		Blinking	As a head or a tail of ONE CHAIN, any node disconnection is occurred.	
		OFF	ONE CHAIN is not available.	

## 1.2 Installation

### 1.2.1 DIN-Rail Mounting

#### DIN-rail mounting①:

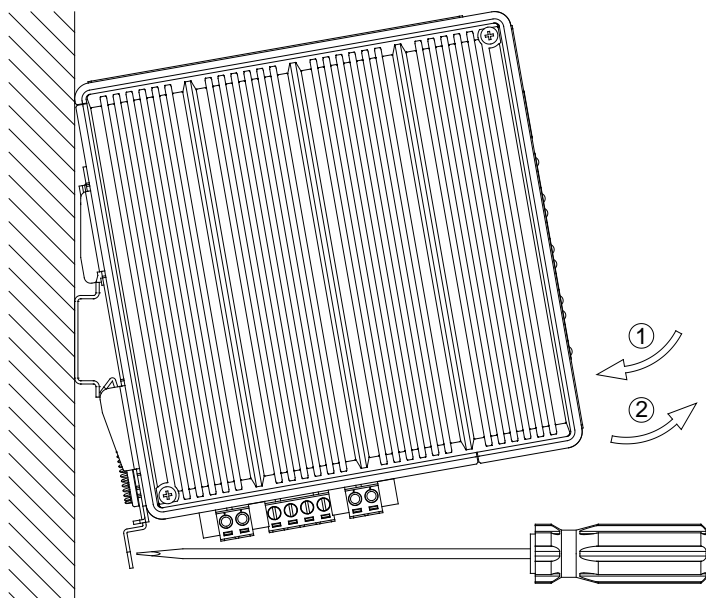
Step 1: Hook the upper end of the DIN clip of the DVS series switch on the DIN-Rail.

Step 2: Lightly push the DVS series switch toward the DIN-Rail until they contact each other closely.

#### DIN-rail removal②:

Step 1: Insert the flat-blade screwdriver into the DIN clip and pull the DIN clip downward.

Step 2: Pull the DVS series switch, and you can remove it from the DIN-Rail

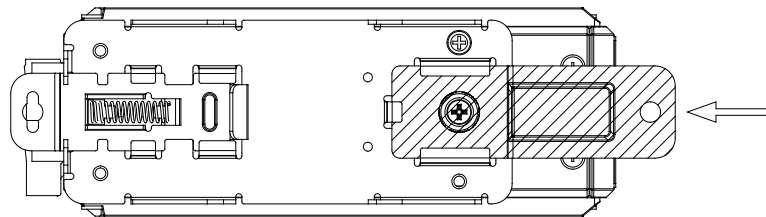


## 1.2.2 Wall-Mounting

### Wall-Mounting:

Step 1: Insert the wall mounting bracket into the slot on the rear panel of the DVS series switch, and tighten the screw on it, as shown in the diagram below.

Step 2: Place the wall mounting bracket in an appropriate position, and tighten the two screws on the bracket and the DIN clip.



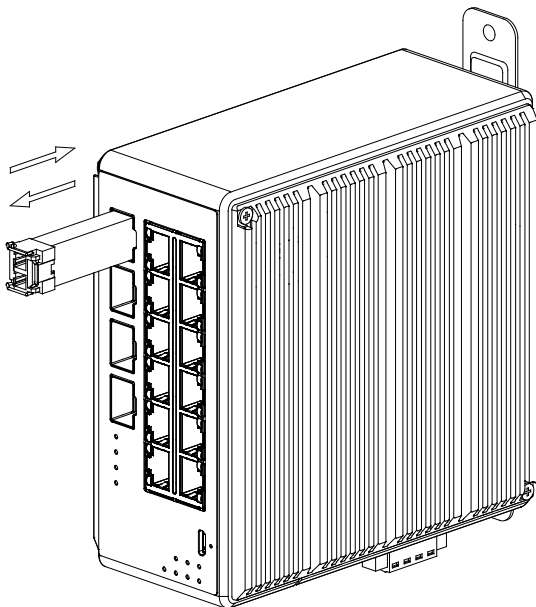
## 1.2.3 SFP installation

### Insert

Insert SFP Module into the SFP combo port.

### Remove

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



1



**Note:**

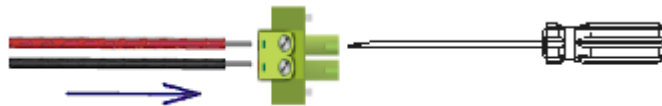
- Delta has LCP-100 and LCP-1000 series SFP module. DVS switch can promise 100% compatible with Delta SFP module.
- The actual link distance of a particular fiber optic link given the optical budget, the number of connectors and splices, and cabling quantity. Please measure and verify the actual link loss values once the link is established to identify any potential performance issues.

### 1.2.4 Wiring the Redundant Power Input

The DVS series switches are equipped with one to two sets of DC input (PWR1 / PWR2). Both sets of DC input can be connected to a wide range of power sources (12 to 48VDC). If one power source fails, the other live source can work as a backup to ensure that the machine operates normally. (Should connected with SELV power sources)

Step 1: Insert the negative and positive DC wires into the terminal block, and make sure that the positive DC wire is connected to V1+ or V2+, and that the negative DC wire is connected to 0V.

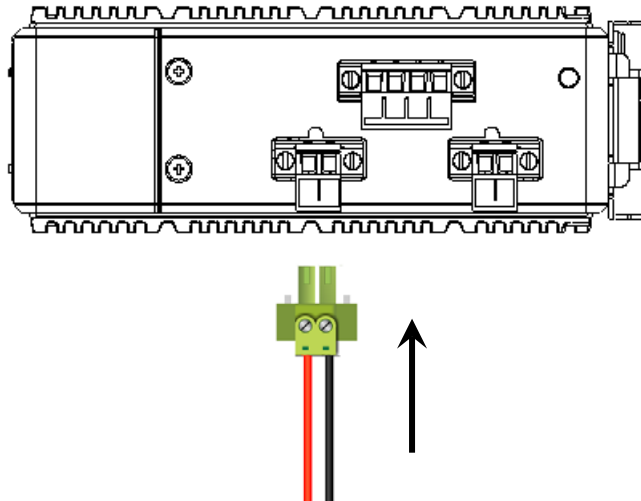
Step 2: To prevent the loose DC wires, tighten the wire clamp screws on the terminal block connector with the flat-blade screwdriver.



**Note:**

Please use copper wire 60/75°C, conductor 16 to 24 AWG; screw up at torque 4.5 in-lbs

Step 3: Insert the plastic terminal block connector into the terminal block receptor on the DVS series switch.

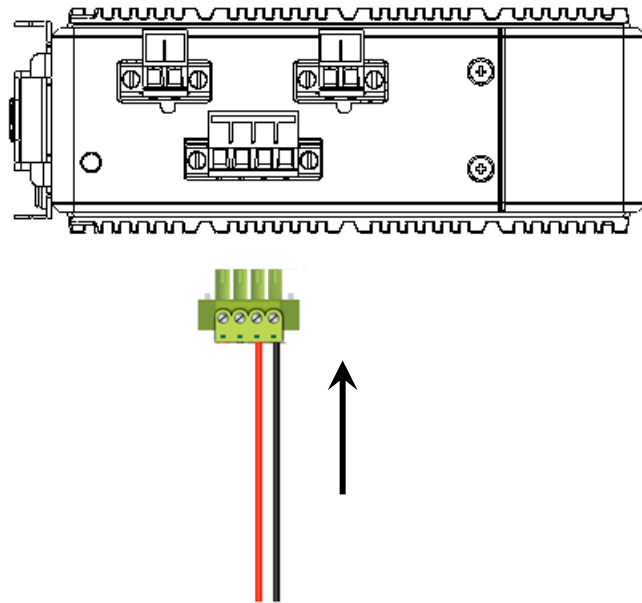


**Note:**

Grounding the ground terminal or Protective conductor terminal (PE) on the DVS series switch can avoid the noise effect due to the electromagnetic interference (EMI).

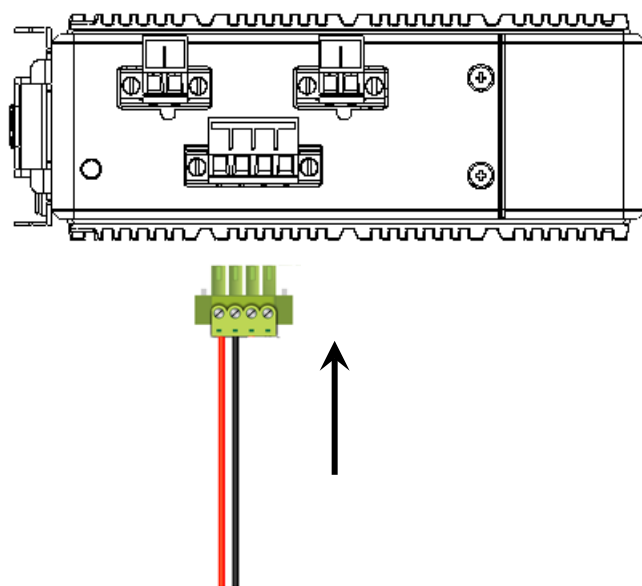
### 1.2.5 Wiring the Alarm Contact

The DVS-G100 series switches are equipped with one alarm. The alarm contact is a dry relay. If one of the two power sources fails, one of digital input is triggered or the communication is interrupted, the contact will turns from an “OPEN” circuit to a “CLOSED” circuit. The relay can be connected to a 1A/24VDC or 0.5/48VDC power source.



### 1.2.6 Wiring the Digital Input

The DVS-G100 series switches are equipped with one sets of digital input. If the power source between 0 to 5V, the state of DI is OFF. If the power source between 11 to 30V, the state of DI is ON. The maximum input current is 6mA. (Note: DI should connected with SELV circuit only.)



## 1.3 Package Checklist

Unpack the package carefully and check the package contents. The package should contain the following items:

- One Delta DVS Managed Ethernet Switch
- Protective Caps for unused RJ45 ports and fiber ports
- Wall mounting Plate x1
- Micro-USB (RS-232 in Micro-USB connector) x1
- 2-PIN Terminal Block x 2, 4-PIN Terminal Block x1
- User manual and Software CD
- Instruction Sheet



**Note:**

Verify that nothing is missing from the DVS-G100 Series package by using the check list above. If any item is found missing or damaged, please contact your local sales representative for support.

## 1.4 MTBF (Mean Time Between Failures)

DVS-G106W02-2GF : More than 2,336,000 hours.

DVS-G112W02-4GF : More than 1,616,000 hours.

DVS-G116W02-4GF : More than 974,000 hours.

---

## Chapter 2 User Interface Introduction

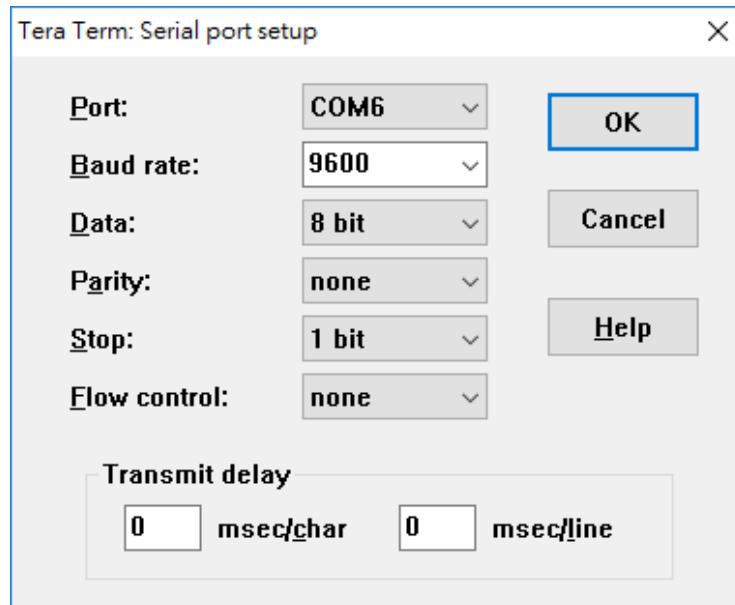
### Table of Contents

2.1	RJ45 Console Configuration.....	2-2
2.2	Telnet Console Configuration .....	2-3
2.3	Web Browser Configuration.....	2-4

## 2.1 USB Console Configuration

Delta DVS G100 series managed switch supports configuration using the CLI interface, available on the Micro USB port to RS232 interface. You can use the terminal software to connect to Delta DVS G100 series managed switch.

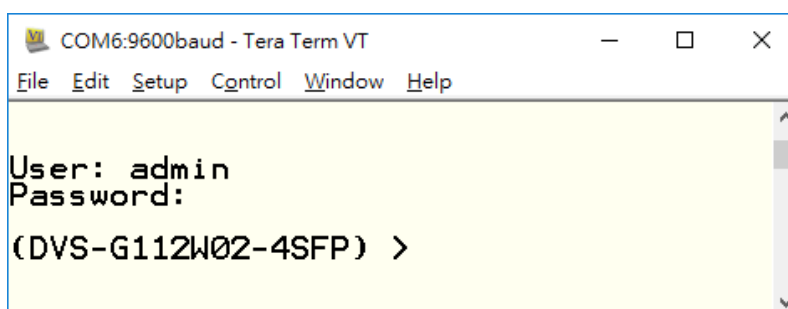
1. Open the terminal software, and select an appropriate COM port for **Console Connection**, **9600** for **Baud Rate**, **8** for **Data Bits**, **None** for **Parity**, and **1** for **Stop Bits**, **None** for **Flow Control**.



**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 enter "en" and then "?" to list the commands.

```

COM6:9600baud - Tera Term VT
File Edit Setup Control Window Help

(DVS-G112W02-4SFP) > en
(DVS-G112W02-4SFP) # ?

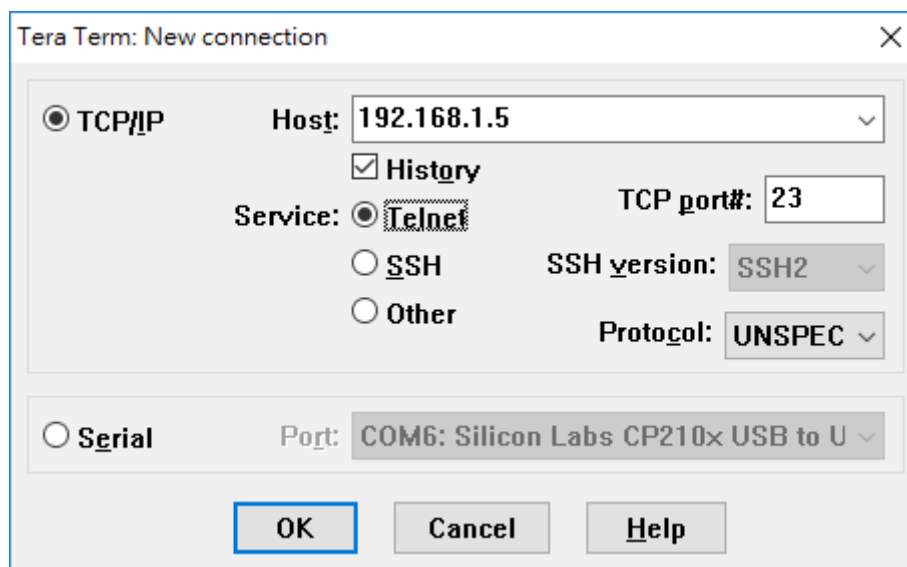
boot                Marks the given image as active for subsequent
                    re-boots.
clear               Resets configuration to factory defaults.
clock              Manage the system clock.
configure          Enter into Global Config Mode.
copy               Copy files.
debug              Configure debug flags.
delete             Deletes given image on the node.
dot1x              Configure dot1x EXEC mode parameters
erase              Erase configuration file.
exit               Exit to EXEC mode.
factory            Resets the switch to factory defaults states.
filedescr          Sets text description for a given image.
listuser           List all valid users, along with their permissible
                    mode.
logout             Exit this session. Any unsaved changes are lost.
no                no
ping              Send ICMP echo packets to a specified IP address.
reload             Reload stack or a switch in the stack.
restore            Set the flag of the restore.
run                run cable diagnostics.
save              Save the running configuration to NVRAM.
script            Apply/Delete/List/Show Configuration Scripts.
sfp               Configure SFP EXEC mode parameters
show              Display Switch Options and Settings.
traceroute        Trace route to destination.
vlan              Type 'vlan database' to enter into VLAN mode.
vtss              Read or write vtss chip's register
write             Save the current configuration to NVRAM.

```

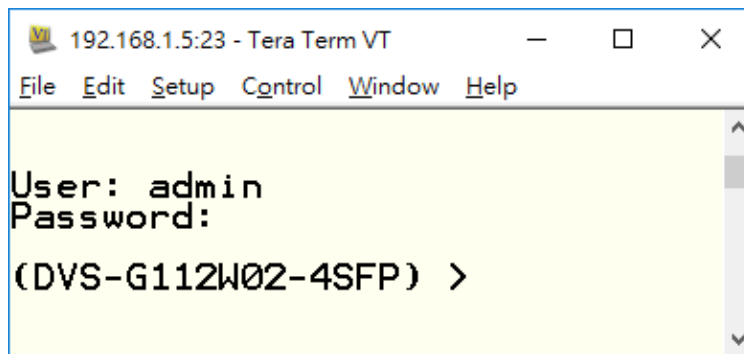
## 2.2 Telnet Console Configuration

A Delta Layer 3 managed 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.X" to login to a Delta switch.



2. After entering the default user name is "admin" and the password is blank., you can use the CLI command to control the switch.



```
192.168.1.5:23 - Tera Term VT
File Edit Setup Control Window Help
User: admin
Password:
(DVS-G112W02-4SFP) >
```

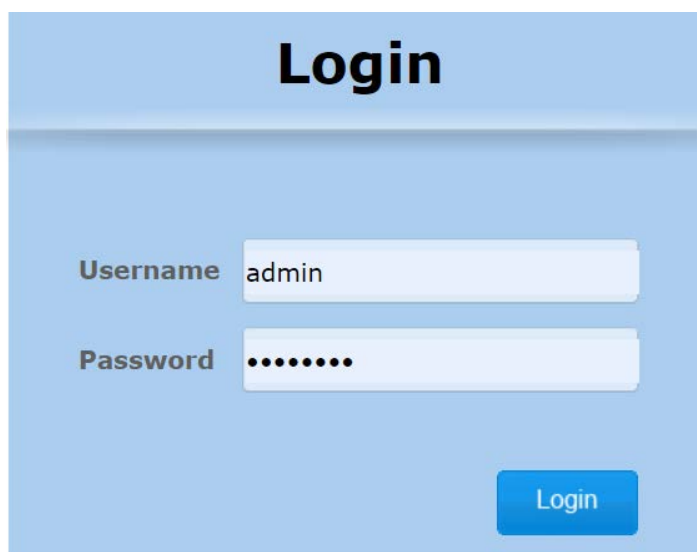
**Note:**

1. The IP Address by default is 192.168.1.5

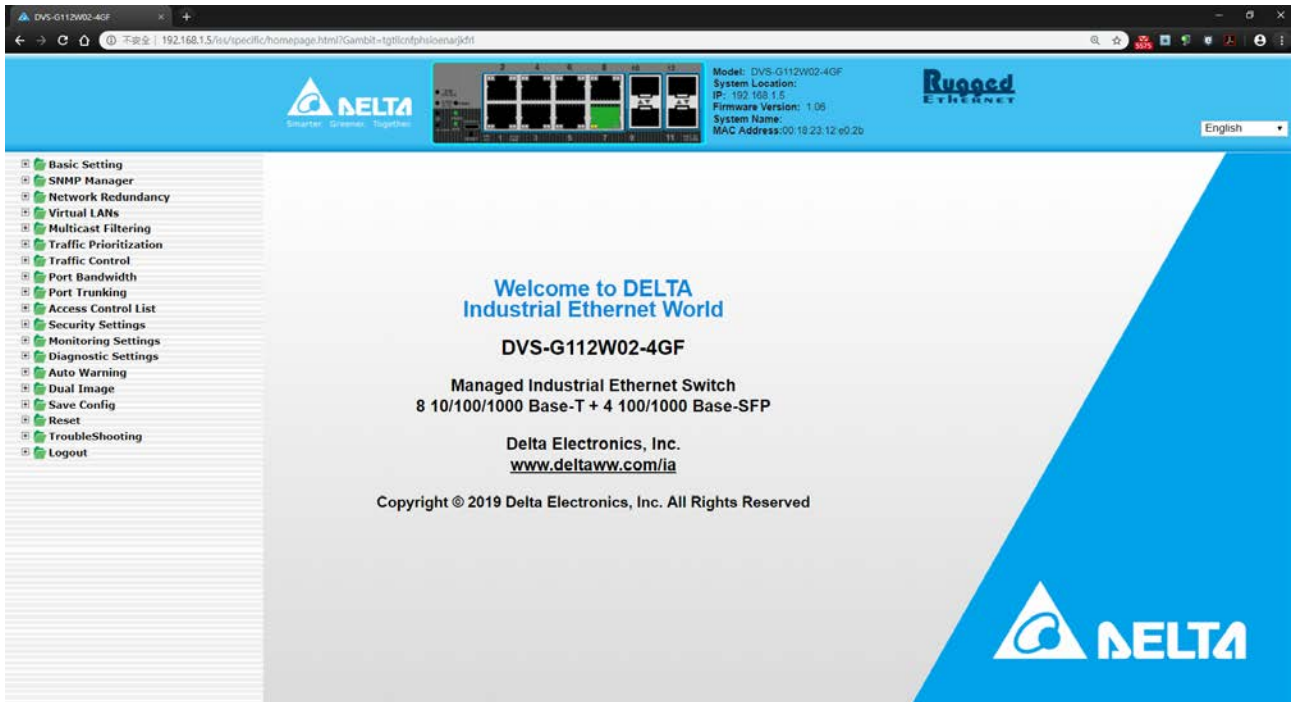
## 2.3 Web Browser Configuration

A Delta Layer 3 managed switch supports a friendly GUI for normal users to configure the switch. You can monitor the port status of a Delta PoE managed switch, and configure the settings of each function via the web interface.

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.)

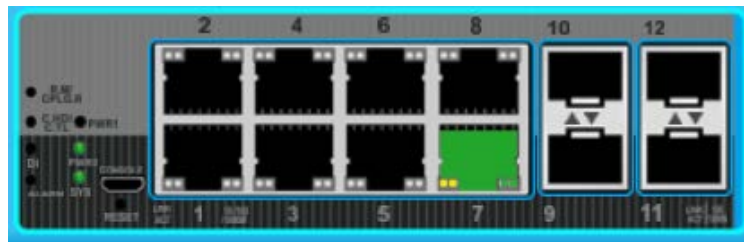
**Note:**

1. The default user name “admin” is in the lowercase not uppercase.
  2. By default, IE5.0 or later version does not allow Java Applets to open sockets. You need to explicitly modify the browser setting in order to enable Java Applets to use network ports.
2. You can use the menu tree in the left side frame to find the function you want to configure. And configure the detailed settings in the right side frame.



2

3. The port status and the LED status on the switch can be monitored in the top frame.



**MEMO**

---

## Chapter 3 Featured Functions

### Table of Contents

<b>3.1</b>	<b>Basic Setting .....</b>	<b>3-5</b>
3.1.1	System Information.....	3-5
3.1.2	Network Interface .....	3-6
3.1.2.1	IPv4 Network Configuration .....	3-6
3.1.2.2	IPv6 Network Configuration .....	3-7
3.1.2.3	IPv6 Network Neighbor .....	3-8
3.1.3	Port Setting.....	3-9
3.1.3.1	Port Settings.....	3-9
3.1.3.2	LAG Settings.....	3-10
3.1.4	Time .....	3-10
3.1.4.1	SNTP Scalars Configuration.....	3-11
3.1.4.2	SNTP Unicast Server Configuration .....	3-12
3.1.5	DHCP/BOOTP Settings .....	3-12
3.1.5.1	DHCP Server .....	3-12
3.1.5.2	DHCP Relay .....	3-17
3.1.5.3	DHCP L2 Relay .....	3-19
3.1.6	DNS .....	3-22
3.1.6.1	DNS Configuration.....	3-22
3.1.6.2	Host Configuration .....	3-23
3.1.7	System File Update.....	3-24
3.1.7.1	Download File .....	3-24
3.1.7.2	Upload File .....	3-26
3.1.8	Management Access .....	3-27
3.1.8.1	HTTP Configuration .....	3-27
3.1.8.2	HTTPS.....	3-28
3.1.8.3	SSH Configuration .....	3-30
3.1.8.4	Telnet Configuration.....	3-31
3.1.8.5	Console Port.....	3-32
3.1.9	Loopback-Detection .....	3-32
3.1.9.1	Global Configuration .....	3-32
3.1.9.2	Port Configuration .....	3-32
3.1.10	EtherNet/IP .....	3-33
<b>3.2</b>	<b>SNMP Manager .....</b>	<b>3-34</b>
3.2.1	SNMP v1/v2c .....	3-34
3.2.1.1	Community Configuration.....	3-34
3.2.1.2	Trap Configuration.....	3-35
3.2.1.3	Trap Flags.....	3-36
3.2.2	SNMP v3.....	3-37
3.2.2.1	User Configuration .....	3-37
<b>3.3</b>	<b>Network Redundancy .....</b>	<b>3-38</b>
3.3.1	STP .....	3-38
3.3.1.1	STP Configuration.....	3-42
3.3.1.2	CST Configuration .....	3-43

3.3.1.3	CST Port Configuration .....	3-46
3.3.1.4	CST Port Status .....	3-48
3.3.1.5	MST Configuration .....	3-50
3.3.1.6	MST Port Status .....	3-51
3.3.1.7	STP Statistics .....	3-53
3.3.2	Redundancy .....	3-54
3.3.2.1	ONE RING Configuration .....	3-54
3.3.2.2	ONE CHAIN Configuration .....	3-55
3.3.2.3	ONE COUPLING Configuration .....	3-55
3.3.2.4	Redundancy Cruiser .....	3-56
3.3.3	Redundancy Application Setting .....	3-58
<b>3.4</b>	<b>Virtual LANs .....</b>	<b>3-64</b>
3.4.1	VLAN Mode Configuration .....	3-65
3.4.2	VLAN Configuration .....	3-65
3.4.3	VLAN Membership .....	3-66
3.4.4	VLAN Status .....	3-67
3.4.5	Port PVID Configuration .....	3-67
3.4.6	GVRP Configuration .....	3-68
3.4.7	QinQ VLAN Configuration .....	3-69
3.4.8	MAC Based VLAN .....	3-70
3.4.9	IP Subnet Based VLAN .....	3-71
<b>3.5</b>	<b>Multicast Filtering .....</b>	<b>3-71</b>
3.5.1	IGMP Snooping Configuration .....	3-73
3.5.2	IGMP VLAN Configuration .....	3-74
3.5.3	IGMP Snooping Multicast Forwarding Table .....	3-75
3.5.4	Multicast MAC Address Configuration .....	3-75
3.5.5	GMRP Configuration .....	3-76
3.5.6	Multicast Forwarding Table .....	3-77
<b>3.6</b>	<b>Traffic Prioritization .....</b>	<b>3-77</b>
3.6.1	QoS .....	3-77
3.6.1.1	QoS Setting .....	3-78
3.6.1.2	CoS Queue Mapping .....	3-78
3.6.1.3	DSCP Queue Mapping .....	3-79
<b>3.7</b>	<b>Traffic Control .....</b>	<b>3-81</b>
3.7.1	Port Isolation Configuration .....	3-81
<b>3.8</b>	<b>Port Bandwidth .....</b>	<b>3-81</b>
3.8.1	Storm Control .....	3-82
3.8.1.1	Storm Control Setting .....	3-82
3.8.1.2	Rate Limiting .....	3-83
<b>3.9</b>	<b>Port Trunking .....</b>	<b>3-83</b>
3.9.1	LAG .....	3-84
3.9.1.1	LAG Membership .....	3-84
3.9.1.2	LAG Information .....	3-85
<b>3.10</b>	<b>Access Control List .....</b>	<b>3-85</b>
3.10.1	MAC ACL .....	3-85
3.10.1.1	MAC Rules .....	3-86
3.10.1.2	MAC Binding Configuration .....	3-88
3.10.1.3	MAC Binding Table .....	3-89
3.10.2	ARP ACL .....	3-89

3.10.2.1	ARP Rules.....	3-90
3.10.2.2	ARP Binding Configuration .....	3-91
3.10.2.3	ARP Binding Table .....	3-92
<b>3.11</b>	<b>Security Settings .....</b>	<b>3-92</b>
3.11.1	Security.....	3-92
3.11.1.1	Port Security.....	3-92
3.11.1.2	IP Source .....	3-94
3.11.1.3	802.1X.....	3-95
3.11.2	Management Security.....	3-100
3.11.2.1	Local Users Management.....	3-100
3.11.2.2	RADIUS Server Config.....	3-101
3.11.2.3	RADIUS Statistics.....	3-102
3.11.2.4	TACACS+ Server .....	3-103
3.11.2.5	TACACS+ AS .....	3-103
3.11.2.6	Login Authentication.....	3-104
3.11.2.7	Login User Sessions.....	3-104
3.11.3	Denial of Service.....	3-105
<b>3.12</b>	<b>Monitoring Settings .....</b>	<b>3-105</b>
3.12.1	MAC Address Table .....	3-106
3.12.2	SFP DDM (Only for SFP Module).....	3-107
3.12.3	System CPU Status.....	3-107
3.12.4	Interface Statistics .....	3-108
3.12.5	ARP Configure.....	3-108
3.12.5.1	Basic.....	3-108
3.12.6	RMON.....	3-109
3.12.6.1	Basic Settings .....	3-109
3.12.6.2	Alarms .....	3-109
3.12.6.3	Events.....	3-110
3.12.6.4	Event Log.....	3-111
3.12.6.5	History .....	3-111
3.12.6.6	RMON Ethernet Statistics .....	3-112
3.12.6.7	Ethernet History Statistics .....	3-114
3.12.7	SYSLOG.....	3-116
3.12.7.1	Show Logs .....	3-116
3.12.7.2	Logs Configuration.....	3-116
3.12.7.3	Syslog Fwd Table.....	3-118
3.12.7.4	Syslog Email Configuration .....	3-119
3.12.7.5	Syslog Email Alarm Table .....	3-119
<b>3.13</b>	<b>Diagnostic Settings.....</b>	<b>3-121</b>
3.13.1	LLDP.....	3-121
3.13.1.1	LLDP Basic Settings.....	3-121
3.13.1.2	LLDP Interface Configuration.....	3-122
3.13.1.3	LLDP TLV Options .....	3-123
3.13.1.4	LLDP Local Information.....	3-124
3.13.1.5	LLDP Neighbor Information.....	3-125
3.13.1.6	LLDP Traffic.....	3-127
3.13.1.7	LLDP-MED Global Configuration.....	3-127
3.13.1.8	LLDP-MED Interface Configuration.....	3-128
3.13.2	Port Mirroring.....	3-129
3.13.2.1	Multiple Port Mirroring.....	3-129
<b>3.14</b>	<b>Auto Warning .....</b>	<b>3-130</b>
3.14.1	Relay Alarm.....	3-130

3.14.1.1	Relay Alarm Setting .....	3-130
3.14.1.2	Relay Alarm Table.....	3-133
<b>3.15</b>	<b>Dual Image .....</b>	<b>3-133</b>
3.15.1	Copy.....	3-133
3.15.2	Configuration.....	3-134
<b>3.16</b>	<b>Save Config .....</b>	<b>3-134</b>
3.16.1	Save Configuration .....	3-134
3.16.2	Auto-Save Configuration .....	3-134
3.16.3	Configuration Copy .....	3-134
3.16.4	Restore .....	3-135
3.16.5	Erase.....	3-135
<b>3.17</b>	<b>Reset .....</b>	<b>3-135</b>
3.17.1	Device Reboot .....	3-135
3.17.2	Factory Default Settings .....	3-136
<b>3.18</b>	<b>Troubleshooting .....</b>	<b>3-136</b>
3.18.1	Ping IPv4.....	3-136
3.18.2	Ping IPv6.....	3-137
3.18.3	Traceroute IPv4 .....	3-138
3.18.4	Traceroute IPv6 .....	3-138
3.19	Logout .....	3-139

## 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.

### 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.

#### System Information

Switch Status	
<b>System Name</b>	<input type="text"/>
<b>System Location</b>	<input type="text"/>
<b>System Contact</b>	<input type="text"/>
<b>Serial Number</b>	DVS1120119100009
<b>System Object ID</b>	1.3.6.1.4.1.6785.501.7.6
<b>Date &amp; Time</b>	Thu 00:04:50 1970-01-01
<b>System Up Time</b>	0 hrs, 4 mins, 52 secs
<b>MAC Address</b>	00:18:23:12:e0:2b
<b>Auto Save</b>	Disable

Versions		
Model Name	Boot Version	Software Version
DVS-G112W02-4GF	0.6	1.06

- System Status

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

Description	Factory default
<b>MAC Address</b>	
The MAC address of the switch.	Fixed
<b>Auto Save</b>	
When enable it, any configuration will be saved to flash automatically in WEB/CLI/SNMP and startup-configuration and backup-configuration can't be erased through WEB or CLI.	Disable

● **Versions**

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

3

### 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.

#### 3.1.2.1 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**.

### IPv4 Network Interface Configuration

**IPv4 Network Interface Configuration**

**IP Address**

**Subnet Mask**

**Default Gateway**

**MAC Address**

**Current Network Configuration Protocol**  None  DHCP  BOOTP


**Management VLAN ID**



**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
<b>IP Address</b>	
Input the IP address of the IPv4 network interface.  <b>Note:</b> 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
<b>Subnet Mask</b>	
Input the IP subnet mask of the IPv4 network interface.	255.255.0..
<b>Default Gateway</b>	
Input the default gateway of the IPv4 network interface.	0.0.0.0.
<b>MAC Address</b>	
This field displays the MAC address of the switch.	MAC address
<b>Current Network Configuration Protocol</b>	
Select one item to specify how the switch gets its IP information: <ul style="list-style-type: none"> <li>● <b>None:</b> Specify the static IP address information.</li> <li>● <b>DHCP:</b> DVS will be a DHCP client, waiting for the DHCP server to assign an IP address. At this point DVS IP address will become 169.254.100.100 if there is no DHCP server to assign an IP address.</li> <li>● <b>BOOTP:</b> DVS will be a BOOT client, waiting for the BOOT server to assign an IP address. At this point DVS IP address will become 169.254.100.100 if there is no BOOTP server to assign an IP address.</li> </ul>	None
<b>Management VLAN ID</b>	
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"

## IPv6 Network Interface Configuration

**Global Configuration**

**Admin Mode**  Disable  Enable

**IPv6 Gateway**

---

**IPv6 Network Interface Configuration**

	IPv6 Prefix/Prefix Length	EUI64
<input type="checkbox"/>	fe80::218:23ff:fe12:e02b/64	- ▾ True


## ● Global Configuration

Description	Factory default
<b>Admin Mode</b>	
Specify the IPv6 administrative status of the network interface by selecting one item: <ul style="list-style-type: none"> <li>● <b>Disable:</b> IPv4 only mode. Only support IPv4, not support IPv6.</li> <li>● <b>Enable:</b> IPv4 / IPv6 mode. Support both IPv4 and IPv6.</li> </ul>	Enable

<b>IPv6 Gateway</b>	
Input the IPv6 address of the IPv6 gateway.	None

● **IPv6 Network Interface Configuration**

Description	Factory default
<b>IPv6 Prefix / Prefix Length</b>	
Enter the IPv6 address followed by a slash and then the prefix length of the network interface.	IPv6 address
<b>EUI64</b>	
Specify whether the IPv6 address is in the 64-bit extended unique identifier (EUI-64) format: <ul style="list-style-type: none"> <li>• <b>True:</b> The IPv6 address is in the EUI-64 format.</li> <li>• <b>False:</b> The IPv6 address is not in the EUI-64 format.</li> </ul>	None

 **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**

IPv6 Network Interface Neighbor Table		
IPv6 Address	MAC Address	Neighbor State
fe80::4419:f6e8:dd10:be18	60:d8:19:18:cf:74	Stale

[Refresh](#)

**IPv6 Network Interface Neighbor Table**

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

### 3.1.3 Port Setting

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
<input type="checkbox"/>			-		-	-		-	-	-
<input type="checkbox"/>	0/1	Link Up	Enable		Normal	Auto	100 Mbps Full Duplex	Disable	Disable	Enable
<input type="checkbox"/>	0/2	Link Down	Enable		Normal	Auto	Unknown	Disable	Disable	Enable
<input type="checkbox"/>	0/3	Link Down	Enable		Normal	Auto	Unknown	Disable	Disable	Enable
<input type="checkbox"/>	0/4	Link Down	Enable		Normal	Auto	Unknown	Disable	Disable	Enable
<input type="checkbox"/>	0/5	Link Down	Enable		Normal	Auto	Unknown	Disable	Disable	Enable
<input type="checkbox"/>	0/6	Link Down	Enable		Normal	Auto	Unknown	Disable	Disable	Enable

#### ● Port Settings

Description	Factory default
<b>Port</b>	
This field displays the interface number.	<i>interface number</i>
<b>Link Status</b>	
This field displays the connection of the interface. <ul style="list-style-type: none"> <li><b>Link Up:</b> There is a network device connecting to the interface.</li> <li><b>Link Down:</b> No network device is connecting to the interface.</li> </ul>	Link down
<b>Admin Mode</b>	
The administrative state of the interface: <ul style="list-style-type: none"> <li><b>Enable:</b> The interface is switched on and the network device can connect to the interface.</li> <li><b>Disable:</b> The interface is switched off and the network device can not connect to the interface.</li> </ul>	Enable
<b>Alias</b>	
Specify an alias for the port to help administrators differentiate between different ports. For example: Head port.	<i>None</i>
<b>Port Type</b>	
This field displays whether the interface is a member of a port channel: <ul style="list-style-type: none"> <li><b>Trunk Member:</b> The interface is a member of a link aggregation group.</li> <li><b>Normal:</b> The interface is not a member of a link aggregation group (port channel).</li> </ul>  <b>Note:</b> If you add ports in the lag, the port type will show "Trunk Member". The LAG configuration could be configured in Port Trunk.	Normal
<b>Physical Mode</b>	
Specify the speed capability of each interface: <ul style="list-style-type: none"> <li><b>Auto:</b> 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.</li> <li><b>10 Mbps Half Duplex:</b> Indicates that the interface works at 10 Mbps in the half duplex mode.</li> <li><b>10 Mbps Full Duplex:</b> Indicates that the interface works at 10 Mbps in the full duplex mode.</li> <li><b>100 Mbps Half Duplex:</b> Indicates that the interface works at 100 Mbps in the half duplex mode.</li> <li><b>100 Mbps Full Duplex:</b> Indicates that the interface works at 100 Mbps in the full duplex mode.</li> </ul>	Auto
<b>Physical Status</b>	
This field displays the actual port speed and the duplex mode.	None
<b>Flow Control Mode</b>	
This field displays whether the flow control is enabled for the port: <ul style="list-style-type: none"> <li><b>Enable:</b> The flow control is enabled. If the port buffers become full, the switch sends pause packets.</li> </ul>	Disable

Description	Factory default
<ul style="list-style-type: none"> <li><b>Disable:</b> The flow control is disabled. If the port buffers become full, the switch does not send pause packets.</li> </ul>	
<b>Jumbo Frame</b>	
The field displays whether the jumbo frame is enabled for the port. <ul style="list-style-type: none"> <li><b>Enable:</b> The jumbo frame is enabled. The switch supports a fixed jumbo frame size - 9000 bytes payload (9018 bytes frame) size.</li> <li><b>Disable:</b> The jumbo frame is disabled.</li> </ul>	Disable
<b>Link Trap</b>	
Specify whether to send a trap when the interface link status changes: <ul style="list-style-type: none"> <li><b>Enable:</b> When the link status changes, the switch sends a trap. This is the default setting.</li> <li><b>Disable:</b> When the link status changes, the switch does not send a trap.</li> </ul>	Enable

### 3.1.3.2 LAG Settings

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

#### LAG Settings

LAG Settings					
	Port	Link Status	Admin Mode	Jumbo Frame	Link Trap
<input type="checkbox"/>			- ▾	- ▾	- ▾
<input type="checkbox"/>	po1	Link Down	Enable	Disable	Enable
<input type="checkbox"/>	po2	Link Down	Enable	Disable	Enable
<input type="checkbox"/>	po3	Link Down	Enable	Disable	Enable

- LAG Settings**

Description	Factory default
<b>Port</b>	
This field shows the interface number.	<i>interface number</i>
<b>Link Status</b>	
This field shows the connection of the interface. <ul style="list-style-type: none"> <li><b>Link Up:</b> The interface is connected to another device.</li> <li><b>Link Down:</b> The interface is not connected to another device.</li> </ul>	Link Down
<b>Admin Mode</b>	
Specify the administrative state of the interface: <ul style="list-style-type: none"> <li><b>Enable:</b> The interface is switched on and can be connected to another device.</li> <li><b>Disable:</b> The interface is switched off and can not be connected to another device.</li> </ul>	Enable
<b>Jumbo Frame</b>	
The field displays whether the jumbo frame is enabled for the port. <ul style="list-style-type: none"> <li><b>Enable:</b> The jumbo frame is enabled. The switch supports a fixed jumbo frame size - 9000 byte payload (9018 byte frame) size.</li> <li><b>Disable:</b> The jumbo frame is disabled.</li> </ul>	Disable
<b>Link Trap</b>	
Specify whether the switch sends a trap when the interface link status changes: <ul style="list-style-type: none"> <li><b>Enable:</b> When the link status changes, the switch sends a trap. This is the default setting.</li> <li><b>Disable:</b> When the link status changes, the switch does not send a trap.</li> </ul>	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

SNTP Scalars Configuration	
<b>SNTP Client Status</b>	<input checked="" type="radio"/> Disabled <input type="radio"/> Enabled
<b>SNTP Server Status</b>	<input checked="" type="radio"/> Disabled <input type="radio"/> Enabled
<b>Date</b>	<input type="text" value="DD/MM/YYYY"/> (DD/MM/YYYY)
<b>Time</b>	<input type="text" value="HH:MM:SS"/> (HH:MM:SS)
<b>Time Zone</b>	<input type="text" value="+00:00"/> (+/-HH:MM)
<b>DST StartTime</b>	<input type="text"/> For example, First-Sun-Mar,05:10
<b>DST EndTime</b>	<input type="text"/> For example, Second-Sun-Nov,06:10



#### ● SNTP Scalars Configuration

Description	Factory default
<b>SNTP Client Status</b>	
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. <ul style="list-style-type: none"> <li><b>Enable:</b> The switch works as an SNTP client.</li> <li><b>Disable:</b> The switch does not work as an SNTP client.</li> </ul>	Disable
<b>SNTP Server Status</b>	
Specify whether the switch works as an SNTP server. <ul style="list-style-type: none"> <li><b>Enable:</b> The switch works as an SNTP server.</li> <li><b>Disable:</b> The switch does not work as an SNTP server.</li> </ul>	Disable
<b>Date</b>	
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
<b>Time</b>	
The time parameter format is HH:MM:SS. When an SNTP client is disabled, you can manually set the time. When an SNTP client is enabled, the field is grayed out.	HH:MM:SS
<b>Time Zone</b>	
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
<b>DST StartTime</b>	
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 format: First-Sat-May-03:00.	None
<b>DST EndTime</b>	
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



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

### 3.1.4.2 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

SNTP Unicast Server Configuration					
	Forward Address Type	Unicast Server IP Address	Unicast Server Type	Last Updated	Tx Requests
<input type="checkbox"/>	-		-		

#### SNTP Unicast Server Configuration

Description	Factory default
<b>Forward Address Type</b> Specify a type of SNTP server IP address: <ul style="list-style-type: none"> <li>• <b>IPv4:</b> Use an IPv4 address to recognize an SNTP server. This is the default setting.</li> <li>• <b>IPv6:</b> Use an IPv6 address to recognize an SNTP server.</li> <li>• <b>DNS:</b> Use FQDN to recognize an SNTP server.</li> </ul>	IPv4
<b>Unicast Server IP Address</b> Enter the server IPv4, IPv6 address or host name (FQDN). (Depend on the type you select in the Forward Address Type field.)	None
<b>Unicast Server Type</b> Specify a type of server by selecting Primary or Secondary from the drop-down list.	None
<b>Last Updated</b> This field displays the last time the SNTP unicast server updated its time information.	None
<b>Tx Requests</b> 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.

The following is a DHCP Server example:

Set Network to 192.168.1.0, DVS will send the IP address of the network segment 192.168.1.1-192.168.1.254 DHCP Client.

## DHCP Server Configuration

DHCP Server Configuration			
<b>Admin Mode</b>	Enable ▾		
<b>Next Server</b>	0.0.0.0		
<b>Boot File</b>	None		
<b>Network</b>	192.168.1.0		
<b>Subnet Mask</b>	255.255.255.0		
<b>Lease Time Type</b>	Infinite ▾		
<b>Lease Time</b>	--	D	--
		H	--
		M	
<b>Default Router</b>			
<b>DNS Server</b>			
<b>Domain Name</b>			

Excluded Addresses			
	IP Range From	IP Range To	Method
<input type="checkbox"/>			

### DHCP Server Configuration

Description	Factory default
<b>Admin Mode</b>	
Specify the status of the DHCP server on the switch: <ul style="list-style-type: none"> <li><b>Disable:</b> The DHCP server is disabled. When you want to enable the DHCP relay function, please select this setting.</li> <li><b>Enable:</b> The DHCP server is enabled.</li> </ul>	Disable
<b>Next Server</b>	
Specify the boot server host name.	0.0.0.0
<b>Boot File</b>	
Specify the boot file name.	None
<b>Network</b>	
Enter the network for the DHCP pool.	None
<b>Subnet Mask</b>	
Enter the IP subnet mask for the DHCP pool.	None
<b>Lease Time Type</b>	
Specify a type of lease time: <ul style="list-style-type: none"> <li><b>Specified Duration:</b> The leased IP address has a specific duration. You need to specify the duration in the Lease Time fields.</li> <li><b>Infinite:</b> The leased IP address does not expire.</li> </ul>	None
<b>Lease Time</b>	
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
<b>Default Router</b>	
Specify the default gateway IP address. The information will be included in the DHCP offer packet.	None

Description	Factory default
<b>DNS Server</b>	
Specify the DNS server IP address. The information will be included in the DHCP offer packet.	None
<b>Domain Name</b>	
Specify the domain name. The information will be included in the DHCP offer packet.	None

**Excluded Addresses**

Description	Factory default
<b>IP Range From</b>	
Enter the start IP address of the exclusion IP range which you created in the DHCP server pool.	None
<b>IP Range To</b>	
Enter the end IP address of the exclusion IP range which you created in the DHCP server pool.	None
<b>Method</b>	
It indicates that the excluded address is created by a DHCP server or a user. There are two values: <ul style="list-style-type: none"> <li>• <b>Auto:</b> The entry is created by a DHCP server.</li> <li>• <b>Manual:</b> The entry is created by a user.</li> </ul>	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**

DHCP Server Pool Option Configuration			
	Option Code	Option Type	Option Value
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="button" value="Add"/> <input type="button" value="Delete"/> <input type="button" value="Cancel"/> <input type="button" value="Apply"/>			

● **DHCP Server Pool Option Configuration**

Description	Factory default
<b>Option Code</b>	
It supports the following configured options now: <ul style="list-style-type: none"> <li>● Option 1 – Subnet Option</li> <li>● Option 3 – Router Option</li> <li>● Option 6 – Domain Name Server</li> <li>● Option 15 – Domain Name</li> <li>● Option 42 – Network Time Protocol Servers Option</li> </ul> (If you need more information, please refer to RFC2132, DHCP Options and BOOTP Vendor Extensions.)	None
<b>Option Type</b>	
Specify the option type: <ul style="list-style-type: none"> <li>• <b>ASCII:</b> Enter an ASCII value in the Option Value field.</li> <li>• <b>Hex:</b> Enter a hexadecimal value in the Option Value field.</li> <li>• <b>IP Address:</b> Enter an IP address or a subnet mask in the Option Value field.</li> </ul>	None
<b>Option Value</b>	
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

DHCP Server Binding Table				
	IP Address	Hardware Type	Hardware Address	Expire Time
<input type="checkbox"/>	192.168.1.11	Ethernet	00:18:23:01:1f:2f	infinite

### DHCP Server Binding Table

Description	Factory default
<b>IP Address</b>	
The IP address of the DHCP client.	None
<b>Hardware Type</b>	
This field displays a type of hardware address of the client. <ul style="list-style-type: none"> <li><b>Client ID:</b> 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.</li> <li><b>Ethernet:</b> The hardware type is Ethernet, and the hardware address is an MAC address.</li> </ul>	None
<b>Hardware Address</b>	
This field displays the MAC address or the string identifier of the DHCP client.	None
<b>Expire Time</b>	
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 Configuration

MAC Based DHCP Mode	
Admin Mode	<input type="radio"/> Disable <input checked="" type="radio"/> Enable

MAC Based DHCP Mode

Description	Factory default
<b>Admin Mode</b>	
Specify the status of the MAC Based DHCP on the switch. <ul style="list-style-type: none"> <li><b>Disable:</b> The MAC Based DHCP Configuration is disabled.</li> <li><b>Enable:</b> The MAC Based DHCP Configuration is enabled.</li> </ul> <b>Note:</b> 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				
	Pool ID	Hardware Type	Hardware Address	IP Address
<input type="checkbox"/>	1	-		

### MAC Based DHCP Binding Configuration

Description	Factory default
<b>Pool ID</b>	
It's the DHCP Pool number.	fixed
<b>Hardware Type</b>	

Description	Factory default
This field displays a type of hardware address of the client. <ul style="list-style-type: none"> <li><b>Client ID:</b> 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.</li> <li><b>Ethernet:</b> The type of the HW address, and the hardware address is an MAC address.</li> </ul>	None
<b>Hardware Address</b>	
This field displays the MAC address or the string identifier.	None
<b>IP Address</b>	
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

3

● **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 Configuration**

**Port Based DHCP Mode**

Admin Mode  Disable  Enable

Port Based DHCP Mode

Description	Factory default
<b>Admin Mode</b>	
Specify the status of the Port Based DHCP on the switch. <ul style="list-style-type: none"> <li><b>Disable:</b> The Port Based DHCP Mode is disabled.</li> <li><b>Enable:</b> The Port Based DHCP Mode is enabled.</li> </ul> <b>Note:</b> 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**

	Pool ID	Interface	IP Address
<input type="checkbox"/>	1	-	

Port Based DHCP Binding Configuration

Description	Factory default
<b>Pool ID</b>	
It's the DHCP Pool number.	1
<b>Interface</b>	
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
<b>IP Address</b>	
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 Bindings Configuration**

RARP Bindings Configuration		
IP Address	Hardware Type	Hardware Address

Refresh

Delete

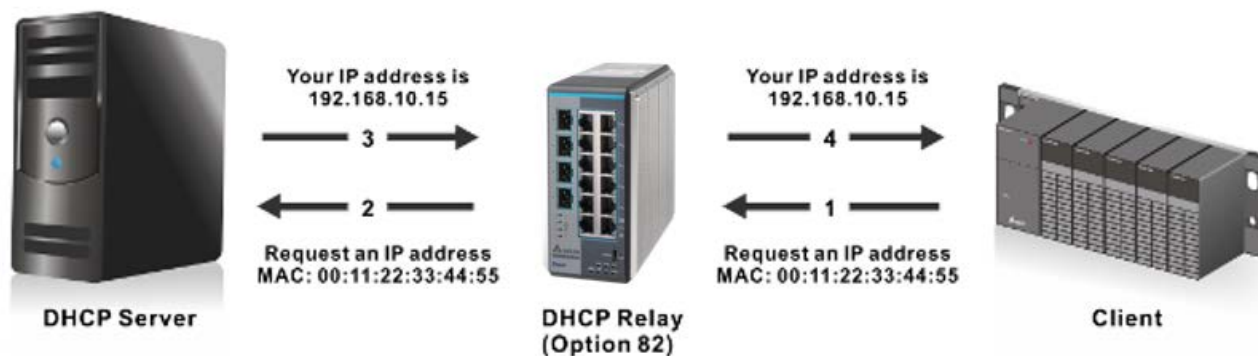
Cancel

## RARP Binding Configuration

Description	Factory default
<b>IP Address</b>	
It's the static IP which acquired from the MAC Based DHCP Binding Configuration or Port Based Binding Configuration.	None
<b>Hardware Type</b>	
This field displays a type of hardware address of the client. <ul style="list-style-type: none"> <li><b>Client ID:</b> 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.</li> <li><b>Ethernet:</b> The type of the HW address, and the hardware address is an MAC address.</li> </ul>	None
<b>Hardware Address</b>	
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.

### DHCP Relay Configuration

**DHCP Relay Configuration**

**Admin Mode** Disable ▾

**Circuit ID Sub-Option** Disable ▾

**Remote ID Sub-Option**

---

**DHCP Server Address Configuration**

#	Server Address
1	<input style="width: 100%;" type="text"/>

#### DHCP Relay Configuration

Description	Factory default
<b>Admin Mode</b>	
Specify the status of the DHCP relay on the switch: <ul style="list-style-type: none"> <li><b>Disable:</b> The DHCP relay is disabled. This is the default setting.</li> <li><b>Enable:</b> The DHCP relay is enabled.</li> </ul> <b>Notice:</b> Before you enabled Admin Mode, please create at least one server IP in DHCP Server Address Configuration.	Disable
<b>Circuit ID sub-option</b>	
Specify whether the circuit ID sub-option (the interface ID of the switch) is enabled. <ul style="list-style-type: none"> <li><b>Disable:</b> The circuit ID can not be added to a DHCP packet. This is the default setting.</li> <li><b>Enable:</b> The circuit ID can be added to a DHCP packet.</li> </ul>	Disable
<b>Remote ID Sub-Option</b>	
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
<b>Server Address</b>	
The IP address of the DHCP server IP.	None

- DHCP Relay Statistics

#### DHCP Relay Statistics

**DHCP Relay Statistics**

No of Packets inserted Circuit-Id option	0
No of Packets inserted Remote-Id suboption	0
No of Packets dropped	0
No of Packets which did not inserted RAI option	0

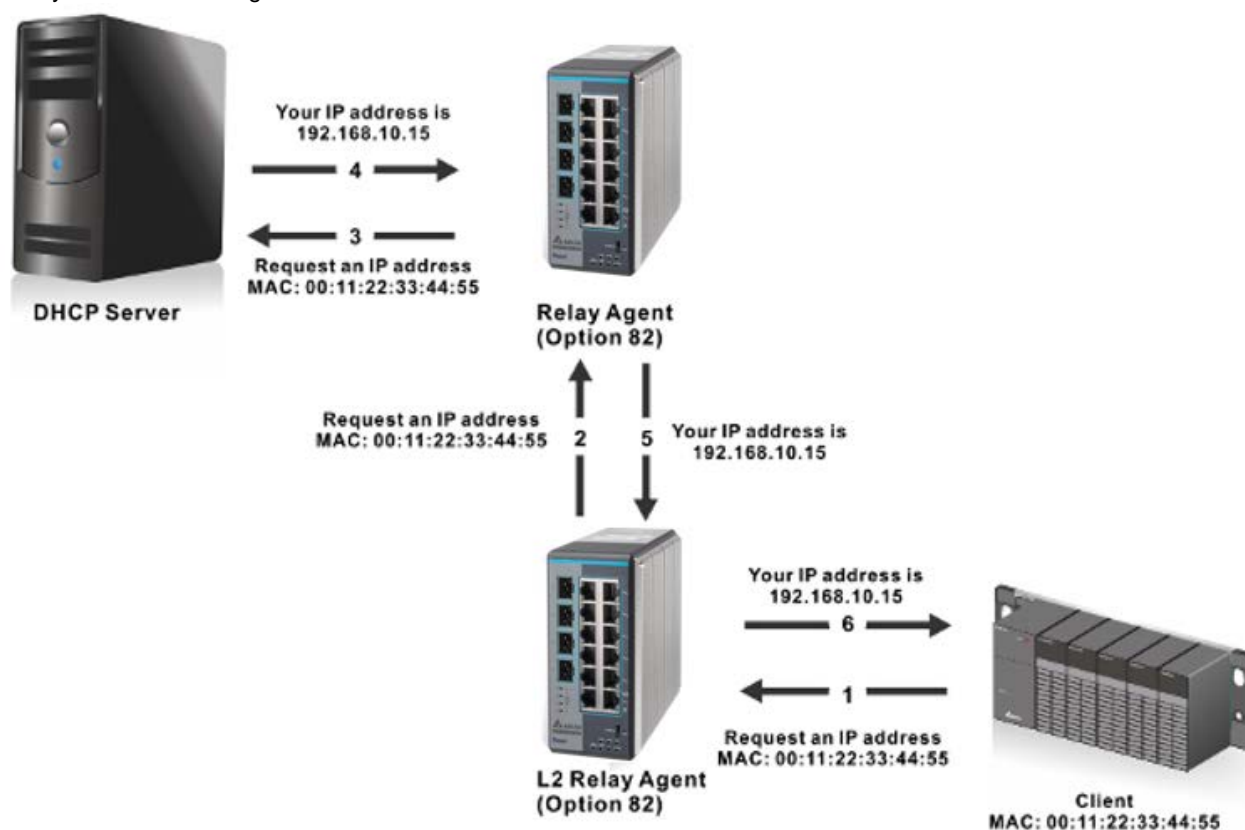
#### DHCP Relay Statistics

Item	Description
<b>No of Packets inserted</b>	The number of packets which inserted the circuit-Id option.

<b>Circuit-Id option</b>	
<b>No of Packets inserted Remote-Id suboption</b>	The number of packets which inserted the remote-Id suboption.
<b>No of Packets dropped</b>	The number of packets which dropped.
<b>No of Packets which did not inserted RAI option</b>	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 Configuration

**DHCP L2 Relay Global Configuration**

**Admin Mode**  Disable  Enable

---

**DHCP L2 Relay VLAN Configuration**

	VLAN ID	Admin Mode	Circuit ID Mode	Remote ID String
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	1	Disable	Disable	

#### DHCP L2 Relay Global Configuration

Description	Factory default
Admin Mode	
Specify whether the global status of the DHCP relay is enabled. <ul style="list-style-type: none"> <li>• <b>Enable:</b> The DHCP relay function is enabled.</li> <li>• <b>Disable:</b> The DHCP relay function is disabled. This is the default setting.</li> </ul>	Disable

#### DHCP L2 Relay VLAN Configuration

Description	Factory default
<b>VLAN ID</b>	
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
<b>Admin Mode</b>	
Specify whether the status of the DHCP relay is enabled on the VLAN: <ul style="list-style-type: none"> <li>• <b>Enable:</b> 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.</li> <li>• <b>Disable:</b> Disable the DHCP relay on the VLAN.</li> </ul>	Disable
<b>Circuit ID</b>	
Specify whether the DHCP relay agent information option (DHCP option 82) is enabled: <ul style="list-style-type: none"> <li>• <b>Enable:</b> Enable the relay agent information option.</li> <li>• <b>Disable:</b> Disable the relay agent information option. This is the default setting for the default VLANs 1, 2, and 3.</li> </ul>	Disable
<b>Remote ID String</b>	
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.

1. 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.

## 2. 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**

DHCP L2 Relay Interface Configuration			
	Interface	Admin Mode	82 Option Trust Mode
<input type="checkbox"/>		- ▾	- ▾
<input type="checkbox"/>	0/1	Disable	Disable
<input type="checkbox"/>	0/2	Disable	Disable
<input type="checkbox"/>	0/3	Disable	Disable
<input type="checkbox"/>	0/4	Disable	Disable
<input type="checkbox"/>	0/5	Disable	Disable
<input type="checkbox"/>	0/6	Disable	Disable
<input type="checkbox"/>	0/7	Disable	Disable
<input type="checkbox"/>	0/8	Disable	Disable
<input type="checkbox"/>	po1	Disable	Disable
<input type="checkbox"/>	po2	Disable	Disable
<input type="checkbox"/>	po3	Disable	Disable

3

**DHCP L2 Relay Interface Configuration**

Description	Factory default
<b>Interface</b>	
The interface number.	<i>interface number</i>
<b>Admin Mode</b>	
Specify whether the DHCP relay is enabled on the interface: <ul style="list-style-type: none"> <li><b>Enable:</b> 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.</li> <li><b>Disable:</b> Disable the DHCP relay on the interface.</li> </ul>	Disable
<b>82 Option Trust Mode</b>	
As a security consideration, specify whether the interface is trusted when the DHCP relay agent information (DHCP option 82) is received on the interface: <ul style="list-style-type: none"> <li><b>Enable:</b> The relay agent information that is received on the interface can be trusted.</li> <li><b>Disable:</b> The relay agent information that is received on the interface can not be trusted and should be ignored.</li> </ul>	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

### DHCP L2 Relay Interface Statistics

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

**DNS Configuration**

DNS Status  Disable  Enable

DNS Default Name  (1 to 255 characters)

DNS Server Configuration			
	Serial No	DNS Server	Preference
<input type="checkbox"/>		<input style="width: 100px;" type="text"/>	
<input type="checkbox"/>	1	192.168.100.1	1

#### DNS Configuration

	Description	Factory default
DNS Status		

Specify whether the switch functions as a DNS client: <ul style="list-style-type: none"> <li>• <b>Disabled:</b> 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.</li> <li>• <b>Enabled:</b> The switch functions as a DNS client and can send DNS queries to a DNS server.</li> </ul>	Enable
<b>DNS Default Name</b>	
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
<b>Serial No</b>	
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
<b>DNS Server</b>	
The DNS server can be added manually or added dynamically through DHCP. The Delta switch can support 8 DNS servers.	None
<b>Preference</b>	
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**

DNS Host Configuration		
	Host Name	IP Address
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	www	192.168.1.50

Dynamic Host Mapping				
Host	Total	Elapsed	Type	Address

**DNS Host Configuration**

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

**Dynamic Host Mapping**

Description	Factory default
<b>Host</b>	
The host name was added dynamically.	None
<b>Total</b>	

The total time to live (TTL) for the dynamic entry.	None
<b>Elapsed</b>	
The elapsed time since the dynamic entry was added to the table.	None
<b>Type</b>	
The dynamic entry types: <ul style="list-style-type: none"> <li>• IPv4</li> <li>• IPv6</li> <li>• Canonical name</li> </ul>	None
<b>Address</b>	
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 current configuration will be lost when you finish the update process, and it will restore the factory default configuration.

● TFTP Download

#### TFTP File Download

**TFTP File Download**

<b>File Type</b>	Archive <input type="button" value="v"/>
<b>Image Name</b>	image1 <input type="button" value="v"/>
<b>Server Address Type</b>	IPv4 <input type="button" value="v"/>
<b>Server Address</b>	<input type="text"/>
<b>Remote File Name</b>	<input type="text"/>

**Transfer Status**

#### TFTP File Download

Description	Factory default
<p><b>File Type</b></p> <p>Specify a type of file in the drop-down list that you want to download:</p> <ul style="list-style-type: none"> <li>• <b>Archive:</b> When you select Archive, the Image Name drop-down list is displayed.</li> <li>• <b>Startup Configuration:</b> When the switch boots up, Startup Configuration will be applied.</li> <li>• <b>SSL Server Certificate PEM File:</b> For more information about the SSL server certificate PEM file, please see the Certificate Information page.</li> <li>• <b>Script File:</b> This file is used to configure the switch by the CLI script.</li> </ul>	None
<b>Image Name</b>	

Description	Factory default
Only when you select Archive from the File Type drop-down list is the Image Name drop-down list displayed. Specify the image: <ul style="list-style-type: none"> <li><b>image1</b>: The downloaded image firmware as image1.</li> <li><b>image2</b>: The downloaded image firmware as image2.</li> </ul>	image1
<b>Server Address Type</b>	
Specify a type of server address and enter the IP address or host name in the Server Address field: <ul style="list-style-type: none"> <li><b>IPv4</b>: The IPv4 address of a TFTP server.</li> <li><b>DNS</b>: The DNS host name of a TFTP server.</li> </ul>	IPv4
<b>Server Address</b>	
Enter an IPv4 address or a DNS host name of the TFTP server.	None
<b>Remote File Name</b>	
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 File Download

**HTTP File Download**

File Type:

Image Name:

Select File:

---

**Transfer Status**

### HTTP Download

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

The screenshot shows a configuration window titled "TFTP File Upload". It contains the following fields:

- File Type:** A dropdown menu with "Archive" selected.
- Image Name:** A dropdown menu with "image1" selected.
- Server Address Type:** A dropdown menu with "IPv4" selected.
- Server Address:** An empty text input field.
- Remote File Name:** An empty text input field.

At the bottom of the window are two buttons: "Cancel" and "Apply".

#### TFTP Upload

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

The screenshot shows a configuration window titled "HTTP File Upload". It contains the following fields:

- File Type:** A dropdown menu with "Archive" selected.
- Image Name:** A dropdown menu with "image1" selected.

At the bottom of the window are two buttons: "Cancel" and "Apply".

## HTTP Upload

Description	Factory default
<b>File Type</b>	
Specify a type of file in the drop-down list that you want to upload: <ul style="list-style-type: none"> <li>• <b>Archive:</b> When you select Archive, the Image Name drop-down list is displayed.</li> <li>• <b>Startup Configuration:</b> When the switch boots up, Startup Configuration will be applied.</li> <li>• <b>Backup Configuration:</b> It is used to backup the Startup Configuration file.</li> <li>• <b>Log:</b> This file records the log information of the switch.</li> <li>• <b>Script File:</b> This file is used to configure the switch by the CLI script.</li> </ul>  <b>Notice:</b> 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: " <b>copy nvram:startup-config nvram:backup-config</b> " to back up the Startup Configuration file by Hyper Terminal or Telnet.	None
Description	Factory default
<b>Image Name</b>	
Only when you select Archive from the File Type drop-down list is the Image Name drop-down list displayed. Specify the image: <ul style="list-style-type: none"> <li>• <b>image1:</b> The uploaded image firmware as image1.</li> <li>• <b>image2:</b> The uploaded image firmware as image2.</li> </ul>	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.

#### 3.1.8.1 HTTP Configuration

##### HTTP Configuration

**HTTP Configuration**

HTTP Access  Disable  Enable

HTTP Port

HTTP Session Timeout (minutes)  (0 to 60)



##### HTTP Configuration

Description	Factory default
<b>HTTP Access</b>	
Specify whether the web management interface can be accessed from a web browser over an HTTP connection. <ul style="list-style-type: none"> <li>• <b>Disable:</b> 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.</li> <li>• <b>Enable:</b> The web management interface can be accessed over an HTTP connection.</li> </ul>	Enable
<b>HTTP Port</b>	
The HTTP port number. The number must be in the range of 1 to 65535. The default setting is port number 80.	80
<b>HTTP Session Timeout (minutes)</b>	

Description	Factory default
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.

## 3

- **HTTPS Configuration**

#### HTTPS Configuration


**HTTPS Configuration**

HTTPS Admin Mode  Disable  Enable

HTTPS Port

HTTPS Session Timeout (minutes)  (1 to 60)

#### HTTPS Configuration

Description	Factory default
<b>HTTPS Admin Mode</b>	
Specify whether the web management interface can be accessed from a web browser over an HTTPS connection. <ul style="list-style-type: none"> <li>• <b>Disable:</b> 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.</li> <li>• <b>Enable:</b> The web management interface can be accessed over an HTTPS connection.</li> </ul>  <b>Notice:</b> If you want to enable the HTTPS Admin mode, you need to use Generate Key, then apply Generate Certificate, please refer to <b>Certificate Management</b> .	Disable
<b>HTTPS Port</b>	
The HTTP port number. The number must be in the range of 1 to 65535.	443
<b>HTTPS Session Timeout (minutes)</b>	
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

**Certificate Management**

None

**Generate Key (RSA-1024 bits)** (It may take a while)

**Generate Certificate**

**Delete Certificate**

=====

**Certificate Present** : No

### Certificate Management

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

**Certificate Download**

**File Type** SSL Server Certificate PEM File

**TFTP Server IP**

**Remote File Name**

**Start File Transfer**

### Certificate Download

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

- **Certificate Information**

**Certificate Information**

**Certificate Information**

```

Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number:
      6f:06:0c:5c:98:5d:69:ba:08:f6:f5:14:98:7f:3d:47
    Signature Algorithm: md5WithRSAEncryption
    Issuer: CN=self-signed
    Validity
      Not Before: Jan  1 01:05:00 1970 GMT
      Not After : Jan  1 01:05:00 1972 GMT
    Subject: CN=192.168.1.15
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      RSA Public Key: (1024 bit)
      Modulus (1024 bit):
        00:bb:c3:9a:6a:e9:83:65:85:7d:fb:ee:d6:0f:93:
        e2:de:f9:5c:63:41:4f:f8:d7:01:4c:a7:d6:52:6c:
        3a:80:cc:19:a5:d2:ff:4f:87:e7:31:87:38:6e:f6:
        21:84:82:80:b0:15:84:f8:f9:85:05:0d:94:c9:29:
        9b:a7:f3:7b:4d:64:cb:dc:73:34:a3:7d:dc:c3:ac:
        e8:be:38:74:46:8a:53:df:71:13:70:41:17:88:0e:
        b3:f9:7c:e4:eb:69:34:96:67:1b:2e:fa:2f:68:8d:
        cc:1b:9e:31:70:68:d8:05:b2:cb:77:b7:46:72:74:
        1f:05:86:e7:17:fc:dd:be:73
      Exponent: 65537 (0x10001)
    Signature Algorithm: md5WithRSAEncryption
      6d:b9:e6:07:7e:17:7a:e6:3b:63:ae:b2:28:98:65:7f:de:b8:
          
```

**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**

**SSH Configuration**

SSH Admin Mode	<input checked="" type="radio"/> Disable	<input type="radio"/> Enable
SSH Version 1	<input type="radio"/> Disable	<input checked="" type="radio"/> Enable
SSH Version 2	<input type="radio"/> Disable	<input checked="" type="radio"/> Enable
SSH Session Timeout (minutes)	<input style="width: 100px;" type="text" value="30"/>	(1 to 160)
Maximum Number of SSH Sessions	<input style="width: 100px;" type="text" value="5"/>	
Current Number of SSH Sessions	<input style="width: 100px;" type="text" value="0"/>	

**SSH Configuration**

Description	Factory default
<b>SSH Admin Mode</b>	
Specify the status of SSH. <ul style="list-style-type: none"> <li><b>Disable:</b> SSH is disabled. This is the default setting.</li> <li><b>Enable:</b> SSH is enabled.</li> </ul>	Disable
<b>SSH Version 1</b>	
Specify whether SSH version 1 is supported. <ul style="list-style-type: none"> <li><b>Disable:</b> SSH version 1 is not supported.</li> <li><b>Enable:</b> SSH version 1 is supported. Both version 1 and version 2 can be supported on the switch.</li> </ul>	Enable
<b>SSH Version 2</b>	
Specify whether SSH version 2 is supported. <ul style="list-style-type: none"> <li><b>Disable:</b> SSH version 2 is not supported.</li> <li><b>Enable:</b> SSH version 2 is supported. Both version 1 and version 2 can be supported on the switch.</li> </ul>	Enable
<b>SSH Session Timeout (minutes)</b>	
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
<b>Maximum Number of SSH Sessions</b>	
The maximum number of inbound SSH sessions. The number must be in the range of 0 to 5.	5
<b>Current Number of SSH Sessions</b>	
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

**Telnet Configuration**

Telnet Admin Mode  Disable  Enable

Telnet Session Timeout (minutes)  (1 to 160)

Maximum Number of Telnet Sessions  (0 to 5)

Current Number of Telnet Sessions




#### Telnet Configuration

Description	Factory default
<b>Telnet Admin Mode</b>	
Specify the status of Telnet. <ul style="list-style-type: none"> <li><b>Disable:</b> Telnet is disabled.</li> <li><b>Enable:</b> Telnet is enabled.</li> </ul>	Enable
<b>Telnet Session Timeout (minutes)</b>	
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
<b>Maximum Number of Telnet Sessions</b>	
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
<b>Current Number of Telnet Sessions</b>	
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

Console Port	
Console Login Timeout (minutes)	<input type="text" value="30"/> (0 to 160)

#### Console Port

Description	Factory default
<b>Console Login Timeout (minutes)</b>	
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

Loopback-Detection Global Configuration	
Module Status	<input type="radio"/> Disable <input checked="" type="radio"/> Enable

#### Loopback-Detection Global Configuration

Description	Factory default
<b>Module Status</b>	
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.

## Loopback-Detection Port Configuration

Loopback-Detection Port Configuration				
	Interface	Port Control	Recovery Mode	Recovery Interval
<input type="checkbox"/>		- ▾	- ▾	
<input type="checkbox"/>	0/1	Disable	Manual	300
<input type="checkbox"/>	0/2	Disable	Manual	300
<input type="checkbox"/>	0/3	Disable	Manual	300
<input type="checkbox"/>	0/4	Disable	Manual	300
<input type="checkbox"/>	0/5	Disable	Manual	300
<input type="checkbox"/>	0/6	Disable	Manual	300
<input type="checkbox"/>	0/7	Disable	Manual	300
<input type="checkbox"/>	0/8	Disable	Manual	300
<input type="checkbox"/>	po1	Disable	Manual	300
<input type="checkbox"/>	po2	Disable	Manual	300
<input type="checkbox"/>	po3	Disable	Manual	300

### Loopback-Detection Port Configuration

Description	Factory default
<b>Interface</b>	
The interface number.	<i>interface number</i>
<b>Port Control</b>	
Enable/Disable the Loopback-Detection feature on the port.	Disable
<b>Recovery Mode</b>	
There are two recovery modes for recovering the blocking port. Loops occur as the reason for blocking the port. <ul style="list-style-type: none"> <li>• <b>Auto Mode:</b> After the port is blocked, the port will be automatically linked up after a recovery interval.</li> <li>• <b>Manual Mode:</b> After the port is blocked, we have to manually enable the port. Follow Basic Setting &gt; Port Setting &gt; Port Settings (Admin Mode) to enable the blocking port.</li> </ul>	Manual
<b>Recovery Interval</b>	
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.	<b>300</b>

### 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.

#### EtherNet/IP Configuration


EtherNet/IP Configuration	
EtherNet/IP Status	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
<input type="button" value="Cancel"/> <input type="button" value="Apply"/>	

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

Community Configuration				
	Community Name	Client Address	Client IP Mask	Access Mode
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	-
<input type="checkbox"/>	public	0.0.0.0	0.0.0.0	ReadOnly
<input type="checkbox"/>	private	0.0.0.0	0.0.0.0	ReadWrite

#### Community Configuration

Description	Factory default
<b>Community Name</b>	
Enter a case-sensitive string. The maximum length is 16 characters. The maximum community is 10.	None
<b>Client Address</b>	
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
<b>Client IP Mask</b>	
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
<b>Access Mode</b>	
Specify the access mode:	None

Description	Factory default
<ul style="list-style-type: none"> <li><b>ReadOnly:</b> Only allow the client to read information.</li> <li><b>ReadWrite:</b> Only allow the client to read information and modify configuration.</li> </ul>	

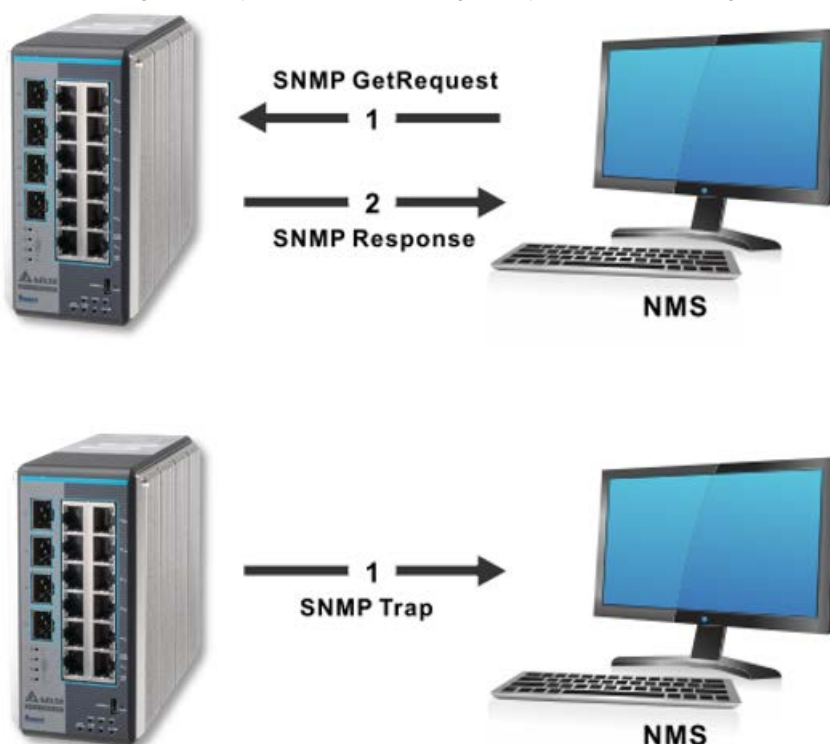


**Notice:**

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

Trap Configuration				
	Community Name	Version	Protocol	Address
<input type="checkbox"/>	<input type="text"/>	<input type="text" value="-"/>	<input type="text" value="-"/>	<input type="text"/>
<input type="button" value="Add"/> <input type="button" value="Cancel"/> <input type="button" value="Delete"/> <input type="button" value="Apply"/>				

#### Trap Configuration

Description	Factory default
<b>Community Name</b> Enter a case-sensitive string. The maximum length is 16 characters. The maximum trap is 10.	None
<b>Version</b> Specify the SNMP version that is used for the trap community: <ul style="list-style-type: none"> <li><b>SNMP v1:</b> Uses SNMP v1 to send traps to the trap community.</li> <li><b>SNMP v2c:</b> Uses SNMP v2c to send traps to the trap community.</li> </ul>	None

Description	Factory default
<b>Protocol</b>	
Specify the IP version that is used for the trap community: <ul style="list-style-type: none"> <li><b>IPv4:</b> Sends traps to an IPv4 address. Input an IPv4 address in the Address field.</li> <li><b>IPv6:</b> Sends traps to an IPv6 address. Input an IPv6 address in the Address field.</li> </ul>	None
<b>Address</b>	
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 field xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx	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

**Trap Flags**

<b>Authentication</b>	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
<b>Cold Start</b>	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
<b>Warm Start</b>	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
<b>Link Up/Down</b>	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
<b>Spanning Tree</b>	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable
<b>Password Change</b>	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable
<b>IP Address Change</b>	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
<b>Loopback-Detection</b>	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
<b>Redundancy</b>	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
<b>POOLUTL</b>	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable

#### Trap Flags

Description	Factory default
<b>Authentication</b>	
Specify whether authentication traps are enabled. <ul style="list-style-type: none"> <li><b>Enable:</b> Specify the switch which sends authentication trap messages.</li> <li><b>Disable:</b> Specify the switch which does not send authentication trap messages.</li> </ul>	Enable
<b>Cold Start</b>	
Specify whether cold-start traps are enabled. <ul style="list-style-type: none"> <li><b>Enable:</b> Specify the switch which sends cold-start trap messages.</li> <li><b>Disable:</b> Specify the switch which does not send cold-start trap messages.</li> </ul>	Enable
<b>Warm Start</b>	
Specify whether warm-start traps are enabled. <ul style="list-style-type: none"> <li><b>Enable:</b> Specify the switch which sends warm-start trap messages.</li> <li><b>Disable:</b> Specify the switch which does not send warm-start trap messages.</li> </ul>	Enable
<b>Link Up/Down</b>	
Specify whether link status traps are enabled. <ul style="list-style-type: none"> <li><b>Enable:</b> Specify the switch which sends link status trap messages when a link comes up or goes down. This is the default setting.</li> <li><b>Disable:</b> Specify the switch which does not send link status trap messages.</li> </ul>	Enable
<b>Spanning Tree</b>	
Specify whether spanning tree traps are enabled.	Disable

Description	Factory default
<ul style="list-style-type: none"> <li>• <b>Enable:</b> Specify the switch which sends spanning tree trap messages.</li> <li>• <b>Disable:</b> Specify the switch which does not send spanning tree trap messages.</li> </ul>	
<b>Password Change</b>	
Specify whether Password Change traps are enabled. <ul style="list-style-type: none"> <li>• <b>Enable:</b> Specify the switch which sends Password Change trap messages.</li> <li>• <b>Disable:</b> Specify the switch which does not send Password Change messages.</li> </ul>	Disable
<b>IP Address Change</b>	
Specify whether IP Address Change traps are enabled. <ul style="list-style-type: none"> <li>• <b>Enable:</b> Specify the switch which sends IP Address Change trap messages.</li> <li>• <b>Disable:</b> Specify the switch which does not send IP Address Change messages.</li> </ul>	Enable
<b>Loopback-Detection</b>	
Specify whether Loopback-Detection traps are enabled. <ul style="list-style-type: none"> <li>• <b>Enable:</b> Specify the switch which sends Loopback-Detection trap messages.</li> <li>• <b>Disable:</b> Specify the switch which does not send Loopback-Detection messages</li> </ul>	Enable
<b>Redundancy</b>	
Specify whether Redundancy traps are enabled. <ul style="list-style-type: none"> <li>• <b>Enable:</b> Specify the switch which sends Redundancy trap messages.</li> <li>• <b>Disable:</b> Specify the switch which does not send Redundancy messages</li> </ul>	Enable
<b>POOLUTL</b>	
Specify whether POOLUTL traps are enabled. <ul style="list-style-type: none"> <li>• <b>Enable:</b> Specify the switch which sends POOLUTL trap messages.</li> <li>• <b>Disable:</b> Specify the switch which does not send POOLUTL messages</li> </ul>	Disable

### 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						
	User Name	Authentication Protocol	Authentication Key	Private Protocol	Privacy Key	Access Mode
<input type="checkbox"/>		-		-		-
<input type="checkbox"/>	admin	No Authentication		No Privacy		ReadWrite
<input type="checkbox"/>	guest	No Authentication		No Privacy		ReadOnly


##### SNMP User Configuration

Description	Factory default
<b>User Name</b>	
Enter a case-sensitive string. The maximum length is 32 characters.	None
<b>Authentication Protocol</b>	
Specify the authentication protocol, if any, for the user: <ul style="list-style-type: none"> <li>• <b>No Authentication:</b> 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.</li> <li>• <b>HMAC-MD5:</b> 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.</li> <li>• <b>HMAC-SHA:</b> Users are authenticated by HMAC with SHA-1. If you select this item,</li> </ul>	None

Description	Factory default
please enter a password in the Authentication Key field.	
<b>Authentication Key</b>	
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
<b>Private Protocol</b>	
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: <ul style="list-style-type: none"> <li>• <b>No Privacy:</b> The users can access data without encryption.</li> <li>• <b>DES:</b> User communication is encrypted by Data Encryption Standard (DES). You need to enter a password in the Privacy Key field.</li> </ul>	None
<b>Privacy Key</b>	
If the privacy protocol is DES, please enter a case-sensitive string for the password. The maximum length is 40 characters.	None
<b>Access Mode</b>	
Specify the access mode: <ul style="list-style-type: none"> <li>• <b>ReadOnly:</b> The client can only have read permission to get information.</li> <li>• <b>ReadWrite:</b> The client can both have the read permission and the configuration permission to modify the information.</li> </ul>	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.**

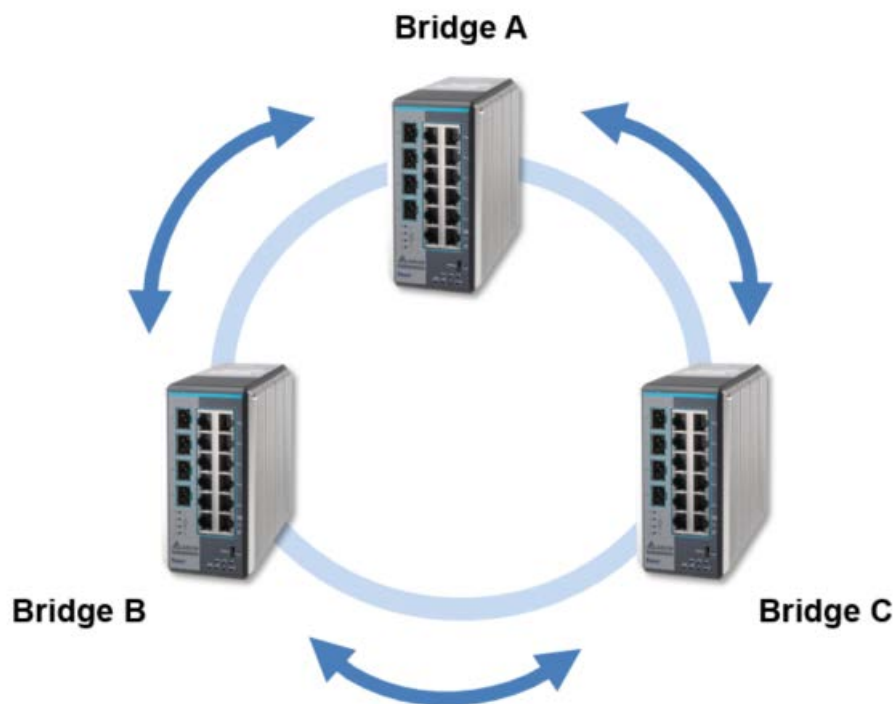
#### 3.3.1 STP

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.

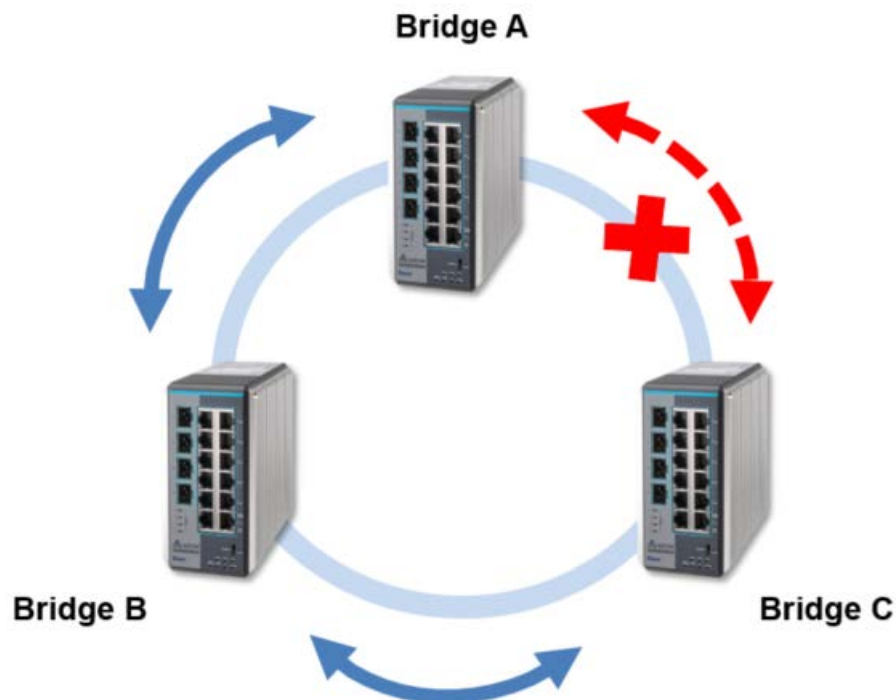
Rapid Spanning Tree Protocol (RSTP) was defined by IEEE in 2001. RSTP provides faster tree convergence after a topology changes. Sometimes it only needs to spend a few hundred milliseconds. And RSTP can be backward compatible with standard STP.

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.

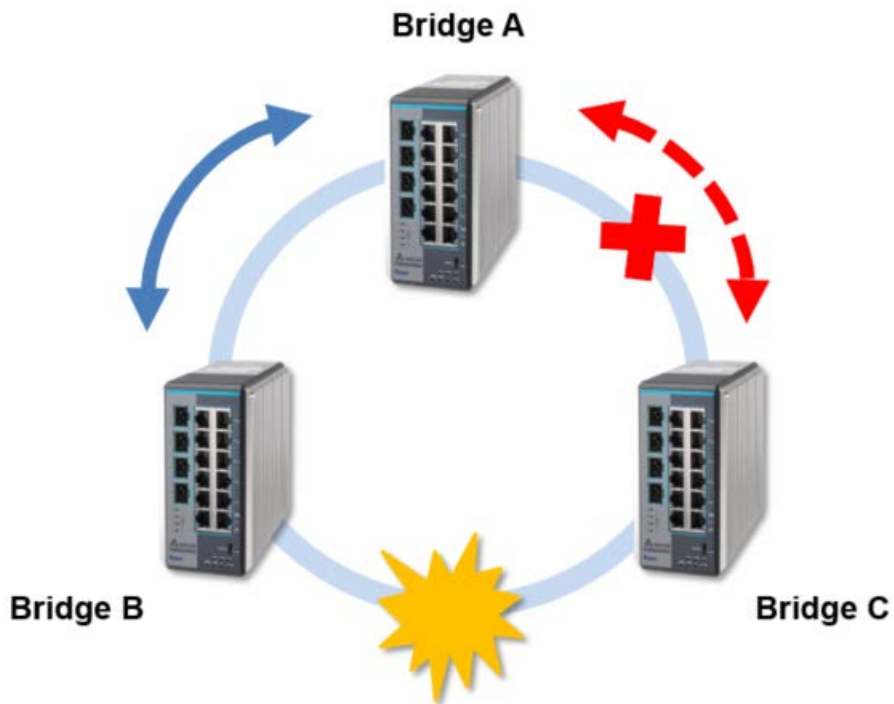
STP/RSTP can let you establish a redundant ring and protect the loop in a network, as shown in the figure below.



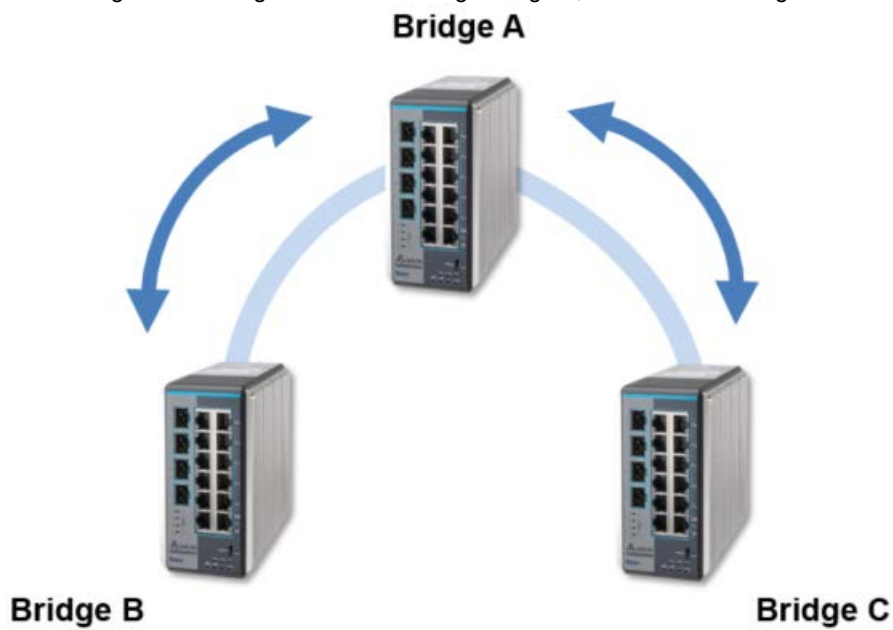
If STP/RSTP is enabled, it will detect duplicate paths, calculate the cost of each path and block the lowest cost path (ex. the path between A and C) from forwarding traffic. So bridges can communicate with each other without loops, as shown in the figure below.



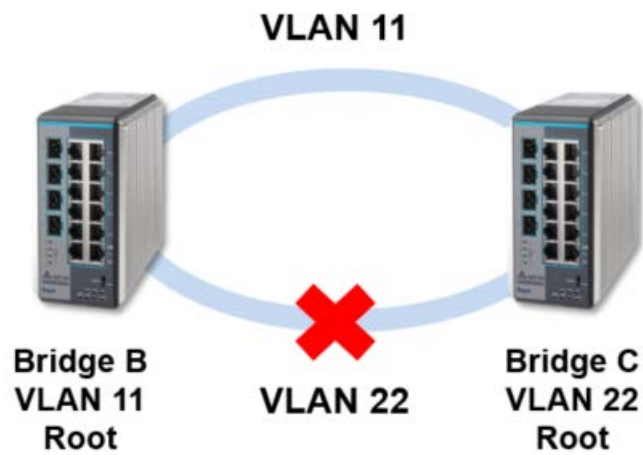
If the link failure is detected between bridge B and bridge C, STP/RSTP will start to reconfigure the network, as shown in the figure below.



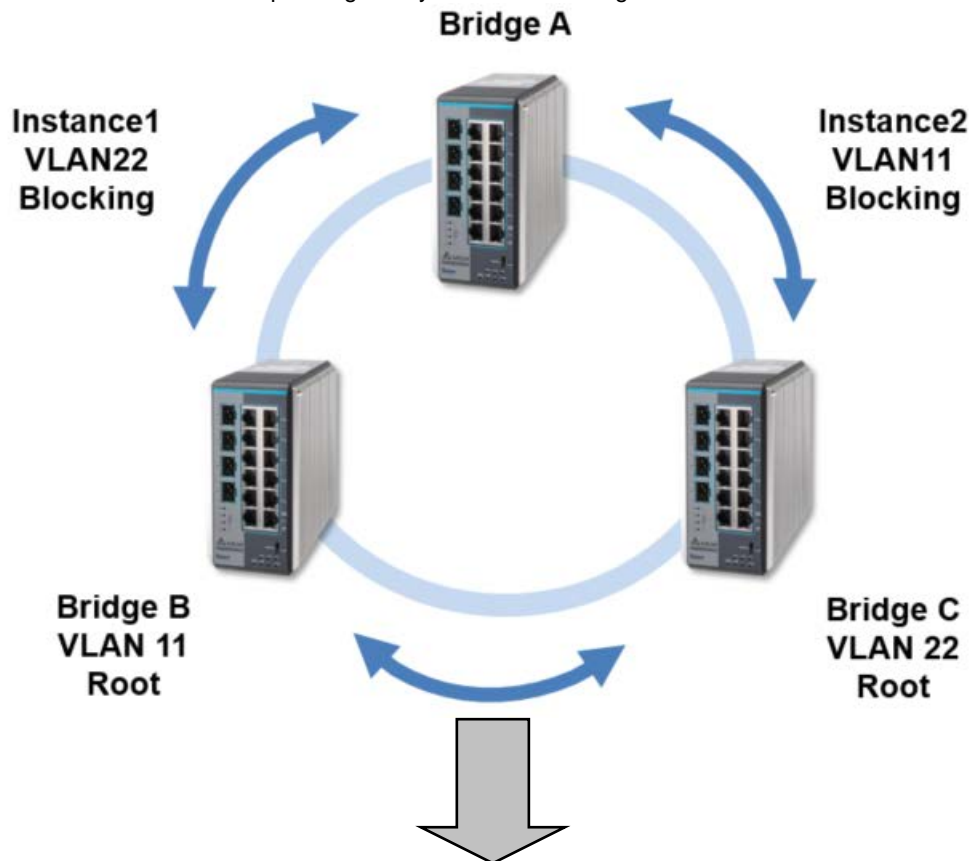
Then the traffic between bridge B and bridge C will flow through bridge A, as shown in the figure below.

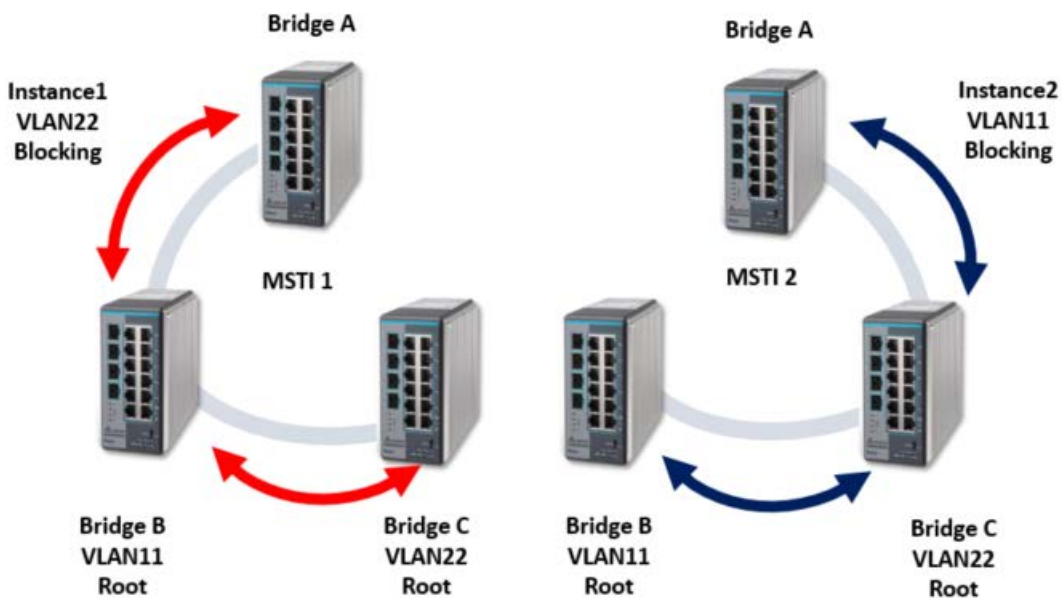


But STP/RSTP can not support more VLANs in your network topology. If there are 2 VLANs between 2 bridges, one path is blocked when STP/RSTP is enabled. So IEEE defined an extension to RSTP to further develop the usefulness of VLANs.



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.





3.3.1.1 STP Configuration

STP Configuration

Global Settings	
Spanning Tree Admin Mode	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Force Protocol Version	<input type="radio"/> STP <input type="radio"/> RSTP <input checked="" type="radio"/> MSTP
Configuration Name	<input type="text" value="00:18:23:01:08:60"/>
Configuration Revision Level	<input type="text" value="0"/> (0 to 65535)
Forward BPDUs while STP Disabled	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Configuration Digest Key	0xac36177f50283cd4b83821d8ab26de62
Configuration Format Selector	0

Global Settings Description

Description	Factory default
<p><b>Spanning Tree Admin Mode</b></p> <p>Specify the admin mode of STP on the switch:</p> <ul style="list-style-type: none"> <li><b>Disable:</b> STP is disabled. The settings do not take effect after you have applied them, but you still can configure STP.</li> <li><b>Enable:</b> STP is enabled. The settings take effect after you have applied them.</li> </ul>	Enable
<p><b>Force Protocol Version</b></p> <p>Specify the version of the STP protocol:</p> <ul style="list-style-type: none"> <li><b>STP:</b> Spanning Tree Protocol.</li> <li><b>RSTP:</b> Rapid Spanning Tree Protocol.</li> <li><b>MSTP:</b> Multiple Spanning Tree Protocol.</li> </ul>	MSTP
<p><b>Configuration Name</b></p> <p>Enter the STP identifier for the switch. You can configure alphanumeric characters and special characters, and the maximum length is 32.</p>	MAC address of the switch
<p><b>Configuration Revision Level</b></p> <p>Enter an identifier that specifies the current configuration. The number must be in the range of 0 to 65535.</p>	0
<p><b>Forward BPDUs while STP Disabled</b></p> <p>Specify whether spanning tree bridge protocol data units (BPDUs) are forwarded:</p> <ul style="list-style-type: none"> <li><b>Disable:</b> When STP is disabled, Spanning tree BPDUs are not forwarded.</li> </ul>	Disable

Description	Factory default
<ul style="list-style-type: none"> <li><b>Enable:</b> When STP is disabled, Spanning tree BPDUs are forwarded.</li> </ul>	
<b>Configuration Digest Key</b>	
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
<b>Configuration Format Selector</b>	
This field displays the configuration identifier format selector that is used.	0

STP Status		
MST ID	VID	FID
0	1	1

Refresh

Cancel

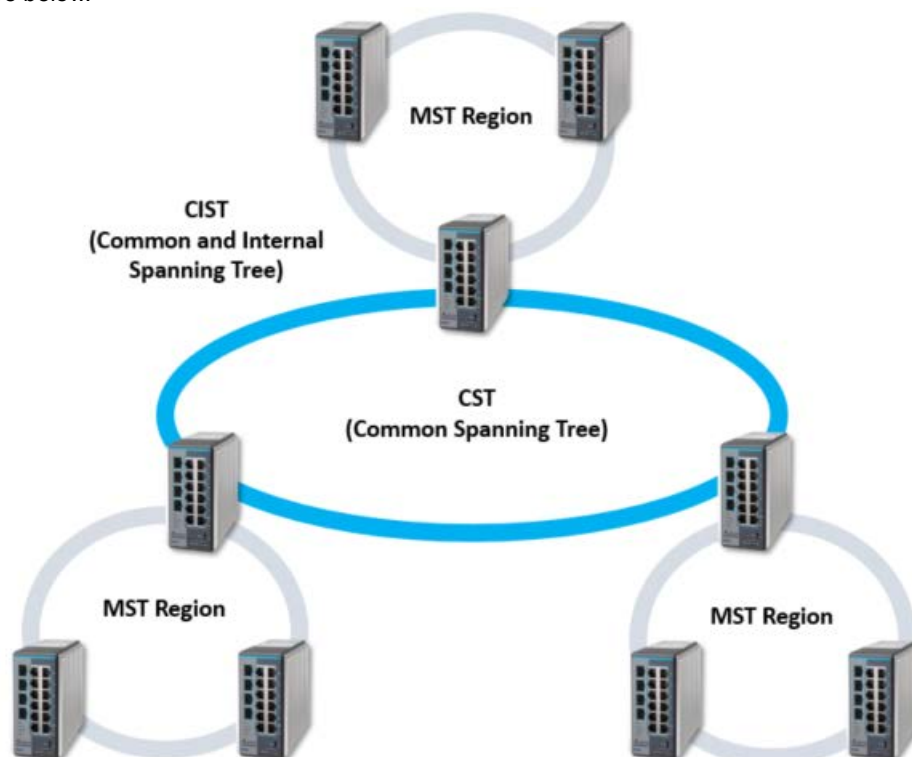
Apply

**STP Status**

Description	Factory default
<b>MST ID</b>	
The ID of the MST instance	0
<b>VID</b>	
The VLAN ID	1
<b>FID</b>	
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	<input type="text" value="32768"/>	(0 to 61440)
Bridge Max Age (secs)	<input type="text" value="20"/>	(6 to 40)
Bridge Hello Time (secs)	<input type="text" value="2"/>	(1 to 2)
Bridge Forward Delay (secs)	<input type="text" value="15"/>	(4 to 30)
Spanning Tree Maximum Hops	<input type="text" value="20"/>	(6 to 40)
Dynamic Path Cost	<input checked="" type="radio"/> Disable <input type="radio"/> Enable	
Extend System ID Status	<input checked="" type="radio"/> Disable <input type="radio"/> 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

### CST Configuration

Description	Factory default
<b>Bridge Priority</b>	
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
<b>Bridge Max Age (secs)</b>	
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
<b>Bridge Hello Time (secs)</b>	
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
<b>Bridge Forward Delay (secs)</b>	
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
<b>Spanning Tree Maximum Hops</b>	
Enter the maximum number of bridge hops; the information for a CST instance can travel before being discarded. Enter a number in the range of 6 to 40.	20

Description	Factory default
<b>Dynamic Path Cost</b>	
Specify whether the path cost is automatically calculated by selecting one of the following radio buttons: <ul style="list-style-type: none"> <li>• <b>Disable:</b> The path cost is not automatically calculated.</li> <li>• <b>Enable:</b> The path cost is automatically calculated.</li> </ul>	Disable
<b>Extend System ID Status</b>	
Specify whether the extended system identifier is added to the bridge priority by selecting one of the following radio buttons: <ul style="list-style-type: none"> <li>• <b>Disable:</b> The extended system identifier is not added to the bridge priority.</li> <li>• <b>Enable:</b> 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.</li> </ul>	Disable

**CTS Status**

Description	Factory default
<b>Bridge Identifier</b>	
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
<b>Time Since Topology Change</b>	
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
<b>Topology Change Count</b>	
The number of times the CST topology has changed.	0
<b>Designated Root</b>	
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
<b>Root Path Cost</b>	
The path cost to the designated root for the CST.	0
<b>Root Port Identifier</b>	
The interface that provides access to the designated root for the CST.	00:00
<b>Max Age (secs)</b>	
The timer that controls the maximum time that passes before an STP bridge port saves its configuration BPDU.	20
<b>Forward Delay (secs)</b>	
The value that is derived from the bridge forward delay parameter of the STP root port.	15
<b>Hold Time (secs)</b>	
The minimum period between the transmissions of configuration BPDUs.	1
<b>CST Regional Root</b>	
The priority and the base MAC address of the CST regional root.	MAC address
<b>CST Path Cost</b>	
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
<input type="checkbox"/>		<input type="text"/>	- ▾	<input type="text"/>		<input type="text"/>
<input type="checkbox"/>	0/1	128	Disable	20000	Disabled	2
<input type="checkbox"/>	0/2	128	Disable	20000	Disabled	2
<input type="checkbox"/>	0/3	128	Disable	20000	Disabled	2
<input type="checkbox"/>	0/4	128	Disable	200000	Disabled	2
<input type="checkbox"/>	0/5	128	Disable	20000	Disabled	2
<input type="checkbox"/>	0/6	128	Disable	200000	Disabled	2
<input type="checkbox"/>	0/7	128	Disable	20000	Disabled	2
<input type="checkbox"/>	0/8	128	Disable	20000	Disabled	2
<input type="checkbox"/>	po1	128	Disable	10000	Disabled	2
<input type="checkbox"/>	po2	128	Disable	10000	Disabled	2
<input type="checkbox"/>	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

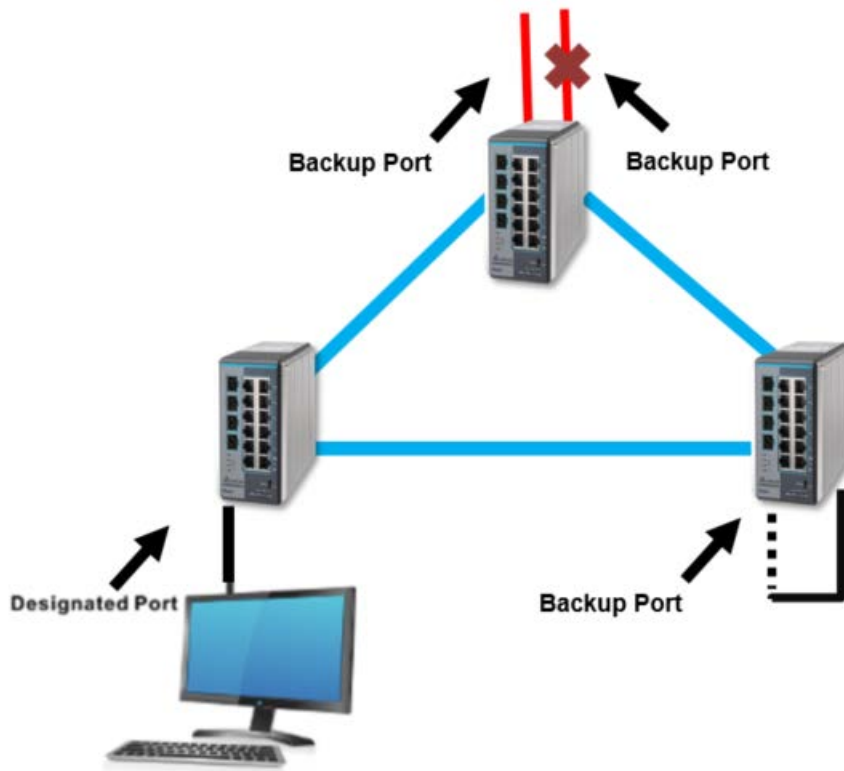
## CST Port Configuration

Description	Factory default
<b>Interface</b>	
This field displays the interface number or port channel number.	<i>interface number</i>
<b>Port Priority</b>	
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
<b>Admin Edge Port</b>	
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: <ul style="list-style-type: none"> <li>• <b>Enable:</b> The interface is an edge port.</li> <li>• <b>Disable:</b> The interface is not an edge port.</li> </ul>	Disable
<b>Port Path Cost</b>	
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
<b>Auto Calculated Port Path Cost</b>	
This field shows whether you have globally enabled or disabled the dynamic path cost on the CST Configuration screen.	Disable
<b>Hello Timer</b>	
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.  <b>Notice:</b> You can set the hello time only when the STP operation mode is MSTP.	2
<b>BPDU Forwarding</b>	
Specify whether the interface sets the mcheck flag to forward BPDUs: <ul style="list-style-type: none"> <li>• <b>Enable:</b> Depending on the STP operation mode, RST or MST BPDUs are forwarded.</li> <li>• <b>Disable:</b> BPDUs are not forwarded.</li> </ul>	Disable
<b>Auto Edge</b>	
Specify whether the interface automatically becomes an edge port if it does not process BPDUs for a while: <ul style="list-style-type: none"> <li>• <b>Enable:</b> The interface becomes an edge port.</li> <li>• <b>Disable:</b> The interface does not become an edge port.</li> </ul>	Enable
<b>Root Guard</b>	
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: <ul style="list-style-type: none"> <li>• <b>Enable:</b> The interface can enter the discarding state.</li> <li>• <b>Disable:</b> The interface can not enter discarding state.</li> </ul>	Disable
<b>TCN Guard</b>	
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. <ul style="list-style-type: none"> <li>• <b>Enable:</b> The interface can propagate the topology change information.</li> <li>• <b>Disable:</b> The interface can not propagate the topology change information.</li> </ul>	Disable
<b>Port Mode</b>	
Specify the Spanning Tree Protocol (STP) administrative mode that is associated with the port or port channel: <ul style="list-style-type: none"> <li>• <b>Disable:</b> STP is disabled for the port or port channel.</li> </ul>	Enable

Description	Factory default
<ul style="list-style-type: none"> <li><b>Enable:</b> STP is enabled for the port or port channel.</li> </ul>	
<b>Port Forwarding State</b>	
This field displays whether the port is up and forwards traffic (Forwarding) or down and discards traffic (Discarding).	Discarding
<b>Protocol Migration</b>	
Force the specified port to set the mcheck flag to transmit RST or MST BPDUs: <ul style="list-style-type: none"> <li><b>True:</b> The interface can receive the BPDU flood.</li> <li><b>False:</b> The interface can not receive the BPDU flood.</li> </ul>	False
<b>PointToPoint Status</b>	
Specify the point-to-point status of the interface in the CIST: <ul style="list-style-type: none"> <li><b>ForceTrue:</b> The interface has a point-to-point connection to a switch, bridge, or end node, irrespective of the actual connection.</li> <li><b>ForceFalse:</b> The interface does not have a point-to-point connection to a switch, bridge, or end node, irrespective of the actual connection.</li> <li><b>Auto:</b> The type of connection is automatically detected.</li> </ul>	Auto

### 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: <ul style="list-style-type: none"> <li><b>Discarding:</b> The interface is in the discarding mode; it can not forward traffic and can not learn new MAC addresses.</li> <li><b>Learning:</b> The interface is in the learning mode; it can not forward traffic, but it can learn new MAC addresses.</li> <li><b>Forwarding:</b> The interface is in the forwarding mode; it can forward traffic and learn new MAC addresses.</li> </ul>
Port Role	The role type of the interface in the spanning tree: One of the following options is displayed: <ul style="list-style-type: none"> <li>Root</li> <li>Master</li> <li>Designated</li> <li>Alternate</li> <li>Backup</li> <li>Disabled</li> </ul>

3

Item	Description
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 advertised by the designated port to the LAN.  <b>Note:</b> 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.  <b>Note:</b> 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: <ul style="list-style-type: none"> <li>• <b>Enabled:</b> The interface is an edge port.</li> <li>• <b>Disabled:</b> The interface is not an edge port.</li> </ul>
Point-to-Point MAC	Connection types: <ul style="list-style-type: none"> <li>• <b>True:</b> The connection is a point-to-point connection.</li> <li>• <b>False:</b> The connection is a shared LAN connection.</li> </ul>
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

MST Configuration									
	MST ID	Priority	Bridge Identifier	VLAN List	Time Since Topology Change	Topology Change Count	Designated Root	Root Path Cost	Root Port Identifier
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	1	4096	10:00:00:18:23:01:20:61	1	0 day 0 hr 0 min 0 sec	0	10:00:00:18:23:01:20:61	0	00:00

#### MST Configuration settings

Description	Factory default
<b>MST ID</b>	
Enter an identifier for the MST instance. Enter a number in the range of 1 to 16.	None
<b>Priority</b>	
Enter the bridge priority. Enter a number between 0 and 61440 which is a multiple of 4096.	32768
<b>VLAN List</b>	
Enter the vlan id list. Enter a number in the range of 1 to 4094	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

MST Port Status									
Select MST									1 ▾
MST Port Status									
	Interface	Port Priority	Port Cost	Port Mode	Auto Calculated Port Path Cost	Port ID	Port Forwarding State	Port Role	Designated Root
<input type="checkbox"/>				- ▾					
<input type="checkbox"/>	0/1	128	20000	Enabled	Disabled	80:01	Discarding	Disabled	80:00:00:18:23:01:20:61
<input type="checkbox"/>	0/2	128	20000	Enabled	Disabled	80:02	Discarding	Disabled	80:00:00:18:23:01:20:61
<input type="checkbox"/>	0/3	128	20000	Enabled	Disabled	80:03	Discarding	Disabled	80:00:00:18:23:01:20:61
<input type="checkbox"/>	0/4	128	200000	Enabled	Disabled	80:04	Discarding	Disabled	80:00:00:18:23:01:20:61
<input type="checkbox"/>	0/5	128	200000	Enabled	Disabled	80:05	Forwarding	Master	80:00:00:18:23:01:20:61
<input type="checkbox"/>	0/6	128	200000	Enabled	Disabled	80:06	Forwarding	Designated	80:00:00:18:23:01:20:61
<input type="checkbox"/>	0/7	128	20000	Enabled	Disabled	80:07	Discarding	Disabled	80:00:00:18:23:01:20:61
<input type="checkbox"/>	0/8	128	20000	Enabled	Disabled	80:08	Discarding	Disabled	80:00:00:18:23:01:20:61
<input type="checkbox"/>	po1	128	10000	Enabled	Disabled	80:09	Discarding	Disabled	80:00:00:18:23:01:20:61
<input type="checkbox"/>	po2	128	10000	Enabled	Disabled	80:0a	Discarding	Disabled	80:00:00:18:23:01:20:61
<input type="checkbox"/>	po3	128	10000	Enabled	Disabled	80:0b	Discarding	Disabled	80:00:00:18:23:01:20:61

[Apply](#) [Refresh](#)

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.  <b>Note:</b> 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. <ul style="list-style-type: none"> <li>• <b>Enable:</b> Enables STP for the interface. This is the default setting.</li> <li>• <b>Disable:</b> Disables STP for the interface.</li> </ul>
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: <ul style="list-style-type: none"> <li>• <b>Discarding:</b> The interface is in the discarding mode; it can not forward traffic and can not learn new MAC addresses.</li> <li>• <b>Learning:</b> The interface is in the learning mode; it can not forward traffic, but it can learn new MAC addresses.</li> <li>• <b>Forwarding:</b> The interface is in the forwarding mode; it can forward traffic and learn new MAC addresses.</li> </ul>
Port Role	The role types of the interface in the MST instance: One of the following options is displayed: <ul style="list-style-type: none"> <li>• Root</li> <li>• Master</li> <li>• Designated</li> <li>• Alternate</li> <li>• Backup</li> <li>• Disabled</li> </ul>
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 advertised by the designated port to the LAN.  <b>Note:</b> 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	 <b>Note:</b> 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.  <b>Note:</b> 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
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

Item	Description
	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								
	Instance ID	Mode	Port1	Port1 Role	Port2	Port2 Role	Ring Status	Admin Status
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>		<input type="text"/>			

#### 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: <ul style="list-style-type: none"> <li><b>Master:</b> The master node manages the ring network, and there can only be one master node in a ring network.</li> <li><b>Slave:</b> The slave nodes forward the hello packets along the ring, and there are up to 250 slave nodes.</li> </ul>
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: <ul style="list-style-type: none"> <li><b>Discover:</b> The ring is not completed yet</li> <li><b>Monitor:</b> The ring is completed and healthy.</li> <li><b>Fault:</b> The ring failed. The backup path is activated.</li> </ul> Slave State: <ul style="list-style-type: none"> <li><b>Forwarding:</b> After the instance is created, it will stay at this state.</li> <li><b>Hold:</b> It is a middle state of the slave when 2 member ports are linked</li> </ul>

Item	Description
	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								
	Instance ID	Mode	Port1	Port1 Role	Port2	Port2 Role	Chain Status	Admin Status
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>		<input type="text"/>			

#### 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: <ul style="list-style-type: none"> <li><b>Head:</b> A Head node has one head port and one member port.</li> <li><b>Tail:</b> A Tail node has one tail port and one member port. The tail has two statuses: block and forwarding.</li> <li><b>Member:</b> A Member node has two member ports.</li> </ul>
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: <ul style="list-style-type: none"> <li><b>Discover:</b> The chain is not completed yet.</li> <li><b>Monitor:</b> The chain is completed and healthy. The Head port is linked up, and no node is disconnected.</li> <li><b>Fault:</b> The chain is disconnected because the member node is linked down or the head port is linked down.</li> <li><b>Hold:</b> The Head port is linked down-&gt;up.</li> </ul> On the Member node: <ul style="list-style-type: none"> <li><b>Forwarding:</b> After the instance is created, it will stay at this state.</li> <li><b>Hold:</b> It is a middle state of the slave when 2 member ports are linked down-&gt;up. It changes to the Forwarding state when it receives the clear-FDB message or HOLD timer timeout.</li> </ul> On the Tail node: <ul style="list-style-type: none"> <li><b>Discover:</b> The chain is not completed yet.</li> <li><b>Monitor:</b> The chain is completed and healthy.</li> <li><b>Fault:</b> The chain failed. The backup path is activated.</li> </ul>
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**

ONE COUPLING Configuration						
Instance ID	Mode	Port	Port Role	Coupling Status	Admin Status	
<input type="text"/>	<input type="text"/>	<input type="text"/>				

3

**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: <ul style="list-style-type: none"> <li><b>Head:</b> 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.</li> <li><b>Tail:</b> 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.</li> </ul>
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: <ul style="list-style-type: none"> <li><b>Monitor:</b> The head port is linked up.</li> <li><b>Fault:</b> The head port is linked down. It will notify the tail node to activate the backup path.</li> <li><b>Link-Up:</b> The head port is linked up. If the head port is linked down at this state, it will change to Fault again.</li> </ul> <li><b>Hold:</b> After the Link-Up timer timeout occurs, the node will change to the HOLD state.</li> Tail State: <ul style="list-style-type: none"> <li><b>Discover:</b> The coupling is not completed yet. It waits for the head port link status message from the head node.</li> <li><b>Monitor:</b> The coupling is completed and healthy.</li> <li><b>Fault:</b> The coupling is disconnected.</li> </ul>
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.

## Redundancy Cruiser

Redundancy Cruiser	
Instance ID	1
Topology	Ring
Status	MONITOR
Master IP	192.168.1.142
Master MAC	00:18:23:01:20:61
Faults Detected	4 <input type="button" value="Clear"/>
Last Active Node on Port 1	None
Last Active Node on Port 2	None

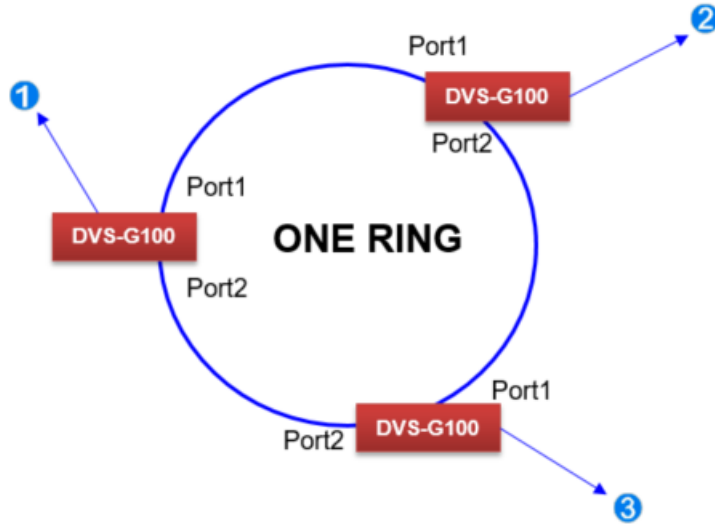
### Redundancy Cruiser

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. <ul style="list-style-type: none"> <li>Ring: It is cruising in ONE RING topology.</li> <li>Chain: It is cruising in ONE CHAIN topology.</li> <li>Coupling: It is cruising in ONE COUPLING topology.</li> </ul>
Status	This field shows the network status which is under monitoring. <ul style="list-style-type: none"> <li>DISCOVER: The topology is not completed yet.</li> <li>MONITOR: The topology is completed and healthy.</li> <li>FAULT: The topology failed. The backup path is activated.</li> </ul>
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.

### 3.3.3 Redundancy Application Setting

Introduce how to set up a basic example of Delta One Ring/One Chain.

- ONE Ring



1. In the CST Port configuration, set the network port mode corresponding to one ring/chain to disable.

- Basic Setting
- SNMP Manager
- Network Redundancy
  - STP
    - STP Configuration
    - CST Configuration**
    - CST Port Configuration
    - CST Port Status
    - MST Configuration
    - MST Port Status
    - STP Statistics
    - ONE RING Plus Configuration

CST Port Configuration											
	Interface	Port Priority	Admin Edge Port	Port Path Cost	Auto Calculated Port Path Cost	Hello Time	BPDU Forwarding	Auto Edge	Root Guard	TCN Guard	Port Mode
<input type="checkbox"/>			-				-	-	-	-	-
<input checked="" type="checkbox"/>	0/1	128	Disable	20000	Disabled	2	Disable	Enable	Disable	Disable	Disable
<input checked="" type="checkbox"/>	0/2	128	Disable	20000	Disabled	2	Disable	Enable	Disable	Disable	Disable
<input checked="" type="checkbox"/>	0/3	128	Disable	20000	Disabled	2	Disable	Enable	Disable	Disable	Disable
<input type="checkbox"/>	0/4	128	Disable	20000	Disabled	2	Disable	Enable	Disable	Disable	Enable
<input type="checkbox"/>	0/5	128	Disable	20000	Disabled	2	Disable	Enable	Disable	Disable	Enable

2. Please follow the number and correspond to the following network maps to make the corresponding settings.

①

ONE RING Plus Configuration								
	Instance ID	Mode	Port1	Port1 Role	Port2	Port2 Role	ONE RING Status	Admin Status
<input type="checkbox"/>		-	-		-			
<input type="checkbox"/>	1	Master	0/1	Head	0/2	Tail	DISCOVER	Active

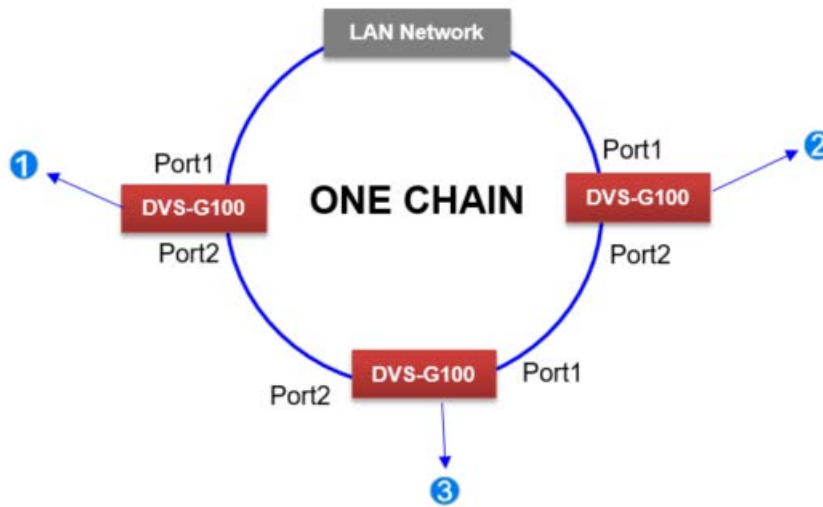
②

ONE RING Plus Configuration								
	Instance ID	Mode	Port1	Port1 Role	Port2	Port2 Role	ONE RING Plus Status	Admin Status
<input type="checkbox"/>		-	-		-			
<input type="checkbox"/>	1	Slave	0/1	Member	0/2	Member	FAULT	Active

③

ONE RING Plus Configuration								
	Instance ID	Mode	Port1	Port1 Role	Port2	Port2 Role	ONE RING Plus Status	Admin Status
<input type="checkbox"/>		-	-		-			
<input type="checkbox"/>	1	Slave	0/1	Member	0/2	Member	FAULT	Active

• ONE Chain



1. In the CST Port configuration, set the network port mode corresponding to one ring/chain to disable.

- Basic Setting
- SNMP Manager
- Network Redundancy
  - STP
    - STP Configuration
    - CST Configuration**
    - CST Port Configuration
    - CST Port Status
    - MST Configuration
    - MST Port Status
    - STP Statistics
    - ONE RING Plus Configuration

CST Port Configuration											
	Interface	Port Priority	Admin Edge Port	Port Path Cost	Auto Calculated Port Path Cost	Hello Time	BPDU Forwarding	Auto Edge	Root Guard	TCN Guard	Port Mode
<input type="checkbox"/>			-				-	-	-	-	-
<input checked="" type="checkbox"/>	0/1	128	Disable	20000	Disabled	2	Disable	Enable	Disable	Disable	Disable
<input checked="" type="checkbox"/>	0/2	128	Disable	20000	Disabled	2	Disable	Enable	Disable	Disable	Disable
<input checked="" type="checkbox"/>	0/3	128	Disable	20000	Disabled	2	Disable	Enable	Disable	Disable	Disable
<input type="checkbox"/>	0/4	128	Disable	20000	Disabled	2	Disable	Enable	Disable	Disable	Enable
<input type="checkbox"/>	0/5	128	Disable	20000	Disabled	2	Disable	Enable	Disable	Disable	Enable

2. Please follow the number and correspond to the following network maps to make the corresponding settings.

**ONE CHAIN Plus Configuration**

	Instance ID	Mode	Port1	Port1 Role	Port2	Port2 Role	ONE CHAIN Plus Status	Admin Status
<input type="checkbox"/>		-	-		-			
<input type="checkbox"/>	1	Head	0/1	Head	0/2	Member	IDLE	Active

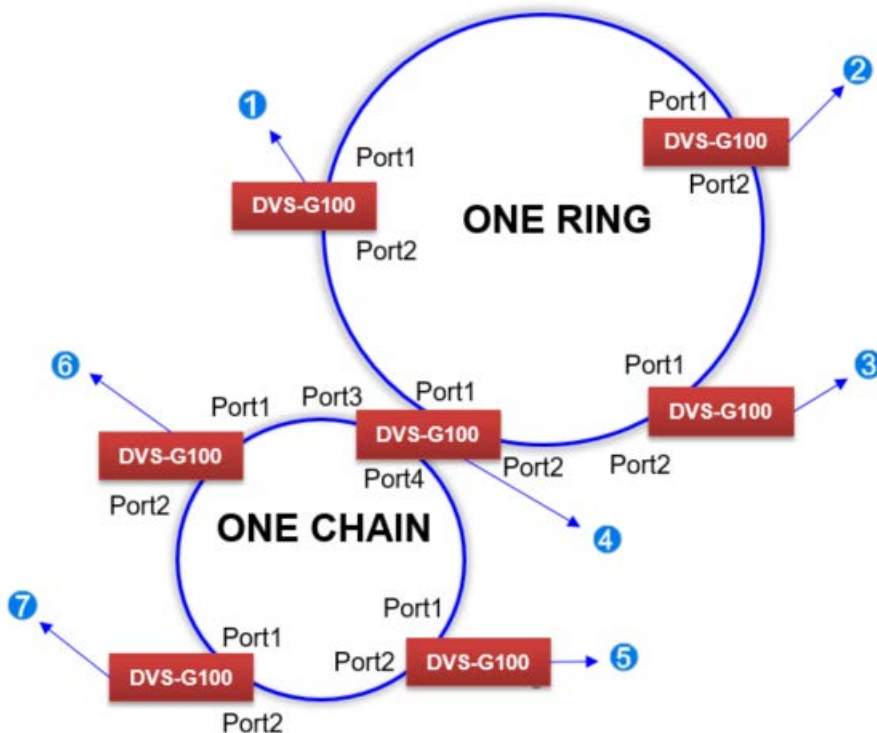
**ONE CHAIN Plus Configuration**

	Instance ID	Mode	Port1	Port1 Role	Port2	Port2 Role	ONE CHAIN Plus Status	Admin Status
<input type="checkbox"/>		-	-		-			
<input type="checkbox"/>	1	Tail	0/1	Tail	0/2	Member	DISCOVER	Active

**ONE CHAIN Plus Configuration**

	Instance ID	Mode	Port1	Port1 Role	Port2	Port2 Role	ONE CHAIN Plus Status	Admin Status
<input type="checkbox"/>		-	-		-			
<input type="checkbox"/>	1	Member	0/1	Member	0/2	Member	FAULT	Active

• ONE RING + CHAIN



1. In the CST Port configuration, set the network port mode corresponding to one ring/chain to disable.

- Basic Setting
- SNMP Manager
- Network Redundancy
  - STP
    - STP Configuration
    - CST Configuration**
    - CST Port Configuration
    - CST Port Status
    - MST Configuration
    - MST Port Status
    - STP Statistics
    - ONE RING Plus Configuration

CST Port Configuration											
Interface	Port Priority	Admin Edge Port	Port Path Cost	Auto Calculated Port Path Cost	Hello Time	BPDU Forwarding	Auto Edge	Root Guard	TCN Guard	Port Mode	
<input checked="" type="checkbox"/>	0/1	128	Disable	20000	Disabled	2	Disable	Enable	Disable	Disable	Disable
<input checked="" type="checkbox"/>	0/2	128	Disable	20000	Disabled	2	Disable	Enable	Disable	Disable	Disable
<input checked="" type="checkbox"/>	0/3	128	Disable	20000	Disabled	2	Disable	Enable	Disable	Disable	Disable
<input type="checkbox"/>	0/4	128	Disable	20000	Disabled	2	Disable	Enable	Disable	Disable	Enable
<input type="checkbox"/>	0/5	128	Disable	20000	Disabled	2	Disable	Enable	Disable	Disable	Enable

2. Please follow the number and correspond to the following network maps to make the corresponding settings.

①

ONE RING Plus Configuration								
Instance ID	Mode	Port1	Port1 Role	Port2	Port2 Role	ONE RING Status	Admin Status	
<input type="checkbox"/>	-	-		-				
<input checked="" type="checkbox"/>	1	Master	0/1	Head	0/2	Tail	DISCOVER	Active

②

ONE RING Plus Configuration								
Instance ID	Mode	Port1	Port1 Role	Port2	Port2 Role	ONE RING Plus Status	Admin Status	
<input type="checkbox"/>	-	-		-				
<input checked="" type="checkbox"/>	1	Slave	0/1	Member	0/2	Member	FAULT	Active

③

ONE RING Plus Configuration								
Instance ID	Mode	Port1	Port1 Role	Port2	Port2 Role	ONE RING Plus Status	Admin Status	
<input type="checkbox"/>	-	-		-				
<input checked="" type="checkbox"/>	1	Slave	0/1	Member	0/2	Member	FAULT	Active

4

ONE RING Plus Configuration								
	Instance ID	Mode	Port1	Port1 Role	Port2	Port2 Role	ONE RING Plus Status	Admin Status
<input type="checkbox"/>		-	-		-			
<input type="checkbox"/>	1	Slave	0/1	Member	0/2	Member	FAULT	Active

5

ONE CHAIN Plus Configuration								
	Instance ID	Mode	Port1	Port1 Role	Port2	Port2 Role	ONE CHAIN Plus Status	Admin Status
<input type="checkbox"/>		-	-		-			
<input type="checkbox"/>	1	Tail	0/1	Tail	0/2	Member	DISCOVER	Active

6

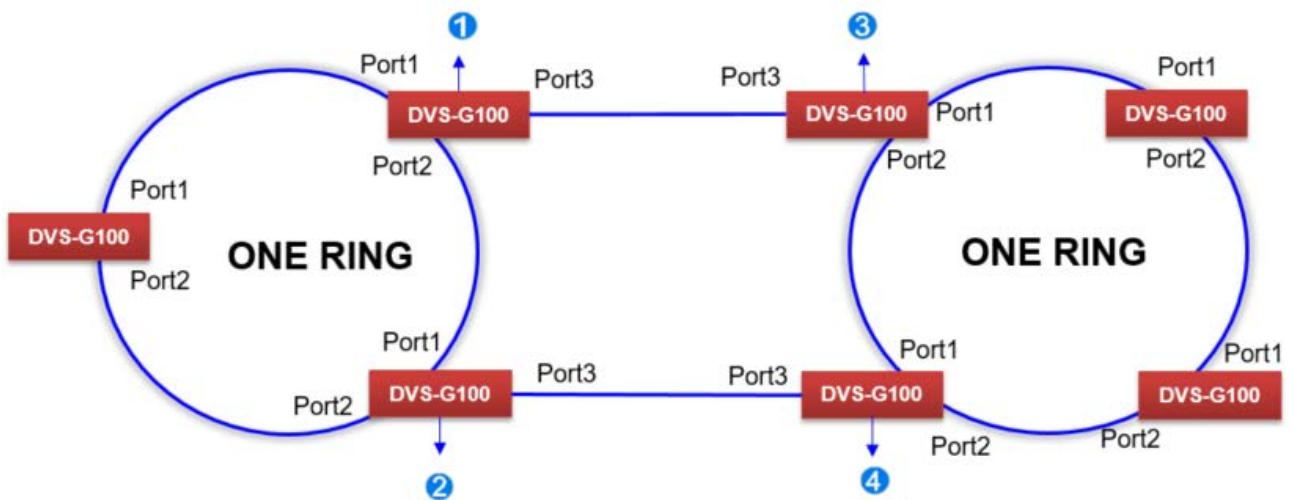
ONE CHAIN Plus Configuration								
	Instance ID	Mode	Port1	Port1 Role	Port2	Port2 Role	ONE CHAIN Plus Status	Admin Status
<input type="checkbox"/>		-	-		-			
<input type="checkbox"/>	1	Head	0/1	Head	0/2	Member	IDLE	Active

7

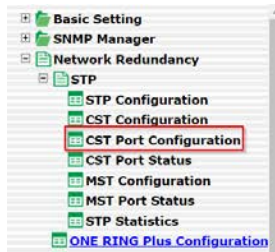
ONE CHAIN Plus Configuration								
	Instance ID	Mode	Port1	Port1 Role	Port2	Port2 Role	ONE CHAIN Plus Status	Admin Status
<input type="checkbox"/>		-	-		-			
<input type="checkbox"/>	1	Member	0/1	Member	0/2	Member	FAULT	Active

3

• Coupling RING



1. In the CST Port configuration, set the network port mode corresponding to one ring/chain to disable.



CST Port Configuration

CST Port Configuration											
	Interface	Port Priority	Admin Edge Port	Port Path Cost	Auto Calculated Port Path Cost	Hello Time	BPDU Forwarding	Auto Edge	Root Guard	TCN Guard	Port Mode
<input type="checkbox"/>			-				-	-	-	-	-
<input checked="" type="checkbox"/>	0/1	128	Disable	20000	Disabled	2	Disable	Enable	Disable	Disable	Disable
<input checked="" type="checkbox"/>	0/2	128	Disable	20000	Disabled	2	Disable	Enable	Disable	Disable	Disable
<input checked="" type="checkbox"/>	0/3	128	Disable	20000	Disabled	2	Disable	Enable	Disable	Disable	Disable
<input type="checkbox"/>	0/4	128	Disable	20000	Disabled	2	Disable	Enable	Disable	Disable	Enable
<input type="checkbox"/>	0/5	128	Disable	20000	Disabled	2	Disable	Enable	Disable	Disable	Enable

2. Please follow the number and correspond to the following network maps to make the corresponding settings.

**1**

ONE RING Plus Configuration								
	Instance ID	Mode	Port1	Port1 Role	Port2	Port2 Role	ONE RING Plus Status	Admin Status
<input type="checkbox"/>		-	-		-			
<input type="checkbox"/>	1	Slave	0/1	Member	0/2	Member	FAULT	Active

ONE COUPLING Plus Configuration						
	Instance ID	Mode	Port	Port Role	ONE COUPLING Plus Status	Admin Status
<input type="checkbox"/>		-	-			
<input type="checkbox"/>	1	Head	0/3	Head	FAULT	Active

**3**

**2**

ONE RING Plus Configuration								
	Instance ID	Mode	Port1	Port1 Role	Port2	Port2 Role	ONE RING Status	Admin Status
<input type="checkbox"/>		-	-		-			
<input type="checkbox"/>	1	Master	0/1	Head	0/2	Tail	DISCOVER	Active

ONE COUPLING Plus Configuration						
	Instance ID	Mode	Port	Port Role	ONE COUPLING Plus Status	Admin Status
<input type="checkbox"/>		-	-			
<input type="checkbox"/>	1	Tail	0/3	Tail	DISCOVER	Active

**3**

ONE RING Plus Configuration								
	Instance ID	Mode	Port1	Port1 Role	Port2	Port2 Role	ONE RING Plus Status	Admin Status
<input type="checkbox"/>		-	-		-			
<input type="checkbox"/>	1	Slave	0/1	Member	0/2	Member	FAULT	Active

ONE COUPLING Plus Configuration						
	Instance ID	Mode	Port	Port Role	ONE COUPLING Plus Status	Admin Status
<input type="checkbox"/>		-	-			
<input type="checkbox"/>	1	Head	0/3	Head	FAULT	Active

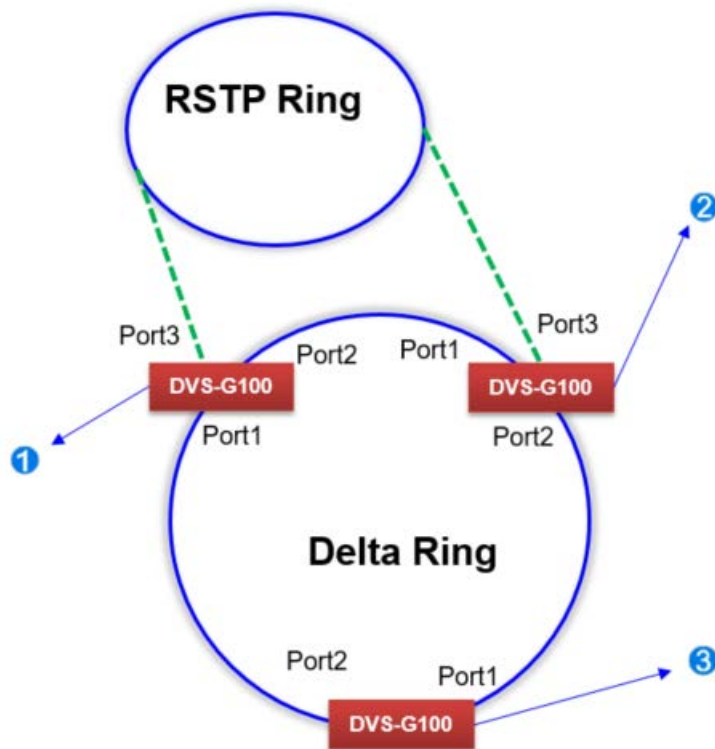
**4**

ONE RING Plus Configuration								
	Instance ID	Mode	Port1	Port1 Role	Port2	Port2 Role	ONE RING Status	Admin Status
<input type="checkbox"/>		-	-		-			
<input type="checkbox"/>	1	Master	0/1	Head	0/2	Tail	DISCOVER	Active

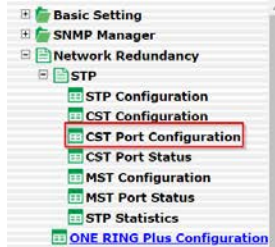
  

ONE COUPLING Plus Configuration						
	Instance ID	Mode	Port	Port Role	ONE COUPLING Plus Status	Admin Status
<input type="checkbox"/>		-	-			
<input type="checkbox"/>	1	Tail	0/3	Tail	DISCOVER	Active

• Dual Homing



1. In the CST Port configuration, set the network port mode corresponding to one ring/chain to disable.



CST Port Configuration

	Interface	Port Priority	Admin Edge Port	Port Path Cost	Auto Calculated Port Path Cost	Hello Time	BPDU Forwarding	Auto Edge	Root Guard	TCN Guard	Port Mode
<input type="checkbox"/>											
<input checked="" type="checkbox"/>	0/1	128	Disable	20000	Disabled	2	Disable	Enable	Disable	Disable	Disable
<input checked="" type="checkbox"/>	0/2	128	Disable	20000	Disabled	2	Disable	Enable	Disable	Disable	Disable
<input checked="" type="checkbox"/>	0/3	128	Disable	20000	Disabled	2	Disable	Enable	Disable	Disable	Disable
<input type="checkbox"/>	0/4	128	Disable	20000	Disabled	2	Disable	Enable	Disable	Disable	Enable
<input type="checkbox"/>	0/5	128	Disable	20000	Disabled	2	Disable	Enable	Disable	Disable	Enable

2. Please follow the number and correspond to the following network maps to make the corresponding settings.

**1**

ONE RING Plus Configuration								
	Instance ID	Mode	Port1	Port1 Role	Port2	Port2 Role	ONE RING Plus Status	Admin Status
<input type="checkbox"/>		-	-		-			
<input type="checkbox"/>	1	Slave	0/1	Member	0/2	Member	FAULT	Active

ONE COUPLING Plus Configuration						
	Instance ID	Mode	Port	Port Role	ONE COUPLING Plus Status	Admin Status
<input type="checkbox"/>		-	-			
<input type="checkbox"/>	1	Head	0/3	Head	FAULT	Active

**3**

**2**

ONE RING Plus Configuration								
	Instance ID	Mode	Port1	Port1 Role	Port2	Port2 Role	ONE RING Status	Admin Status
<input type="checkbox"/>		-	-		-			
<input type="checkbox"/>	1	Master	0/1	Head	0/2	Tail	DISCOVER	Active


ONE COUPLING Plus Configuration						
	Instance ID	Mode	Port	Port Role	ONE COUPLING Plus Status	Admin Status
<input type="checkbox"/>		-	-			
<input type="checkbox"/>	1	Tail	0/3	Tail	DISCOVER	Active

**3**

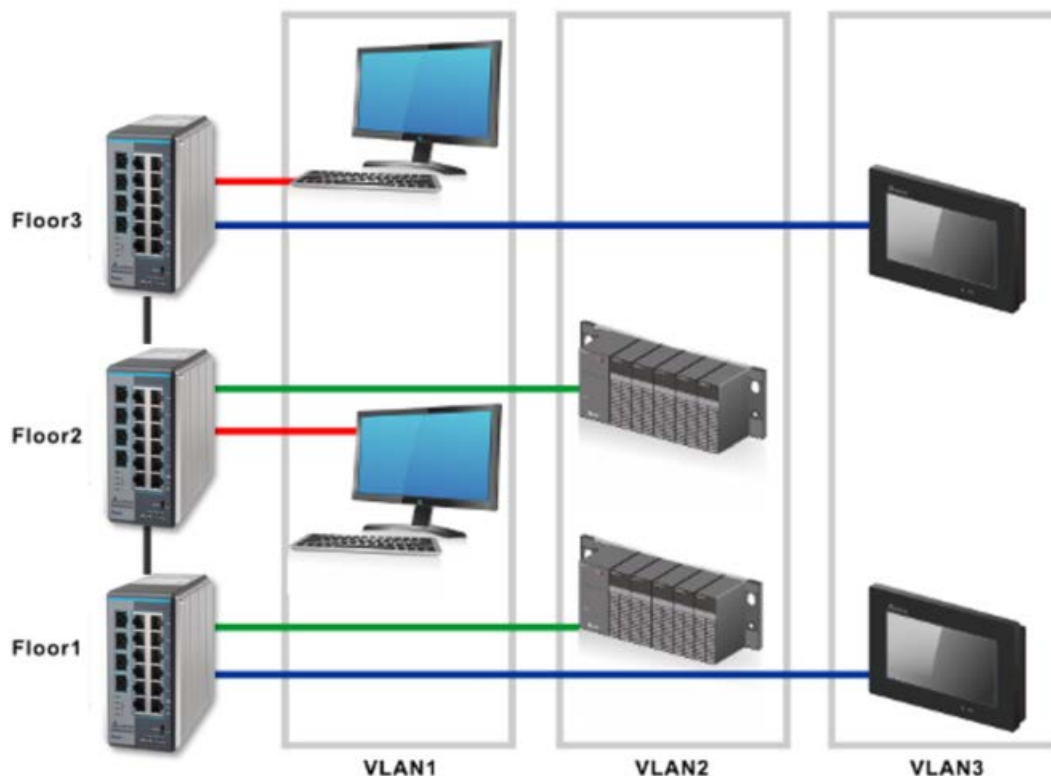
ONE RING Plus Configuration								
	Instance ID	Mode	Port1	Port1 Role	Port2	Port2 Role	ONE RING Plus Status	Admin Status
<input type="checkbox"/>		-	-		-			
<input type="checkbox"/>	1	Slave	0/1	Member	0/2	Member	FAULT	Active

### 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 Unaware. You can choose the properly VLAN mode on the Delta managed switch so that it can increase the efficiency of your network.

#### VLAN Mode Configuration

VLAN Mode Configuration	
VLAN Mode	<input checked="" type="radio"/> 802.1Q <input type="radio"/> VLAN Unaware
<input type="button" value="Cancel"/> <input type="button" value="Apply"/>	

#### 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 functionalities 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**

VLAN Configuration			
	VLAN ID	VLAN Name	VLAN Type
<input type="checkbox"/>	1	Default	Default
<input type="checkbox"/>	2	VLAN2	Static
<input type="checkbox"/>	3	VLAN3	Static

**VLAN Configuration**

Description	Factory default
<b>VLAN ID</b>	
Enter the identifier for the new VLAN. The range can be set in the range of 1 to 4094.	None
<b>VLAN Name</b>	
Enter a name for the VLAN. The name can be up to 32 alphanumeric characters long, including blanks.	None
<b>VLAN Type</b>	
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 Membership									
VLAN ID	1		Group Operation		-				
VLAN Name	Default		UNTAGGED PORT MEMBERS						
VLAN Type	Default		TAGGED PORT MEMBERS						
Port	1	2	3	4	5	6	7	8	
	U	T	T	X	U	U	U	U	
LAG	1		2		3				
	U		U		U				

**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

Status	Description
	interface or LAG are tagged with the port VLAN ID. Click <b>Tagged Port Members</b> 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 <b>Untagged Port Members</b> 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
<input type="checkbox"/>			-	-	
<input type="checkbox"/>	0/1	1	All	Disabled	0
<input type="checkbox"/>	0/2	1	All	Disabled	0
<input type="checkbox"/>	0/3	1	All	Disabled	0
<input type="checkbox"/>	0/4	1	All	Disabled	0
<input type="checkbox"/>	0/5	1	All	Disabled	0
<input type="checkbox"/>	0/6	1	All	Disabled	0
<input type="checkbox"/>	0/7	1	All	Disabled	0
<input type="checkbox"/>	0/8	1	All	Disabled	0
<input type="checkbox"/>	po1	1	All	Disabled	0
<input type="checkbox"/>	po2	1	All	Disabled	0
<input type="checkbox"/>	po3	1	All	Disabled	0

Apply

### Port PVID Configuration

Description	Factory default
<b>Port</b>	
This field displays the interface number or port channel number.	<i>interface number</i>
<b>PVID</b>	
This field displays the current PVID.	1
<b>Acceptable Frame Types</b>	
Specify the types of frames that can be received on the interface: <ul style="list-style-type: none"> <li><b>All:</b> 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.</li> <li><b>Tagged:</b> Only forward VLAN-tagged frames, drop all other frames.</li> <li><b>Untagged and Priority Tagged:</b> Forward untagged and priority-tagged frames, drop VLAN-tagged frames.</li> </ul>	All
<b>Ingress Filtering</b>	
Specify whether the ingress filtering is applied: <ul style="list-style-type: none"> <li><b>Enabled:</b> 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.</li> <li><b>Disabled:</b> The ingress filtering is disabled for the interface. All frames are forwarded.</li> </ul>	Disabled
<b>Port Priority</b>	
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		
GVRP Mode <input type="radio"/> Disable <input checked="" type="radio"/> Enable		
GVRP Port Configuration		
	Interface	Port GVRP Mode
<input type="checkbox"/>		-
<input type="checkbox"/>	0/1	Enable
<input type="checkbox"/>	0/2	Enable
<input type="checkbox"/>	0/3	Enable
<input type="checkbox"/>	0/4	Enable
<input type="checkbox"/>	0/5	Enable
<input type="checkbox"/>	0/6	Enable
<input type="checkbox"/>	0/7	Enable
<input type="checkbox"/>	0/8	Enable
<input type="checkbox"/>	po1	Enable
<input type="checkbox"/>	po2	Enable
<input type="checkbox"/>	po3	Enable

**GVRP Configuration**

Description	Factory default
<b>GVRP Mode</b>	
Specify whether the GVRP mode is enabled. <ul style="list-style-type: none"> <li><b>Disable:</b> The GVRP mode is disabled.</li> <li><b>Enable:</b> The GVRP mode is enabled.</li> </ul>	Enable

**GVRP Port Configuration**

Description	Factory default
<b>Interface</b>	
This field displays the interface number.	<i>interface number</i>
<b>Port GVRP Mode</b>	
Specify whether the GVRP mode is enabled on the interface.	Enable

**3.4.7 QinQ 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.

**QinQ VLAN Configuration**

Global Configuration	
Global Status	<input type="button" value="Disable"/> ▾
Global EtherType	<input type="button" value="Custom Tag"/> ▾
Custom Value	<input type="text" value="0x8100"/> (0x0001 to 0xFFFF)

**Global Configuration**

Description	Factory default
<b>Global Status</b>	

Specify whether the status in global configuration is activated or not.	Disable
<b>Global EtherType</b>	
Specify which EtherType can be globally configured. <ul style="list-style-type: none"> <li>• <b>802.1Q Tag:</b> Set EtherType as 802.1Q mode.</li> <li>• <b>vMAN Tag:</b> Set EtherType as vMAN mode.</li> <li>• <b>Custom Tag:</b> Set EtherType as Custom mode. You can define the TPID of the VLAN, and the range is 0x0001 to 0xFFFF.</li> </ul>	802.1Q
<b>Custom Value</b>	
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		
	Interface	Admin Mode
<input type="checkbox"/>		- ▾
<input type="checkbox"/>	0/1	Disable
<input type="checkbox"/>	0/2	Disable
<input type="checkbox"/>	0/3	Disable
<input type="checkbox"/>	0/4	Disable
<input type="checkbox"/>	0/5	Disable
<input type="checkbox"/>	0/6	Disable
<input type="checkbox"/>	0/7	Disable
<input type="checkbox"/>	0/8	Disable
<input type="checkbox"/>	0/9	Disable
<input type="checkbox"/>	0/10	Disable
<input type="checkbox"/>	0/11	Disable
<input type="checkbox"/>	0/12	Disable

**Double VLAN Configuration**

Description	Factory default
<b>Interface</b>	
The interface number.	<i>interface number</i>
<b>Admin Mode</b>	
Enable/Disable the feature on the port. <ul style="list-style-type: none"> <li>• <b>Enable:</b> Enable Double VLAN ( Q-in-Q ) function. The port will become provider port</li> <li>• <b>Disable:</b> Disable the Double VLAN (Q-in-Q) function, and the port becomes a customer port.</li> </ul>	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.

**MAC Based VLAN Configuration**

MAC Based VLAN Configuration		
	MAC Address	VLAN ID
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
<input type="button" value="Add"/> <input type="button" value="Delete"/> <input type="button" value="Cancel"/>		

**MAC Based VLAN**

Description	Factory default
<b>MAC Address</b>	
Specify a unicast mac address.	None
<b>VLAN ID</b>	
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 Configuration**

IP Subnet Based VLAN Configuration			
	IP Address	Subnet Mask	VLAN ID
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

**IP Subnet Based VLAN**

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

**3.5 Multicast Filtering**

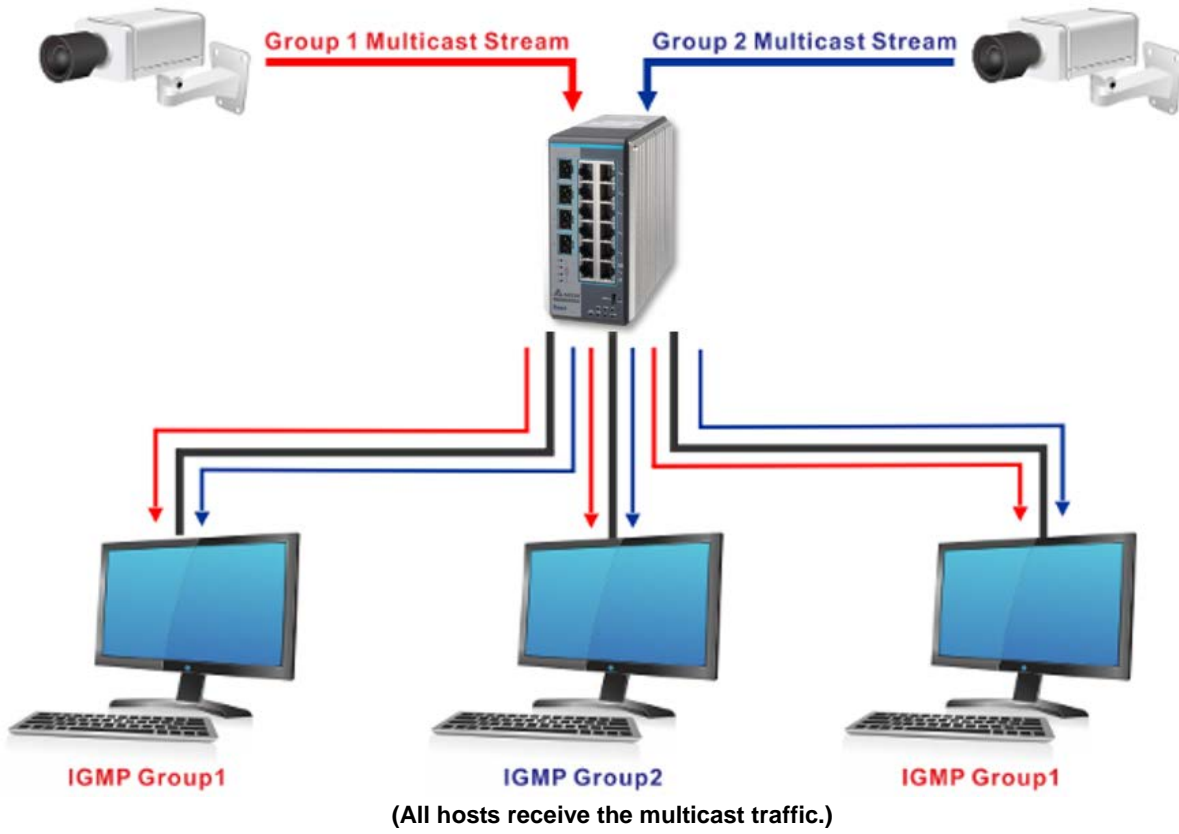
Multicast IP traffic is traffic that is assigned to a host group. Host groups are identified by class D IP addresses, which range from 224.0.0.0 to 239.255.255.255. A multicast IP packet is only sent by one host to multiple hosts. Only those hosts that belong to a specific multicast group will receive 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.

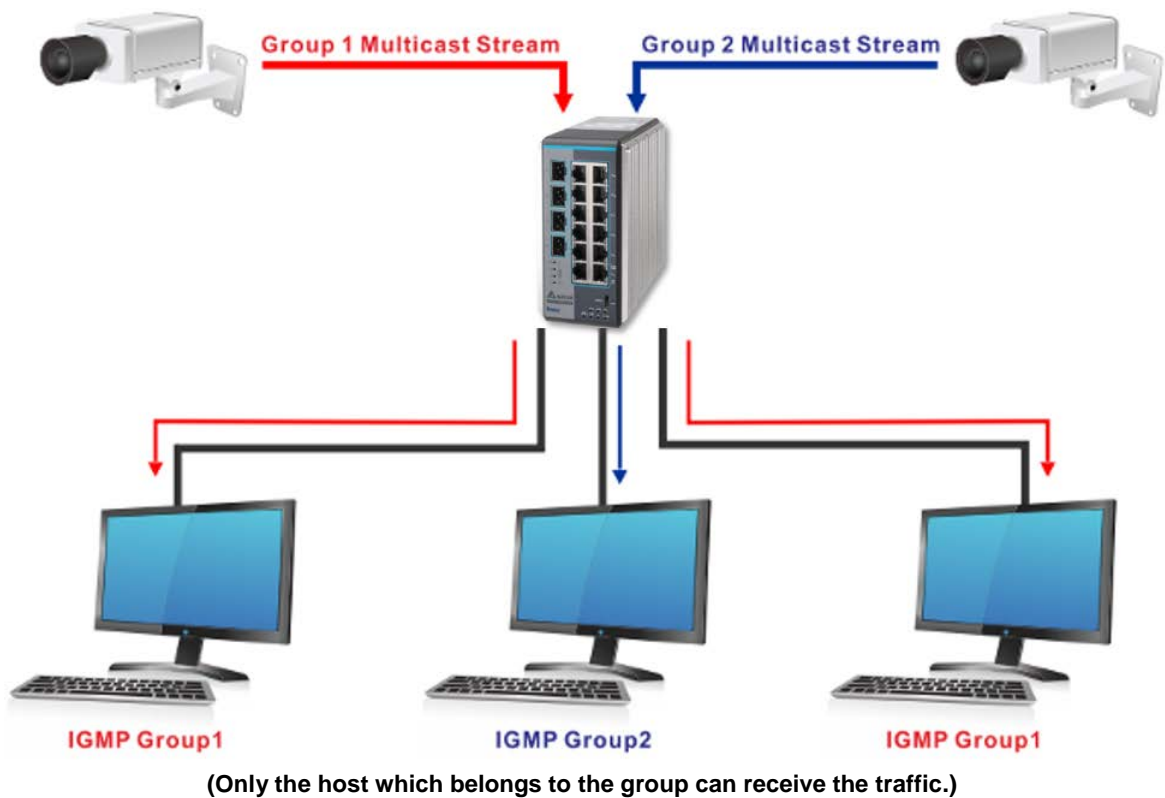
**IMPORTANT:**

**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:**



**Network with Multicast Filtering:**



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

**IGMP Snooping Configuration**

**Admin Mode**  Disable  Enable

**Unknown Multicast Filtering**  Disable  Enable

**Querier Version**

**Querier Interval (secs)**  (60 to 600)

---

**VLAN IDs Enabled for IGMP Snooping**

1,3

#### IGMP Snooping Configuration

Description	Factory default
-------------	-----------------

3

Description	Factory default
<b>Admin Mode</b>	
Specify the status of IGMP Snooping: <ul style="list-style-type: none"> <li><b>Disable:</b> The IGMP Snooping is disabled. The IGMP setting still can be configured, but the settings do not take effect after you have applied them.</li> <li><b>Enable:</b> 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.</li> </ul>	Disable
<b>Unknown Multicast Filtering</b>	
Specify the status of the unknown multicast filtering: <ul style="list-style-type: none"> <li><b>Disable:</b> Unknown multicast traffic is not filtered and is forwarded.</li> <li><b>Enable:</b> Unknown multicast traffic is filtered and dropped.</li> </ul>	Disable
<b>Querier Version</b>	
Specify the IGMP protocol version used in periodic IGMP queries. <ul style="list-style-type: none"> <li><b>IGMP v1:</b> Support the member query and the report function.</li> <li><b>IGMP v2:</b> Support the general query (the same as IGMPv1), the group-specific query, the maximum response time, and the leave group message function.</li> </ul>	2
<b>Querier Interval (secs)</b>	
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**

IGMP VLAN Configuration					
	VLAN ID	Admin Mode	Configured Querier Status	Current Querier Status	Maximum Response Time (tenths of a second)
<input type="checkbox"/>	1				
<input type="button" value="Add"/> <input type="button" value="Delete"/> <input type="button" value="Cancel"/> <input type="button" value="Apply"/>					

**IGMP VLAN Configuration**

Description	Factory default
<b>VLAN ID</b>	
Select a VLAN ID for which you want to create an IGMP snooping configuration.	None
<b>Admin Mode</b>	
Specify the IGMP querying status for VLAN: <ul style="list-style-type: none"> <li><b>Disable:</b> The query can not be forwarded to all multicast groups in VLAN.</li> <li><b>Enable:</b> The query can be forwarded to all multicast groups in VLAN.</li> </ul>	Enable
<b>Configured Querier Status</b>	
Specify the configured querier status: <ul style="list-style-type: none"> <li><b>Disable:</b> 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.</li> <li><b>Enable:</b> The IGMP querying is enabled for the VLAN.</li> </ul>	Disable
<b>Current Querier Status</b>	
The field displays the current querier status in the VLAN.	Disable



Description	Factory default
<b>MAC Address</b>	
Specify the multicast MAC address.	None
<b>Member Ports</b>	
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

### 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 activated on Port Configuration.

#### GMRP Configuration

GMRP Configuration	
<b>GMRP Mode</b>	<input type="radio"/> Disable <input checked="" type="radio"/> Enable

GMRP Port Configuration		
	Interface	Port GMRP Mode
<input type="checkbox"/>		-
<input type="checkbox"/>	0/1	Enable
<input type="checkbox"/>	0/2	Enable
<input type="checkbox"/>	0/3	Enable
<input type="checkbox"/>	0/4	Enable
<input type="checkbox"/>	0/5	Enable
<input type="checkbox"/>	0/6	Enable
<input type="checkbox"/>	0/7	Enable
<input type="checkbox"/>	0/8	Enable
<input type="checkbox"/>	po1	Enable
<input type="checkbox"/>	po2	Enable
<input type="checkbox"/>	po3	Enable

#### GMRP Configuration

Description	Factory default
Specify whether the GMRP mode is enabled. <ul style="list-style-type: none"> <li><b>Disable:</b> The GMRP mode is disabled.</li> <li><b>Enable:</b> The GMRP mode is enabled.</li> </ul>	Enable

**GMRP Port Configuration**

Description	Factory default
<b>Interface</b>	
This field displays the interface number.	<i>interface number</i>
<b>Port GMRP Mode</b>	
Specify whether the GMRP mode is enabled on the interface. <ul style="list-style-type: none"> <li><b>Disable:</b> The GMRP mode on the interface is disabled.</li> <li><b>Enable:</b> The GMRP mode on the interface is enabled.</li> </ul>	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**

Multicast Forwarding Table			
Auto-refresh		<input type="checkbox"/>	
VLAN ID	MAC Address	Type	Forwarding Interfaces
<a href="#">Refresh</a>			

**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

#### 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
<b>Global Trust Mode</b>	
Make a selection from the Global Trust Mode drop-down list that affects all interfaces or aggregation groups: <ul style="list-style-type: none"> <li>● <b>trust dot1p:</b> All interfaces or aggregation groups are configured for the 802.1p marking to classify traffic.</li> <li>● <b>trust ip-dscp:</b> All interfaces and aggregation groups are configured for the IP DSCP packet matching to classify traffic.</li> </ul>	trust dot1p
<b>Global Schedule Scheme</b>	
Make a selection from the Global Schedule Scheme drop-down list that affects all interfaces: <ul style="list-style-type: none"> <li>● <b>sp:</b> 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.</li> <li>● <b>wrr:</b> 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.</li> </ul>	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
<b>Interface Trust Mode</b>	
Make a selection from the Interface Trust Mode drop-down list that affects an individual interfaces or aggregation groups: <ul style="list-style-type: none"> <li>● <b>trust dot1p:</b> The interface or aggregation groups are configured for the 802.1p marking to classify traffic.</li> <li>● <b>trust ip-dscp:</b> The interface and aggregation groups are configured for the IP DSCP packet matching to classify traffic.</li> </ul>	trust dot1p
<b>Interface Schedule Scheme</b>	
Make a selection from the Global Schedule Scheme drop-down list that affects all interfaces: <ul style="list-style-type: none"> <li>● <b>sp:</b> 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.</li> <li>● <b>wrr:</b> 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.</li> </ul>	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.

### Cos Queue Mapping

Interface Selection								
Interface	0/1 ▾							

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

#### 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 Isolation Configuration

This function supports two mode group which are isolated or community. When enabled, the member port in the group cannot forward its ingress 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

Port Isolation Configuration			
	Group Name	Group ID	Group Mode
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	- <input type="text"/>
<input type="button" value="Add"/> <input type="button" value="Delete"/> <input type="button" value="Cancel"/>			

#### Port Isolation Configuration


Description	Factory default
<b>Group Name</b> Specify the Port Isolation group name, and the name string can be up to 24 bytes of non-blank characters.	None
<b>Group ID</b> Specify the Port Isolation group ID, and the range of group is 1 to 24.	None
<b>Group Mode</b> Specify the Port Isolation group mode. <ul style="list-style-type: none"> <li><b>Isolated:</b> The members in the group cannot forward its ingress traffic to any other member ports in the same group.</li> <li><b>Community:</b> Each member port can forward traffic to other members in the same group, but not to member ports in other group.</li> </ul>	None

#### Port Isolation Membership

Description	Factory default
<b>Group ID</b> Display the Group IDs which added in the Port isolation configuration.	Fixed
<b>Group Name</b> Display the Group Name and it's related to the Group ID.	Fixed
<b>Group Mode</b> Display the Group mode and it's related to the Group ID	Fixed
<b>Port Number</b> 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.



**Note:**

We strongly recommend using Recovery time 1000pps for optimal performance of this feature.

#### Storm Control Setting

Global Configuration		
	Recovery Mode	Recovery Level
Broadcast Storm	Enable ▼	1000pps ▼
Multicast Storm	Disable ▼	1000pps ▼
Unicast Storm	Disable ▼	1000pps ▼
<input type="button" value="Refresh"/> <input type="button" value="Apply"/>		

#### Storm Control Setting

Description	Factory default
<b>Port</b>	
The interface number.	<i>interface number</i>
<b>Recovery Mode</b>	
Specify the recovery mode by making a selection from the drop-down list: <ul style="list-style-type: none"> <li>• <b>Disable:</b> The recovery mode is disabled. No traffic is discarded.</li> <li>• <b>Enable:</b> When traffic on the port exceeds the threshold that is configured in the Recovery Level field, the switch discards the traffic.</li> </ul>	Enable
<b>Recovery Level Type</b>	
Specify the link speed recovery level type.	Mbps
<b>Recovery Level</b>	
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

Rate Limiting			
	Port	Egress RateLimit (kbps)	Ingress RateLimit (kbps)
<input type="checkbox"/>		<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	0/1	0	0
<input type="checkbox"/>	0/2	0	0
<input type="checkbox"/>	0/3	0	0
<input type="checkbox"/>	0/4	0	0
<input type="checkbox"/>	0/5	0	0
<input type="checkbox"/>	0/6	0	0
<input type="checkbox"/>	0/7	0	0
<input type="checkbox"/>	0/8	0	0



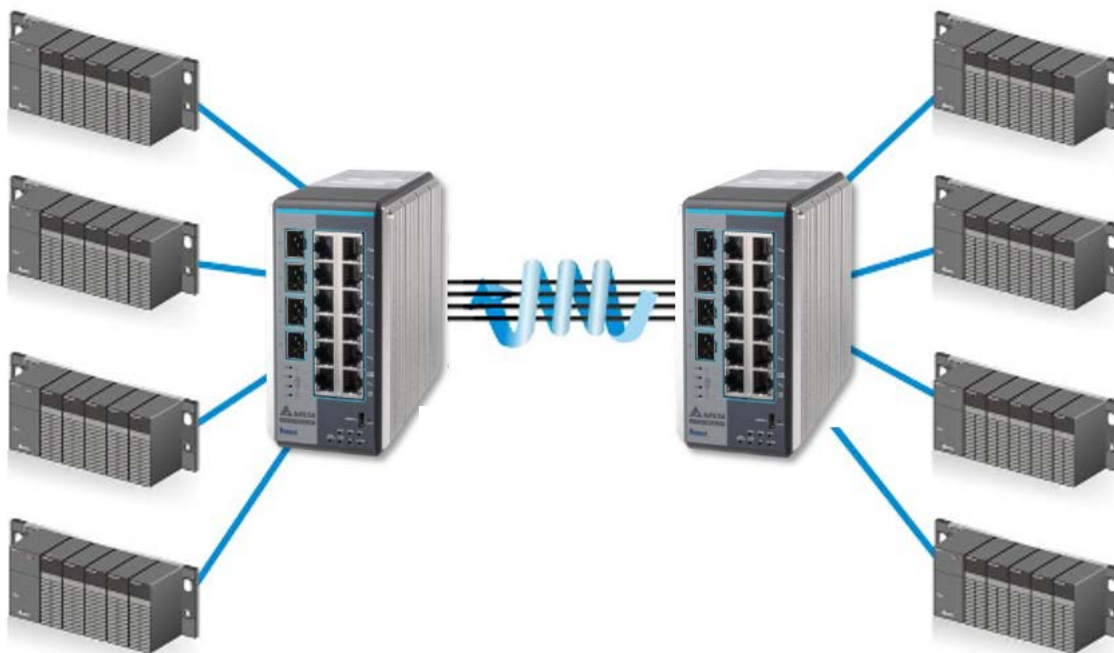
#### Rate Limiting

Description	Factory default
<b>Port</b>	
The interface number	<i>interface number</i>
<b>Egress RateLimit (kbps)</b>	
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
<b>Ingress RateLimit (kbps)</b>	
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

LAG Membership									
LAG ID	Lag 1			Static Mode			Disable		
Port	1	2	3	4	5	6	7	8	
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

#### 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

LAG Information				
LAG ID	Static Mode	Configured Ports	Active Ports	LAG State
lag 1	Disable			DOWN
lag 2	Disable			DOWN
lag 3	Disable			DOWN

Refresh

#### 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

MAC ACL	
Current Number of ACLs	<input type="text" value="1"/>
Maximum ACLs	<input type="text" value="100"/>

MAC ACL Table			
	Name	Rules	Direction
<input type="checkbox"/>	<input type="text"/>		
<input type="checkbox"/>	<a href="#">Marketing</a>	2	In Bound

### 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.



### MAC Rules


Rules	
ACL Name	<input type="text" value="Marketing"/>

Rule Table						
	ID	Action	Match Every	Destination MAC	Destination MAC Mask	EtherType Key
<input type="checkbox"/>	<input type="text"/>	-	-	<input type="text"/>	<input type="text"/>	-
<input type="checkbox"/>	1	Permit	False	00:11:22:aa:bb:cc	ff:ff:ff:ff:ff:ff	
<input type="checkbox"/>	2	Deny	True			

EtherType User Value	Source MAC	Source MAC Mask	VLAN
	00:22:44:22:44:66	ff:ff:ff:ff:ff:ff	2

Rule Table

Description	Factory default
<b>ID</b>	
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
<b>Action</b>	
Specify the action for the rule: <ul style="list-style-type: none"> <li>• <b>Permit:</b> Packets that meet the ACL criteria are forwarded.</li> <li>• <b>Deny:</b> Packets that meet the ACL criteria are dropped.</li> </ul>	None
<b>Match Every</b>	
Specify whether all packets need to match the rule: <ul style="list-style-type: none"> <li>• <b>True:</b> 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.</li> <li>• <b>False:</b> Not all packets need to match the rule. Other rules are also considered.</li> </ul>	True
<b>Destination MAC</b>	
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
<b>Destination MAC Mask</b>	
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. <p> <b>Note:</b> 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).</p>	None
<b>EtherType Key</b>	
Specify the EtherType that needs to be compared with the information in a packet: <b>Appletalk, IBM SNA, IPX, MPLS multicast, MPLS unicast, NetBIOS, Novell, PPPoE, EthernCAT, Profinet-RT, SERCOS III, CC-link IE, Powerlink, User Value.</b> If you select User Value, enter the value in the EtherType User Value field.	None
<b>EtherType User Value</b>	
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
<b>Source MAC</b>	
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
<b>Source MAC Mask</b>	
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. <p> <b>Note:</b> 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,</p>	None

Description	Factory default
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).	
<b>VLAN</b>	
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.  <b>Note:</b> 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**

**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**

MAC Binding Configuration									
ACL ID				Direction					
Sequence Number	0		(1 ~ 4294967295)						
Port	1	2	3	4	5	6	7	8	
LAG	1		2			3			

Interface Binding Status				
Interface	Direction	ACL Type	ACL ID	Seq No

Cancel Apply

**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

Setting	Description
	the interface or interfaces, the ACL replaces the existing ACL that uses the same sequence number.

### 3.10.1.3 MAC Binding Table

The MAC binding information is displayed on this page.

#### MAC Binding Table

MAC Binding Table					
<input type="checkbox"/>	Interface	Direction	ACL Type	ACL ID	Seq No
<input type="checkbox"/>	0/2	In Bound	MAC ACL	Marketing	1
<input type="checkbox"/>	0/5	In Bound	MAC ACL	Marketing	1
<input type="checkbox"/>	po1	In Bound	MAC ACL	Marketing	1

#### 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.

### 3.10.2 ARP ACL

ARP ACL consists of a set of rules that are matched sequentially to compare the packets. With a ARP ACL, you can specify the IP 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.

#### ARP ACL

ARP ACL	
Current Number of ACLs	<input type="text" value="2"/>
Maximum ACLs	<input type="text" value="100"/>

ARP ACL Table			
<input type="checkbox"/>	Name	Rules	Direction
<input type="checkbox"/>	<input type="text"/>		
<input type="checkbox"/>	<a href="#">SSSS</a>	0	

#### ARP 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 ARP ACLs that can be configured (100).

#### ARP 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 ARP ACL.
Direction	The direction of the packet traffic that is affected by the ARP ACL. This is a fixed entry that always shows In Bound; only inbound traffic is subject to the ARP ACL.

### 3.10.2.1 ARP Rules

After creating an ACL name, you can configure the action, match, Sender IP address, Target IP address and Target IP Mask on this page. It can determine whether the packet is forwarded normally or discarded.

3



**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.

#### ARP Rules

**Rules**

ACL Name SSSS ▾

---

**Rule Table**

	ID	Action	Match Every	Opcode Type	Sender IP Address	Sender IP Mask
<input type="checkbox"/>	[ ]	- ▾	- ▾	- ▾	[ ]	[ ]

Target IP Address	Target IP Mask
[ ]	[ ]

#### Rule Table

Description	Factory default
<b>ID</b>	
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
<b>Action</b>	
Specify the action for the rule: <ul style="list-style-type: none"> <li><b>Permit:</b> Packets that meet the ACL criteria are forwarded.</li> <li><b>Deny:</b> Packets that meet the ACL criteria are dropped.</li> </ul>	None
<b>Match Every</b>	
Specify whether all packets need to match the rule: <ul style="list-style-type: none"> <li><b>True:</b> 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.</li> <li><b>False:</b> Not all packets need to match the rule. Other rules are also considered.</li> </ul>	True
<b>Sender IP Address</b>	
Specify the Sender IP Address of the destination device that needs to be compared with the information in a packet. Enter a IP address in the XXX.XXX.XXX.XXX(EX. 192.168.1.1) format.	None
<b>Sender IP Mask</b>	
Specify the Send IP mask that is associated with the Send IP address.	None
<b>Opcode Type</b>	
Specify the EtherType that needs to be compared with the information in a packet: <b>ARP Request, ARP Reply, RARP Reply</b>	None

Description	Factory default
<b>Target IP Address</b>	
Specify the Sender IP Address of the destination device that needs to be compared with the information in a packet. Enter a IP address in the XXX.XXX.XXX.XXX(EX. 192.168.1.1) format.	None
<b>Target IP Mask</b>	
Specify the Send IP mask that is associated with the Send IP address.	None

### 3.10.2.2 ARP Binding Configuration

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

#### ARP Binding Configuration

#### ARP 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 ARP ACL is bound
Direction	The packet filtering direction for the ARP 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 ARP 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.

### 3.10.2.3 ARP Binding Table

The MAC binding information is displayed on this page.

#### ARP Binding Table


ARP Binding Table					
<input type="checkbox"/>	Interface	Direction	ACL Type	ACL ID	Seq No
<input type="checkbox"/>	0/4	In Bound	ARP ACL	ssss	456

#### MAC Binding Table

Setting	Description
Interface	The interface to which the ARP ACL is bound
Direction	The packet filtering direction for the ARP ACL. The only valid direction is Inbound, which means the ARP 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 ARP 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.

## Port Security Configuration

Interface Configuration		
	Port	Port Security
<input type="checkbox"/>		- ▾
<input type="checkbox"/>	0/1	Disable
<input type="checkbox"/>	0/2	Disable
<input type="checkbox"/>	0/3	Disable
<input type="checkbox"/>	0/4	Disable
<input type="checkbox"/>	0/5	Disable
<input type="checkbox"/>	0/6	Disable
<input type="checkbox"/>	0/7	Disable
<input type="checkbox"/>	0/8	Disable

### Interface Configuration

Description	Factory default
<b>Port</b>	
The interface number	<i>interface number</i>
<b>Port Security</b>	
Specify whether the port security is enabled: <ul style="list-style-type: none"> <li><b>Enable:</b> The port security is enabled for the individual interface. The port security also needs to be globally enabled for it to be effective.</li> <li><b>Disable:</b> The port security is disabled for the individual interface. This setting overrides the global port security setting.</li> </ul>	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.

#### Security MAC Address

Security MAC Address Table	
Port List	0/1 ▾
VLAN ID	MAC Address
1	00:11:22:11:22:33

### 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

Add Static Unicast MAC Address	
Vlan Id	- ▾
Destination Port	- ▾
Mac Address	<input type="text"/>

Static Unicast Mac Address Table				
<input type="checkbox"/>	Vlan Id	Mac Address	Destination Port	Status
<input type="checkbox"/>	1	00:11:22:11:22:33	0/1	

### 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.  <b>Note:</b> 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 <b>Permanent</b> 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

IP Source		
<input type="checkbox"/>	IP Address	Subnet Mask
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>

### IP Source

Setting	Description
<b>IP Address</b>	
Enter the source IP address for security.	None
<b>Subnet Mask</b>	
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.

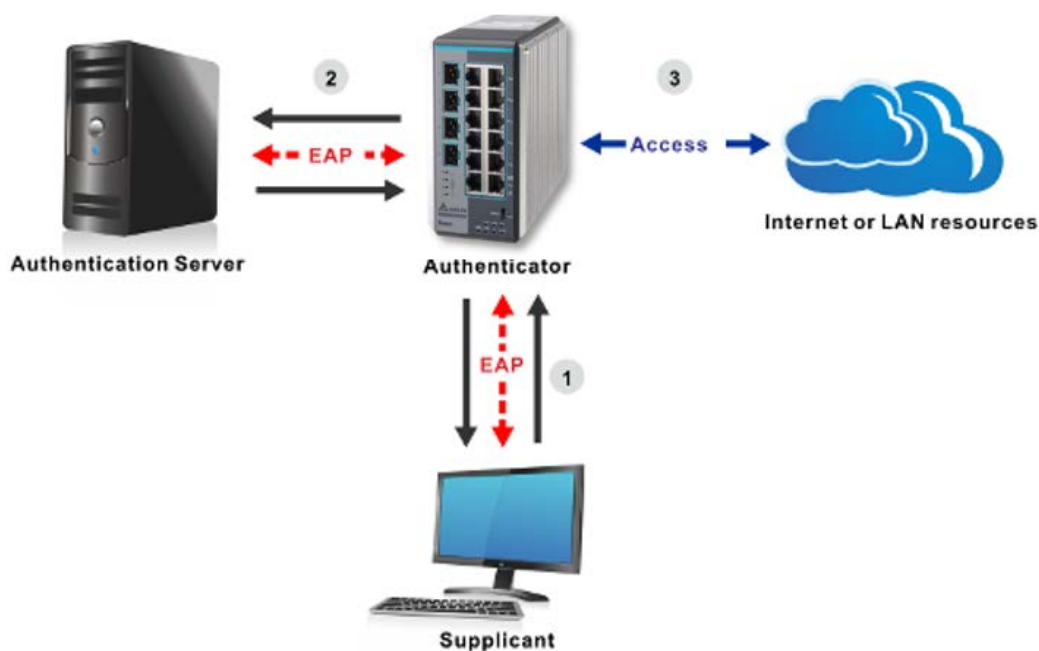
There are three components used to create a port-based authentication mechanism based on 802.1X:

**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

802.1X Configuration	
<b>System Control</b>	<input type="radio"/> Shutdown <input checked="" type="radio"/> Start
<b>802.1X Authentication</b>	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
<b>Authentication Mode</b>	<input checked="" type="radio"/> Local <input type="radio"/> Remote
<b>Remote Authentication Server Type</b>	<input type="radio"/> TACACS+ <input checked="" type="radio"/> RADIUS
<b>Network Access Server ID</b>	<input type="text" value="fsNas1"/>

#### 802.1X Basic Settings

Description	Factory default
<b>System Control</b>	
Specify whether the 802.1X authentication module on the switch is running or shut down. <ul style="list-style-type: none"> <li><b>Shutdown:</b> The 802.1X authentication is shut down. You can not configure or enable the 802.1X authentication.</li> <li><b>Start:</b> The 802.1X authentication is running, and you can configure and enable it.</li> </ul>	Start
<b>802.1X Authentication</b>	
Specify the status of the 802.1X authentication on the switch. <ul style="list-style-type: none"> <li><b>Disable:</b> 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.</li> <li><b>Enable:</b> The 802.1X authentication is enabled. You can configure the 802.1x authentication, and the settings take effect after you have applied them.</li> </ul>	Enable
<b>Authentication Mode</b>	
Specify the 802.1X authentication mode. <ul style="list-style-type: none"> <li><b>Local:</b> 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.</li> <li><b>Remote:</b> 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.</li> </ul>	Local
<b>Remote Authentication Server Type</b>	
If you select the Remote mode of Authentication Mode, specify whether a RADIUS or TACACS+ server should be used. <ul style="list-style-type: none"> <li><b>TACACS+:</b> The user ID and the password are authenticated through a TACACS+ server.</li> <li><b>RADIUS:</b> The user ID and the password are authenticated through a RADIUS server.</li> </ul>	RADIUS
<b>Network Access Server ID</b>	
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
<input type="checkbox"/>		-	-		-
<input type="checkbox"/>	0/1	ForceAuthorized	Disabled	3600	Disabled
<input type="checkbox"/>	0/2	ForceAuthorized	Disabled	3600	Disabled
<input type="checkbox"/>	0/3	ForceAuthorized	Disabled	3600	Disabled
<input type="checkbox"/>	0/4	ForceAuthorized	Disabled	3600	Disabled
<input type="checkbox"/>	0/5	ForceAuthorized	Disabled	3600	Disabled
<input type="checkbox"/>	0/6	ForceAuthorized	Disabled	3600	Disabled
<input type="checkbox"/>	0/7	ForceAuthorized	Disabled	3600	Disabled
<input type="checkbox"/>	0/8	ForceAuthorized	Disabled	3600	Disabled

Apply Cancel Refresh

**Port Authentication**

Description	Factory default
<b>Port</b>	
This field displays the port number.	Port number
<b>Control Mode</b>	
Specify the control mode for the port authorization. The control mode is active only if the link status of the interface is up. <ul style="list-style-type: none"> <li><b>ForceUnauthorized:</b> Places the interface in the unauthorized state. The switch can not provide authentication services for a client through the interface.</li> <li><b>Auto:</b> After any supplicant completes the authentication successfully on the interface, others can access the network service through the same interface without the authentication.</li> <li><b>ForceAuthorized:</b> Places the interface in the authorized state. The interface sends and receives normal traffic without the client port-based authentication.</li> </ul>	ForceAuthorized
<b>Periodic Reauthentication</b>	
Specify whether the supplicant is periodically reauthenticated for the interface: <ul style="list-style-type: none"> <li><b>Enabled:</b> The supplicant is reauthenticated according to the reauthentication period.</li> <li><b>Disabled:</b> The supplicant is not reauthenticated.</li> </ul>	Disable
<b>Reauthentication Period</b>	
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
<b>EAPOL Packets Flood</b>	
Specify whether the EAPOL packet flood mode is enabled for the interface: <ul style="list-style-type: none"> <li><b>Enabled:</b> 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.</li> <li><b>Disabled:</b> The EAPOL packet flood mode is disabled.</li> </ul>	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**

Add Local Authentication Server					
	User Name	Password	Permission	Auth-TimeOut (secs)	Port List
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	- ▾	<input type="text"/>	<input type="text"/>

**Local Authentication Server Configuration**

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

3

Description	Factory default
<ul style="list-style-type: none"> <li><b>Allow:</b> Allows the user access to the interface.</li> <li><b>Deny:</b> Denies the user access to the interface.</li> </ul>	
<b>Auth-TimeOut (secs)</b>	
<p>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 reauthentication period that is configured for the individual interface.</p> <p> <b>Note:</b> 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.</p> <p> <b>Note:</b> 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.</p>	None
<b>Port List</b>	
<p>Specify the interfaces from which the authentication needs to be obtained. Leave the field blank to include all interfaces.</p> <p> <b>Note:</b> The range of port list is dependant on what type of DVS managed switch you used.</p>	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**

Port Summary					
	Port	Control Mode	Reauthentication Enabled	Port Status	User Name
<input type="checkbox"/>		-	-	-	
<input type="checkbox"/>	0/1	ForceAuthorized	Disabled	Unauthorized	No User
<input type="checkbox"/>	0/2	ForceAuthorized	Disabled	Unauthorized	No User
<input type="checkbox"/>	0/3	ForceAuthorized	Disabled	Unauthorized	No User
<input type="checkbox"/>	0/4	ForceAuthorized	Disabled	Unauthorized	No User
<input type="checkbox"/>	0/5	ForceAuthorized	Disabled	Authorized	No User
<input type="checkbox"/>	0/6	ForceAuthorized	Disabled	Authorized	No User
<input type="checkbox"/>	0/7	ForceAuthorized	Disabled	Unauthorized	No User
<input type="checkbox"/>	0/8	ForceAuthorized	Disabled	Unauthorized	No User

**Port Summary**

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

### EAP Statistics

This page allows you to view the EAP statistics.

#### EAP Statistics

EAP Statistics									
Port	EAPOL								
	Frames Received	Frames Transmitted	Start Frames Received	Logoff Frames Received	Last Frame Version	Last Frame Source	Invalid Frames Received	Length Error Frames Received	
0/1	0	0	0	0	0	00:00:00:00:00:00	0	0	
0/2	0	0	0	0	0	00:00:00:00:00:00	0	0	
0/3	0	0	0	0	0	00:00:00:00:00:00	0	0	
0/4	0	0	0	0	0	00:00:00:00:00:00	0	0	
0/5	0	0	0	0	0	00:00:00:00:00:00	0	0	
0/6	0	0	0	0	0	00:00:00:00:00:00	0	0	
0/7	0	0	0	0	0	00:00:00:00:00:00	0	0	
0/8	0	0	0	0	0	00:00:00:00:00:00	0	0	



EAP			
Response/ID Frames Received	Response Frames Received	Request/ID Frames Transmitted	Request Frames Transmitted
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

**EAP Statistics**

Item	Description
Port	The interface number
<b>EAPOL (Extensible Authentication Protocol over LAN)</b>	
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
<b>EAP (Extensible Authentication Protocol)</b>	
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**

Manage Users				
	User Name	Edit Password	Password	Confirm Password
<input type="checkbox"/>	admin	Disabled	*****	*****

**User Management**

Description	Factory default
-------------	-----------------

<b>User Name</b>	
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
<b>Edit Password</b>	
Select Enabled, and then edit the password.	None
<b>Password</b>	
Enter a password. Passwords are 1–20 alphanumeric characters in length and are case sensitive. The password is displayed as eight asterisks (*).	None
<b>Confirm Password</b>	
Enter the same password that you entered in the <b>Password</b> 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

Add RADIUS Server							
Server ID	Address Type	Server Address	Shared Secret	Response Time (secs)	Retry Count	Port	
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="button" value="Add"/> <input type="button" value="Cancel"/> <input type="button" value="Delete"/> <input type="button" value="Apply"/>							

#### RADIUS Server Configuration

Description	Factory default
<b>Server ID</b>	
The identifier of the server	None
<b>Address Type</b>	
Specify a type of address for the RADIUS server: <ul style="list-style-type: none"> <li><b>IPv4:</b> The RADIUS server has an IPv4 address.</li> <li><b>DNS:</b> The RADIUS server has a DNS host name.</li> </ul>	None
<b>Server Address</b>	
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
<b>Shared secret</b>	
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
<b>Response Time (secs)</b>	
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
<b>Retry Count</b>	
Enter the maximum number of times an authentication request is retransmitted. Enter a number in the range of 1 to 254.	3
<b>Port</b>	
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

RADIUS Server Statistics								
Index	RADIUS Server	UDP Port Number	Round Trip Time	Access Requests	Access Retransmissions	Access Accepts	Access Rejects	Access Challenge
1	192.168.1.10	17	0	0	0	0	0	0

[Refresh](#)

Malformed Access Responses	Bad Authenticators	Pending Requests	Timeouts	Unknown Types	Packets Dropped
0	0	0	0	0	0

#### 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

TACACS+ Server Configuration						
	Address Type (*)	IP Address (*)	Shared Secret(*)	Single Connection	Server Port	Server Timeout (secs)
<input type="checkbox"/>	-			-		
<input type="checkbox"/>	IPv4	192.168.1.10	password	Yes	5432	10

#### TACACS+ Server Configuration

Description	Factory default
<b>Address Type (*)</b> Specify a type of address for the TACACS+ server. <ul style="list-style-type: none"> <li><b>IPv4:</b> The TACACS+ server has an IPv4 address.</li> <li><b>DNS:</b> The TACACS+ server has a DNS host name.</li> </ul>	None
<b>IP Address (*)</b> 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
<b>Shared Secret (*)</b> 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
<b>Single Connection</b> Specify a type of connection: <ul style="list-style-type: none"> <li><b>Yes:</b> Allows only a single TCP connection with the TACACS server.</li> <li><b>No:</b> Allows multiple TCP connections with the TACACS server.</li> </ul>	No
<b>Server Port</b> 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
<b>Server Timeout (secs)</b> 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

TACACS+ AS Configuration		
ActiveServer Address Type	ActiveServer Address	Retransmit
-		

#### TACACS+ AS Configuration

Description	Factory default
<b>Active Server Address Type</b> Specify a type of address for the TACACS+ AS.	None

<ul style="list-style-type: none"> <li>• <b>IPv4:</b> The TACACS+ AS server has an IPv4 address.</li> <li>• <b>DNS:</b> The TACACS+ AS server has a DNS host name.</li> </ul>	
<b>Active Server Address</b>	
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
<b>Retransmit</b>	
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

**Authentication Configuration**

Login Authentication Mode Local

#### Login Authentication

Description	Factory default
<b>Login Authentication Mode</b>	
Specify the login authentication method: <ul style="list-style-type: none"> <li>• <b>Local:</b> 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.</li> <li>• <b>RADIUS:</b> The user ID and the password are authenticated through a RADIUS server.</li> <li>• <b>TACACS+:</b> The user ID and the password are authenticated through a TACACS+ server.</li> </ul>	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

Login User Sessions			
ID	Type	User	Peer-Address
w1	http	admin	192.168.1.202

#### Login User Sessions

Item	Description
ID	The unique session identifier
Type	The session types: <ul style="list-style-type: none"> <li>• console</li> <li>• telnet</li> <li>• ssh</li> <li>• http</li> <li>• https</li> </ul>

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

**Denial of Service Configuration**

**Denial of Service SIP=DIP**       Disable       Enable

**Denial of Service First Fragment**       Disable       Enable

**Denial of Service Min TCP Hdr Size**       (0 to 255)

**Denial of Service TCP Fragment**       Disable       Enable

**Denial of Service TCP Flag**       Disable       Enable

**Denial of Service L4 Port**       Disable       Enable

**Denial of Service ICMP**       Disable       Enable


**Denial of Service Max ICMP Size**       (0 to 1023)

#### Denial of Service Configuration

Description	Factory default
<p><b>Denial of Service SIP=DIP</b></p> <p>Select one of the following radio buttons:</p> <ul style="list-style-type: none"> <li><b>Disable:</b> This is the default setting.</li> <li><b>Enable:</b> Packets that have a source IP (SIP) address equal to the destination IP (DIP) address are dropped.</li> </ul>	Disable
<p><b>Denial of Service TCP Flag</b></p> <p>Select one of the following radio buttons:</p> <ul style="list-style-type: none"> <li><b>Disable:</b> This is the default setting.</li> <li><b>Enable:</b> All of the following packets are dropped: <ul style="list-style-type: none"> <li>- Packets that have a TCP flag SYN set and a TCP source port with a number lower than 1024</li> <li>- Packets that have TCP control flags set to 0 and the TCP sequence number set to 0</li> <li>- Packets that have TCP flags FIN, URG, and PSH set and TCP sequence number set to 0</li> <li>- Packets that have both the TCP flags SYN and FIN set</li> </ul> </li> </ul>	Disable
<p><b>Denial of Service L4 Port</b></p> <p>Select one of the following radio buttons:</p> <ul style="list-style-type: none"> <li><b>Disable:</b> This is the default setting.</li> <li><b>Enable:</b> 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.</li> </ul>	Disable

## 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.

#### MAC Address Table

**Address Aging Time**

Address Aging Timeout (seconds)  \* Sec. (10-1000000)

**MAC Address Table**

Search By --

Total MAC Addresses 1

Auto-refresh

VLAN ID	MAC Address	Port	status
1	98:e7:f4:4f:8f:db	0/1	Learned

#### Address Aging Time

Description	Factory default
<b>Address Aging Timeout (seconds)</b>	
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: <ul style="list-style-type: none"> <li><b>Invalid:</b> The MAC address is invalid. Normally, invalid MAC addresses are deleted, so this is an error condition.</li> <li><b>Self:</b> The MAC address is the address of a physical interface of the switch.</li> <li><b>Learned:</b> The MAC address was learned through incoming traffic and is being used.</li> <li><b>Static:</b> The MAC address was manually added and can not be relearned.</li> <li><b>Other:</b> The MAC address does not fall into one of the other</li> </ul>

Item	Description
	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												
<input type="checkbox"/>	Port	Status	Temperature		Voltage		Bias		Tx Power		Rx Power	
			Current	Range	Current	Range	Current	Range	Current	Range	Current	Range
<input type="checkbox"/>	0/7	Not Present	unknown	unknown	unknown	unknown	unknown	unknown	unknown	unknown	unknown	unknown
<input type="checkbox"/>	0/8	Not Present	unknown	unknown	unknown	unknown	unknown	unknown	unknown	unknown	unknown	unknown




#### 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 transission are fully compatible with Delta managed switches ONLY. If users are intending to use SFP modules of 3<sup>rd</sup>-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.

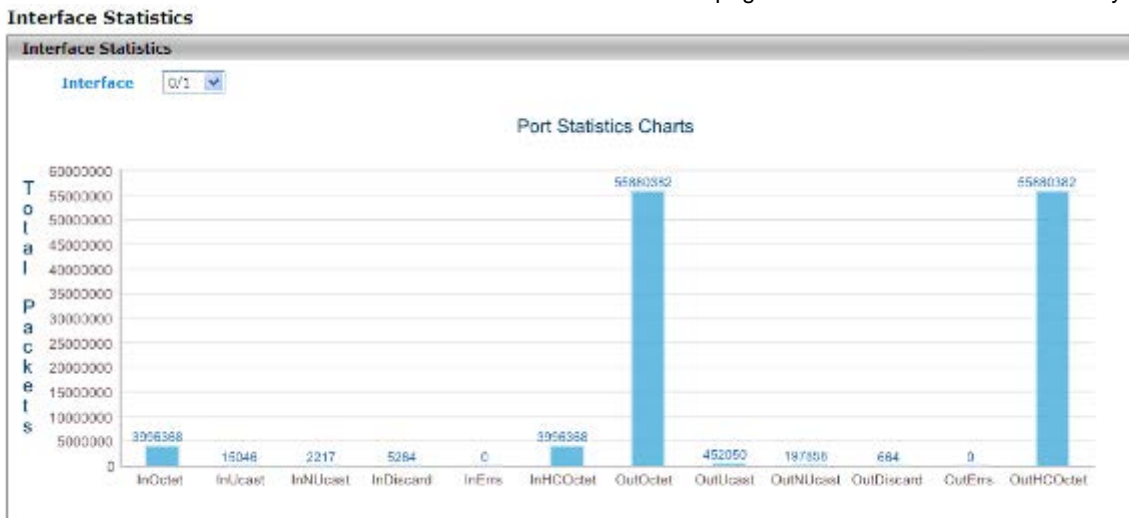
#### System CPU Status

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 %	

### 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**

ARP Table		
IP Address	Port	MAC Address
192.168.1.13	0/1	98:e7:f4:4f:8f:db

[Refresh](#)

**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: <ul style="list-style-type: none"> <li>• <b>Invalid:</b> The MAC address is invalid. Normally, invalid MAC addresses are deleted, so this is an error condition.</li> <li>• <b>Self:</b> The MAC address is the address of a physical interface of the switch.</li> <li>• <b>Learned:</b> The MAC address was learned through incoming traffic and is being used.</li> <li>• <b>Static:</b> The MAC address was manually added and can not be relearned.</li> <li>• <b>Other:</b> The MAC address does not fall into one of the other categories.</li> </ul>

### 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.

##### RMON Basic Settings

Basic Settings	
RMON Status	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
<input type="button" value="Cancel"/> <input type="button" value="Apply"/>	

#### 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





RMON Alarm Configuration						
	Index	Interval	Interface	Variable	Sample Type	Rising Threshold
	<input type="text" value="*"/>	<input type="text" value="*"/>	<input type="text" value="*"/>	<input type="text" value="*"/>	<input type="text" value="*"/>	<input type="text" value="*"/>
<input type="checkbox"/>	1	50	0/1	etherStatsBroadcastPkts	Absolute Value	30
<input type="checkbox"/>	2	100	0/1	etherStatsOversizePkts	Absolute Value	20

Note :1.Before setting the threshold values, corresponding ethernet index and events has to be created.  
2.Falling Threshold value has to be lesser than Rising Threshold value.

Falling Threshold	Rising Event Index	Falling Event Index	Owner
<input type="text" value="*"/>	<input type="text" value="*"/>	<input type="text" value="*"/>	<input type="text" value="*"/>
20	1	1	Delta
15	2	2	Delta

##### RMON Alarm Configuration

Description	Factory default
<b>Index</b>	
Enter an index that uniquely identifies the entry in the RMON Alarm Configuration	None

Description	Factory default
table. Enter a number between 1 and 65535.	
<b>Interval</b>	
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
<b>Interface</b>	
Specify the interface number.	None
<b>Variable</b>	
Specify the SNMP event that you want to sample.	None
<b>Sample Type</b>	
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: <ul style="list-style-type: none"> <li>• <b>Absolute Value:</b> The value of the variable is compared directly with the thresholds at the end of the sampling interval.</li> <li>• <b>Delta Value:</b> 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.</li> </ul>	None
<b>Rising Threshold</b>	
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. <p> <b>Note:</b> The rising threshold value needs to be greater than the falling threshold value.</p>	None
<b>Falling Threshold</b>	
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. <p> <b>Note:</b> The falling threshold value needs to be less than the rising threshold value.</p>	None
<b>Rising Event Index</b>	
Specify the index of the event that needs to be raised when a rising threshold is crossed. The value is between 1 and 65535. <p> <b>Note:</b> The drop-down list is associated with the <b>RMON Event Configuration table</b>. If there is no corresponding entry in the <b>RMON Event Configuration table</b>, no association can exist.</p>	None
<b>Falling Event Index</b>	
Specify the index of the event that needs to be raised when a falling threshold is crossed. <p> <b>Note:</b> The drop-down list is associated with the <b>RMON Event Configuration table</b>. If there is no corresponding entry in the <b>RMON Event Configuration table</b>, no association can exist.</p>	None
<b>Owner</b>	
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**

RMON Event Configuration						
Index	Description	Type	Community	Owner	Last Time Sent	
<input type="checkbox"/> *	<input type="text"/>	-				
<input type="checkbox"/> 1	Broadcast	Log and Trap	SNMPTrap	Delta	0 day 0 hr 55 min 30 sec	
<input type="checkbox"/> 2	Packets	Log		David	0 day 0 hr 56 min 20 sec	

**RMON Event Configuration**

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

RMON Event Log			
Event	Log No.	Log Time	Description
<input type="button" value="Refresh"/>			

**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

History Control Configuration					
	Index	Data Source	Buckets Requested	Interval	Owner
<input type="checkbox"/>	1 *	0/1 *	50	1800	Delta

#### History Control Configuration

Description	Factory default
<b>Index</b>	
Enter an index that uniquely identifies the entry in the History Control Configuration table. Enter a number between 1 and 65535.	None
<b>Data Source</b>	
Specify a source interface.	None
<b>Buckets Requested</b>	
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
<b>Interval</b>	
Specify the period in seconds between two successive pollings to collect the statistics. Enter a number between 1 to 3600 seconds.	1800
<b>Owner</b>	
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

Ethernet Statistics	
Interface	0/7 ▼

Ethernet Statistics	
Drop Events	0
Packets	58856
Broadcast Packets	3177
Multicast Packets	746
CRC Errors	0
Under Size Packets	0
Over Size Packtes	0
Fragments	8
Jabbers	0
Collisions	68
Packets 64 Octets	20863
Packets 65-127 Octets	11775
Packets 128-255 Octets	4237
Packets 256-511 Octets	5506
Packets 512-1023 Octets	3061
Packets 1024-1518 Octets	13414

[Refresh](#)

## 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 integral number of octets (FCS error) or a bad FCS with a non integral number

3

Item	Description
	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

Item	Description
	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.

#### Show System Logs

Message Log					
Index	Severity	Date	Time	Model Name	Logs
1	<134>	1970-01-01	04:37:05	DVS-108W02-2SFP	MSR configuration changed
2	<134>	1970-01-01	04:37:06	DVS-108W02-2SFP	CLI User admin logged out
3	<134>	1970-01-01	04:37:11	DVS-108W02-2SFP	CLI User admin logged in

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 <b>Logs Configuration</b> .
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

System Logs Configuration	
Logging on	<input type="button" value="Enable"/> ▾
Service timestamps	<input type="button" value="Enable"/> ▾
Logging console	<input type="button" value="Enable"/> ▾
Logging mail	<input type="button" value="Disable"/> ▾
Logging auto-save-logs	<input type="button" value="Enable"/> ▾
Logging buffered	<input type="text" value="50"/>
Logging time-range(mins)	<input type="text" value="60"/>
Logging manual-save-logs	<input type="button" value="ManualSave"/>
Severity	<input type="button" value="critical"/> ▾
Logging filesize	<input type="text" value="10240"/>

## System Logs Configuration

Description	Factory default
<b>Logging on</b>	
Specify whether the logging is enabled or disabled: <ul style="list-style-type: none"> <li>• <b>Enable:</b> The logging is enabled.</li> <li>• <b>Disable:</b> 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.</li> </ul>	Enable
<b>Service timestamps</b>	
Specify whether or not a time stamp is added to log messages: <ul style="list-style-type: none"> <li>• <b>Enable:</b> A time stamp is added.</li> <li>• <b>Disable:</b> A time stamp is not added.</li> </ul>	Enable
<b>Logging console</b>	
Specify whether the logging over the console port is enabled or disabled: <ul style="list-style-type: none"> <li>• <b>Enable:</b> The logging over the console port is enabled.</li> <li>• <b>Disable:</b> The logging over the console port is disabled.</li> </ul>	Enable
<b>Logging mail</b>	
Specify whether log messages can be sent to a specified email address: <ul style="list-style-type: none"> <li>• <b>Enable:</b> The sending of log messages to a specified email is enabled.</li> <li>• <b>Disable:</b> The sending of log messages to a specified email is disabled.</li> </ul>	Disable
<b>Logging auto-save-logs</b>	
<ul style="list-style-type: none"> <li>• Specify whether log messages can be saved in a flash memory automatically:</li> <li>• <b>Enable:</b> Log messages can be saved in a flash memory automatically. The saving time depends on the Logging time-range setting.</li> <li>• <b>Disable:</b> Log messages can not be saved in a flash memory automatically.</li> </ul>	Enable
<b>Logging buffered</b>	
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
<b>Logging time-range (min)</b>	
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
<b>Logging manual-save-logs</b>	
Click the button to save logs in a flash memory manually.	None
<b>Severity</b>	
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: <ul style="list-style-type: none"> <li>• <b>emergency:</b> The highest warning level (level 0). An emergency message is saved if the switch is down or not functioning correctly.</li> <li>• <b>alert:</b> 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.</li> <li>• <b>critical:</b> 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</li> </ul>	critical

3

Description	Factory default
functional. <ul style="list-style-type: none"> <li><b>error:</b> The level that indicates that a device error has occurred (level 3), such as an interface going offline</li> <li><b>warning:</b> The lowest level of a device warning (level 4).</li> <li><b>notice:</b> Normal but significant conditions (level 5). Provides the network administrators with the switch information.</li> <li><b>Informational:</b> Provides the switch information (level 6).</li> <li><b>debug:</b> Provides the detailed information about the switch (level 7). This level generates a lot of messages.</li> </ul>	
<b>Logging filesize</b>	
Specify the size of the system file in which the log files are saved. Enter a file size between 1024 and 102400 bytes.  <b>Note:</b> 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

Forward Files Table					
	Fwd Severity	Fwd Address Type	Server IP Address	Fwd Port	Fwd TransType
<input type="checkbox"/>	-	-			-
<input type="checkbox"/>	informational	IPv4	192.168.1.5	2	SYSLOG_TCP

#### Syslog Fwd Table

Description	Factory default
<b>Fwd Severity</b>	
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
<b>Fwd Address Type</b>	
Specify a type of server address and enter the address or the host name in the Server IP Address field: <ul style="list-style-type: none"> <li>IPv4: The syslog server has an IPv4 address.</li> <li>IPv6: The syslog server has an IPv6 address.</li> <li>DNS: The syslog server has a DNS host name.</li> </ul>	None
<b>Server IP Address</b>	
Enter the IP address or the host name of the syslog server.  <b>Note:</b> For an IPv6 address, enter the address in the xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx format.	None
<b>Fwd Port</b>	
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	514

Description	Factory default
sent.	
<b>Fwd TransType</b>	
Specify whether log messages are sent as UDP or TCP messages: <ul style="list-style-type: none"> <li>• <b>SYSLOG_UDP</b>: Log messages are sent as UDP messages.</li> <li>• <b>SYSLOG_TCP</b>: Log messages are sent as TCP messages.</li> </ul>	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

**Email Server Settings**

Mail Server IP/Name:

the Esmtip Authentication Choice

Account Name:

Change Account Password

Old Password:

New Password:

Retype Password:

1st Email Address:

2nd Email Address:

3rd Email Address:

4th Email Address:

#### Email Server Configuration

Description	Factory default
<b>Mail Server IP / Name</b>	
Enter the IP address of the mail server.	None
<b>The Esmtip Authentication Choice</b>	
Specify whether the mail server needs the authentication. If the box is selected, please enter the account name of the email.	None
<b>Change Account Password</b>	
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
<b>Email Address</b>	
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							
<input checked="" type="checkbox"/>	Switch Cold Start	<input checked="" type="checkbox"/>	Switch Warm Start	<input checked="" type="checkbox"/>	Power Transition(Off->On)	<input checked="" type="checkbox"/>	Power Transition(On->Off)
<input checked="" type="checkbox"/>	DI-ON	<input checked="" type="checkbox"/>	DI-OFF	<input checked="" type="checkbox"/>	Authentication Failure	<input checked="" type="checkbox"/>	Dot1d Bridge New Root
<input checked="" type="checkbox"/>	Dot1d Bridge Topology Changed	<input checked="" type="checkbox"/>	LLDP Remote Tables Change	<input checked="" type="checkbox"/>	Configuration Changed	<input checked="" type="checkbox"/>	Firmware Update
<input checked="" type="checkbox"/>	IP Changed	<input checked="" type="checkbox"/>	Password Changed	<input checked="" type="checkbox"/>	Redundancy		

Port Events											
Port	Link-ON	Link-OFF	DDM Failure					Overload	Threshold(%)	Duration(s)	Loopback-Detection
			Temp Alarm	Voltage	Bias	TX Power	RX Power				
0/1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	1	1	<input checked="" type="checkbox"/>
0/2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	1	1	<input checked="" type="checkbox"/>
0/3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	1	1	<input checked="" type="checkbox"/>
0/4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	1	1	<input checked="" type="checkbox"/>
0/5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	1	1	<input checked="" type="checkbox"/>
0/6	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	1	1	<input checked="" type="checkbox"/>
0/7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	1	1	<input checked="" type="checkbox"/>
0/8	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	1	1	<input checked="" type="checkbox"/>

**System Events**

Description	Factory default
<b>Switch Cold Start</b>	
Specify whether to send an alarm email when switch cold starts.	Checked
<b>Switch Warm Start</b>	
Specify whether to send an alarm email when switch warm starts.	Checked
<b>Power Transition (Off-&gt;On)</b>	
Specify whether to send an alarm email when there is a transition in power from Off to On.	Checked
<b>Power Transition (On-&gt;Off)</b>	
Specify whether to send an alarm email when there is a transition in power from On to Off.	Checked
<b>DI-ON</b>	
Specify whether to send an alarm email when DI is On.	Checked
<b>DI-OFF</b>	
Specify whether to send an alarm email when DI is Off.	Checked
<b>Authentication Failure</b>	
Specify whether to send an alarm email when there is authentication failure.	Checked
<b>Dot1d Bridge New Root</b>	
Specify whether to send an alarm email when a new node is added to the 802.1d network.	Checked
<b>Dot1d Bridge Topology Changed</b>	
Specify whether to send an alarm email when the 802.1d bridge topology is changed.	Checked
<b>LLDP Remote Tables Change</b>	
Specify whether to send an alarm email when the LLDP remote table is changed.	Checked
<b>Configuration-Changed</b>	
Specify whether to send an alarm email when the configuration is changed.	Checked
<b>Firmware Update</b>	
Specify whether to send an alarm email when the firmware has been updated.	Checked
<b>IP Changed</b>	
Specify whether to send alarm email when the IP address has changed.	Checked

Description	Factory default
<b>Password Changed</b>	
Specify whether to send alarm email when the password has changed.	Checked
<b>Redundancy</b>	
Specify whether to send alarm email when the redundancy has changed.	Checked

**Port Events**

Description	Factory default
<b>Port</b>	
This field displays the interface number.	<i>interface number</i>
<b>Link-ON</b>	
Specify whether to send an alarm email when the Link is ON.	Checked
<b>Link-OFF</b>	
Specify whether to send an alarm email when the Link is OFF.	Checked
<b>DDM Failure</b>	
Specify whether to send an alarm email when the DDM failure event is detected.	Checked
<b>Overload</b>	
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
<b>Loopback-Detection</b>	
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	
LLDP Status	Enable ▾
Transmit Interval (8 to 32768)	30
Holdtime Multiplier	4
Reinitialization Delay	2
TX Delay	2
Notification Interval	5

3

#### LLDP Basic Settings

Description	Factory default
<b>LLDP Status</b>	
Specify the status of LLDP on the switch: <ul style="list-style-type: none"> <li><b>Enable:</b> LLDP is enabled. You can configure LLDP, and the settings take effect after you have applied them.</li> <li><b>Disable:</b> LLDP is disabled. You can still configure LLDP, but the settings do not take effect after you have applied them.</li> </ul>	Enable
<b>Transmit Interval (8 to 32768)</b>	
Enter the interval in seconds to transmit the LLDP frames. Enter a number in the range of 8 to 32768 seconds.	30
<b>Holdtime Multiplier</b>	
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
<b>Reinitialization Delay</b>	
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
<b>TX Delay</b>	
It is used to delay the tx_relay time and the value is fixed at 2 seconds.	2
<b>Notification Interval</b>	
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

Interface Settings				
	Port	Link Status	Admin Status	Notification Status
<input type="checkbox"/>			- ▾	- ▾
<input type="checkbox"/>	0/1	Down	TX and RX	Disabled
<input type="checkbox"/>	0/2	Down	TX and RX	Disabled
<input type="checkbox"/>	0/3	Up	TX and RX	Disabled
<input type="checkbox"/>	0/4	Down	TX and RX	Disabled
<input type="checkbox"/>	0/5	Down	TX and RX	Disabled
<input type="checkbox"/>	0/6	Down	TX and RX	Disabled
<input type="checkbox"/>	0/7	Up	TX and RX	Disabled
<input type="checkbox"/>	0/8	Up	TX and RX	Disabled

### Interface Settings

Description	Factory default
<b>Port</b>	
This field displays the interface number.	<i>interface number</i>
<b>Link Status</b>	
This field displays the status of the interface link.	Up or Down
<b>Admin Status</b>	
Specify the status and the direction of the interface: <ul style="list-style-type: none"> <li><b>TX:</b> The interface processes outgoing traffic only.</li> <li><b>RX:</b> The interface processes incoming traffic only.</li> <li><b>TX and RX:</b> The interface processes both incoming and outgoing traffic.</li> <li><b>Disabled:</b> The interface is disabled.</li> </ul>	TX and RX
<b>Notification Status</b>	
Specify the notification status: <ul style="list-style-type: none"> <li><b>Enabled:</b> Notifications are sent.</li> <li><b>Disabled:</b> Notifications are not sent.</li> </ul>	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 Options

LLDP TLV Options							
	Port	Port Description	System Name	System Description	System Capability	MAC PHY Config	Management Address
<input type="checkbox"/>		- ▾	- ▾	- ▾	- ▾	- ▾	- ▾
<input type="checkbox"/>	0/1	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled
<input type="checkbox"/>	0/2	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled
<input type="checkbox"/>	0/3	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled
<input type="checkbox"/>	0/4	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled
<input type="checkbox"/>	0/5	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled
<input type="checkbox"/>	0/6	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled
<input type="checkbox"/>	0/7	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled
<input type="checkbox"/>	0/8	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled

### LLDP TLV Option

Item	Description
Port	Specify the interface number.
Port Description	Specify whether to send the options in the LLDP frames. <ul style="list-style-type: none"> <li>• <b>Enable:</b> The information is transmitted. This is the default setting.</li> <li>• <b>Disable:</b> The information is not transmitted.</li> </ul>
System Name	
System Description	
System Capability	
MAC PHY Config	
Management Address	

### 3.13.1.4 LLDP Local Information

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

#### LLDP Local Information

**LLDP Local Information**

**Interface** 0/1 ▾

**LLDP Local Information**

**Chassis ID Subtype**      MAC Address

**Chassis ID**              00:18:23:01:20:61

**System Name**

**System Description**      DVS108W02 - 8 Port with 2 SFP.

**System Capability Supported**      Bridge ;

**System Capability Enabled**      Bridge ;

**Port ID Subtype**            Interface Alias

**Port ID**                    Slot0/1

**Port Description**           Slot 0: Port 1: Fastethernet-Level

**Enabled Tx TLVs**            Port Description, System Name, System Description, System Capability, Management Address, Mac Phy

**Management Addresses**

**SubType**                    IPv4

**Address**                    192.168.1.142

**Extended 802.3 TLV Info**

**--MAC PHY Configuration & Status--**

**Auto-Neg Support & Status**      Not Supported ,Disabled

**Advertised Capability Bits**      0000

**Operational MAU Type**        0

Refresh

#### 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 <b>System Information</b> page

Item	Description	
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, 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.

#### LLDP Neighbor Information

**LLDP Neighbor Information**

**Show Neighbor** All ▾

**Interface** - ▾

---

**LLDP Neighbor Statistics**

Chassis ID	Local Interface	Hold Time	Capability	Port ID
00:18:23:01:20:58	0/8	120	B	Slot0/8
00:18:23:01:1f:14	0/7	120	B	Slot0/7
Total Entries Displayed :		2		

Refresh
Clear

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	
Show Neighbor	Detail ▾
Interface	0/7 ▾

### LLDP Neighbor Information

Description	Factory default
<b>Show Neighbor</b>	
<ul style="list-style-type: none"> <li><b>All:</b> The information is for all interfaces.</li> <li><b>Detail:</b> The information is for one single interface.</li> </ul>	All
<b>Interface</b>	
Specify one interface for information.	None

LLDP Neighbor Detail Statistics	
<b>Chassis ID Subtype</b>	MAC Address
<b>Chassis ID</b>	00:18:23:01:1f:14
<b>Port ID Subtype</b>	Interface Alias
<b>Port ID</b>	Slot0/7
<b>Port Description</b>	Slot 0: Port 7: Gigabit-Level
<b>Local Interface</b>	0/7
<b>Time Remaining</b>	102
<b>System Name</b>	Not Advertised
<b>System Description</b>	DVS108W02 - 8 Port with 2 SFP.
<b>System Capability Supported</b>	Bridge ;
<b>System Capability Enabled</b>	Bridge ;
<b>Management Addresses</b>	
<b>If ID</b>	12
<b>SubType</b>	IPv4
<b>Address</b>	192.168.1.152
<b>OID</b>	1 3 6 1 2 1 2 2 1 1
<b>Extended 802.1 Tlvs:</b>	
<b>Port VLAN ID</b>	Not Advertised
<b>Port &amp; Protocol VLAN ID:</b>	Not Advertised
<b>VLAN Name:</b>	Not Advertised
<b>Extended 802.3 TLV:</b>	
<b>MAC PHY Configuration:</b>	
<b>Auto-Neg Support</b>	Supported
<b>Auto-Neg Status</b>	Enabled
<b>Advertised Capability Bits</b>	6c01
	10base-T(HD)
	10base-T(FD)
	100base-TX(HD)
	100base-TX(FD)
	1000base-T(FD)
<b>Operational MAU Type</b>	30
<b>Link Aggregation:</b>	Not Advertised
<b>Maximum Frame Size</b>	Not Advertised

**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	
<b>Total Frames Out</b>	10866
<b>Total Entries Aged</b>	1
<b>Total Frames In</b>	10825
<b>Total Frames Received In Error</b>	0
<b>Total Frames Discarded</b>	0
<b>Total TLVs Unrecognized</b>	0
<b>Total TLVs Discarded</b>	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**

LLDP MED Global Configuration		
<b>Fast Start Repeat Count</b>	<input type="text" value="3"/>	(1 to 10 Times)
<b>Device Class</b>	Network Connectivity	

**Cancel Apply**

**LLDP MED Global Configuration**

Description	Factory default
<b>Fast Start Repeat Count</b>	
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
<b>Device Class</b>	
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: <ul style="list-style-type: none"> <li>• <b>Class I:</b> Generic (for example, an IP communication controller)</li> <li>• <b>Class II:</b> Media (for example, a conference bridge)</li> <li>• <b>Class III:</b> Communication (for example, an IP phone)</li> <li>• <b>Network Connectivity (device):</b> Generally a LAN switch or a router, an IEEE 802.1 bridge, or an IEEE 802.11 wireless access point</li> </ul>	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**

LLDP-MED Interface Configuration				
	Interface	MED Status	Notification Status	MED Capabilities
<input type="checkbox"/>		- ▾	- ▾	- ▾
<input type="checkbox"/>	0/1	Disable	Disable	none
<input type="checkbox"/>	0/2	Disable	Disable	none
<input type="checkbox"/>	0/3	Disable	Disable	none
<input type="checkbox"/>	0/4	Disable	Disable	none
<input type="checkbox"/>	0/5	Disable	Disable	none
<input type="checkbox"/>	0/6	Disable	Disable	none
<input type="checkbox"/>	0/7	Disable	Disable	none
<input type="checkbox"/>	0/8	Disable	Disable	none

**LLDP-MED Interface Configuration**

Description	Factory default
<b>Interface</b>	
This field displays the interface number or the port channel number.	<i>interface number</i>
<b>Med Status</b>	
Specify the MED status: <ul style="list-style-type: none"> <li>• <b>Enabled:</b> MED is enabled for the interface.</li> <li>• <b>Disabled:</b> MED is disabled for the interface.</li> </ul>	Disabled
<b>Notification Status</b>	
Specify the notification status: <ul style="list-style-type: none"> <li>• <b>Enabled:</b> MED notifications are sent for the interface.</li> <li>• <b>Disabled:</b> MED notifications are not sent for the interface.</li> </ul>	Disabled
<b>MED Capabilities</b>	
Specify the MED TLVs which are transmitted: <ul style="list-style-type: none"> <li>• <b>none:</b> No MED TLVs are transmitted.</li> </ul>	None

Description	Factory default
<ul style="list-style-type: none"> <li>• <b>network-policy:</b> The network policy information is transmitted.</li> <li>• <b>capabilities:</b> The capabilities information is transmitted.</li> <li>• <b>both:</b> Both the network policy information and the capabilities information are transmitted.</li> </ul>	

### 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

**Multiple Port Mirroring**


**Monitored Port**     0/1    0/2    0/3    0/4    0/5    0/6    0/7    0/8

**Session Mode**     ▼

**Watch Direction**     ▼

**Mirror Port**     ▼

#### Multiple Port Mirroring

Description	Factory default
<b>Monitored Port</b>	
Specify the monitored port or ports for the monitoring.	Unchecked
<b>Session Mode</b>	
Specify whether the port mirroring session mode is enabled: <ul style="list-style-type: none"> <li>• <b>Enable:</b> The port mirroring is enabled. The setting applies to all interfaces.</li> <li>• <b>Disable:</b> The port mirroring is disabled. The setting applies to all interfaces.</li> </ul>  <p><b>Note:</b> When you configure the session mode for an individual interface, it is applied to all interfaces. You can select <b>Enable</b> 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 <b>Delete</b> to remove the port mirroring configuration for the interface.</p>	None
<b>Watch Direction</b>	
Specify the direction in which the port mirroring occurs: <ul style="list-style-type: none"> <li>• <b>Tx and Rx:</b> Both outgoing traffic and incoming traffic are mirrored.</li> <li>• <b>Tx Only:</b> Only outgoing traffic is mirrored.</li> <li>• <b>Rx Only:</b> Only incoming traffic is mirrored.</li> </ul>	None
<b>Mirror Port</b>	
Specify the port which is the mirror port.	None


Status Table				
	Monitored Port	Mirror Port	Session Mode	Direction
<input type="checkbox"/>	0/1		Disable	
<input type="checkbox"/>	0/2		Disable	
<input type="checkbox"/>	0/3		Disable	
<input type="checkbox"/>	0/4		Disable	
<input type="checkbox"/>	0/5		Disable	
<input type="checkbox"/>	0/6		Disable	
<input type="checkbox"/>	0/7		Disable	
<input type="checkbox"/>	0/8		Disable	

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. <ul style="list-style-type: none"> <li>• <b>Enable:</b> The port mirroring is enabled.</li> <li>• <b>Disable:</b> The port mirroring is disabled.</li> </ul>
Direction	The direction of the port mirroring. <ul style="list-style-type: none"> <li>• <b>Tx and Rx:</b> Both outgoing traffic and incoming traffic are mirrored.</li> <li>• <b>Tx Only:</b> Only outgoing traffic is mirrored.</li> <li>• <b>Rx Only:</b> Only incoming traffic is mirrored.</li> </ul>

### 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.**

#### 3.14.1 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.

## Relay Alarm I Events Settings

System Events					
Power1	Disabled ▾		Power2	Disabled ▾	
DI1	Disabled ▾		DI2	Disabled ▾	
Redundancy	Disabled ▾				

Port Events					
	Port	Link	Traffic-Overload	Traffic-Threshold(%)	Traffic-Duration(s)
<input type="checkbox"/>		- ▾	- ▾		
<input type="checkbox"/>	0/1	Disabled	Disabled	1	1
<input type="checkbox"/>	0/2	Disabled	Disabled	1	1
<input type="checkbox"/>	0/3	Disabled	Disabled	1	1
<input type="checkbox"/>	0/4	Disabled	Disabled	1	1
<input type="checkbox"/>	0/5	Disabled	Disabled	1	1
<input type="checkbox"/>	0/6	Disabled	Disabled	1	1
<input type="checkbox"/>	0/7	Disabled	Disabled	1	1
<input type="checkbox"/>	0/8	Disabled	Disabled	1	1

## Relay Alarm II Events Settings

System Events					
Power1	Disabled ▾		Power2	Disabled ▾	
DI1	Disabled ▾		DI2	Disabled ▾	
Redundancy	Disabled ▾				


  

Port Events					
	Port	Link	Traffic-Overload	Traffic-Threshold(%)	Traffic-Duration(s)
<input type="checkbox"/>		- ▾	- ▾		
<input type="checkbox"/>	0/1	Disabled	Disabled	1	1
<input type="checkbox"/>	0/2	Disabled	Disabled	1	1
<input type="checkbox"/>	0/3	Disabled	Disabled	1	1
<input type="checkbox"/>	0/4	Disabled	Disabled	1	1
<input type="checkbox"/>	0/5	Disabled	Disabled	1	1
<input type="checkbox"/>	0/6	Disabled	Disabled	1	1
<input type="checkbox"/>	0/7	Disabled	Disabled	1	1
<input type="checkbox"/>	0/8	Disabled	Disabled	1	1

### System Events

Description	Factory default
<b>Power 1</b> Specify the power event status: <ul style="list-style-type: none"> <li>• <b>Disable:</b> Disable Power 1 to trigger relay alarm 1 or 2.</li> <li>• <b>On to Off:</b> When the status of Power 1 changes from On to Off, relay alarm 1 or 2 is triggered.</li> <li>• <b>Off to On:</b> When the status of Power 1 changes from Off to On, relay alarm</li> </ul>	Disable

3

Description	Factory default
1 or 2 is triggered.	
<b>Power 2</b>	
Specify the power event status: <ul style="list-style-type: none"> <li>• <b>Disable:</b> Disable Power 2 to trigger relay alarm 1 or 2.</li> <li>• <b>On to Off:</b> When the status of Power 2 changes from On to Off, relay alarm 1 or 2 is triggered.</li> <li>• <b>Off to On:</b> When the status of Power 2 changes from Off to On, relay alarm 1 or 2 is triggered.</li> </ul>	Disable
<b>DI 1</b>	
Specify the DI event status: <ul style="list-style-type: none"> <li>• <b>Disable:</b> Disable DI 1 to trigger relay alarm 1.</li> <li>• <b>On to Off:</b> When the status of DI 1 changes from On to Off, relay alarm 1 is triggered.</li> <li>• <b>Off to On:</b> When the status of DI 1 changes from Off to On, relay alarm 1 is triggered.</li> </ul>	Disable
<b>DI 2</b>	
Specify the DI event status: <ul style="list-style-type: none"> <li>• <b>Disable:</b> Disable DI 2 to trigger relay alarm 1 or 2.</li> <li>• <b>On to Off:</b> When the status of DI 2 changes from On to Off, relay alarm 1 or 2 is triggered.</li> <li>• <b>Off to On:</b> When the status of DI 2 changes from Off to On, relay alarm 1 or 2 is triggered.</li> </ul>	Disable
<b>Redundancy</b>	
Specify the redundancy event status: <ul style="list-style-type: none"> <li>• <b>Disable:</b> Disable ONE RING, ONE CHAIN, or ONE COUPLING event to trigger relay alarm 1 or 2.</li> <li>• <b>Enable:</b> Enable ONE RING, ONE CHAIN, or ONE COUPLING event to trigger relay alarm 1 or 2.</li> </ul>  <b>Note:</b> If the hardware version is too old, this function will not be activated.	Disable

**Port Events**

Description	Factory default
<b>Link</b>	
Specify the port link event status: <ul style="list-style-type: none"> <li>• <b>Disable:</b> Disable the port link to trigger relay alarm 1 or 2.</li> <li>• <b>On to Off:</b> When the status of the port link changes from On to Off, relay alarm 1 is triggered.</li> <li>• <b>Off to On:</b> When the status of the port link changes from Off to On, relay alarm 1 is triggered.</li> </ul>	Disable
<b>Traffic-Overload</b>	
Specify the traffic overload event status. The traffic overload is used to monitor the port's <b>ingress</b> traffic flow. It has two parameters: threshold and duration. <ul style="list-style-type: none"> <li>• <b>Disable:</b> Disable traffic-overload to trigger relay alarm 1 or 2.</li> <li>• <b>Enabled:</b> Enable traffic-overload to trigger relay alarm 1 or 2.</li> </ul>	Disable
<b>Traffic-Threshold (%)</b>	
Specify the traffic speed threshold percentage of the port. Enter the value between 1 and 100.	1
<b>Traffic-Duration (s)</b>	
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**

Current Alarm List		
Index	Event	Relay
1	Port 3 Link up	1
2	Port 6 traffic overload	1


**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.

**Copy**

Copy		
Source Image	<input type="radio"/> Image1	<input type="radio"/> Image2
Destination Image	<input type="radio"/> Image1	<input type="radio"/> Image2
Transfer Status		
<input type="button" value="Cancel"/> <input type="button" value="Apply"/>		

### 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.

#### Dual Image Configuration

Dual Image Configuration					
	Image Name	Active Image	Next Active Image	Description (1-256)	Version
<input type="checkbox"/>			- ▾		
<input type="checkbox"/>	image1	True	True		1.18
<input type="checkbox"/>	image2	False	False		



**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.

#### Save Configuration

**Save Configuration**

Saving all applied changes will cause all changes to configuration panels that were applied, but not saved, to be saved, thus retaining their new values across a system reboot.

#### 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.

#### Auto-Save Configuration

**Auto-Save Configuration**

Auto-Save Mode       Disable       Enable

#### 3.16.3 Configuration Copy

This feature support user to backup the configuration file.

#### Configuration Copy

**Configuration Copy**

Source File Name       Startup Configuration       Backup Configuration

Destination File Name       Startup Configuration       Backup Configuration

**Note:**

Before you use the function, create 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

Restore Configuration	
Restore Option	<input type="radio"/> No Restore <input checked="" type="radio"/> Startup 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. <b>Note:</b> Please make sure that you have saved the settings on the switch before restart the switch.

### 3.16.5 Erase

#### Erase File

Erase File	
File Type	Startup Configuration <input type="button" value="v"/>

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.

#### Device Reboot

Device Reboot	
Check this box and click APPLY below to reboot	<input type="checkbox"/>

### 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.

#### Factory Default Settings

**Factory Default Settings**

Check this box and click **APPLY** below to reset

**Apply**

## 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

**Details**

**IP Address/Hostname**

**Count**  (1 to 10)

**Interval(secs)**  (1 to 100)

**Datagram Size**  (0 to 2080)

**Ping**

Reply Received From :192.168.1.30, TimeTaken : 10 msec

--- 192.168.1.30 Ping Statistics ---

1 Packets Transmitted, 1 Packets Received, 0% Packets Loss

**Apply**

#### Ping

Description	Factory default
<b>IP Address/Hostname</b> Specify the IP address or the host name that you want to ping. Enter an IPv4 address or a host name.	None
<b>Count</b> Specify the number of echo requests to be sent. Enter a number between 1 and 10.	3
<b>Interval(secs)</b> 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
<b>Datagram Size</b> 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> msec  
--- 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

**Details**

Ping Global ▾

IPv6 Address/Host Name

Datagram Size  (48 to 2048)

Ping

#### Ping IPv6

Description	Factory default
<b>Ping</b>	
Specify a type of IP address. <ul style="list-style-type: none"> <li>• <b>Global:</b> The global IP address</li> <li>• <b>Link Local:</b> The link local IP address. They are assigned with the fe80::/64 prefix.</li> </ul>	Global
<b>IPv6 Address/Host Name</b>	
Specify the IPv6 address or the host name that you want to ping. Enter an address in the xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx format.	None
<b>Datagram Size</b>	
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

TraceRoute	
IP Address/Hostname	<input type="text" value="172.16.0.1"/>

Results	
Results	<pre> 1      172.16.155.254    100 ms  110 ms  100 ms 2      172.31.4.250    100 ms  110 ms  100 ms 3      10.17.192.33    110 ms  100 ms  100 ms 4      10.17.192.82   110 ms  100 ms  110 ms 5      172.31.1.253   100 ms  100 ms  110 ms 6      172.16.0.1     100 ms  110 ms  100 ms                     </pre>

#### 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

TraceRoute IPv6	
IPv6 Address/Host Name	<input type="text"/>

Results	
Results	<div style="border: 1px solid gray; height: 100px;"></div>

#### 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:xxxx: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

<b>4.1</b>	<b>Starting the Configuration</b> .....	<b>4-3</b>
<b>4.2</b>	<b>Device</b> .....	<b>4-4</b>
4.2.1	Search .....	4-4
4.2.2	Live Viewer .....	4-4
<b>4.3</b>	<b>Settings</b> .....	<b>4-4</b>
4.3.1	Device Configuration .....	4-5
4.3.2	Configuration Web Page.....	4-6
<b>4.4</b>	<b>Tools</b> .....	<b>4-7</b>
4.4.1	IP Setting .....	4-7
4.4.2	Ping Test.....	4-7
4.4.3	Parameter Import .....	4-8
4.4.4	Parameter Export.....	4-8
4.4.5	Device Reboot .....	4-9
4.4.6	Update Firmware .....	4-9
<b>4.5</b>	<b>Help</b> .....	<b>4-10</b>

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-G106W02-2GF
- DVS-G112W02-4GF
- DVS-G116W02-4GF
- 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
- DVS-G928W01
- IFD9506
- IFD9507
- RTU-EN01
- DVPEN01-SL
- DVP12SE
- DVP-FEN01
- DVPSCM12-SL
- DVPSCM52-SL
- ASDA-M
- CMC-MOD01
- CMC-EIP01

More models are coming soon.

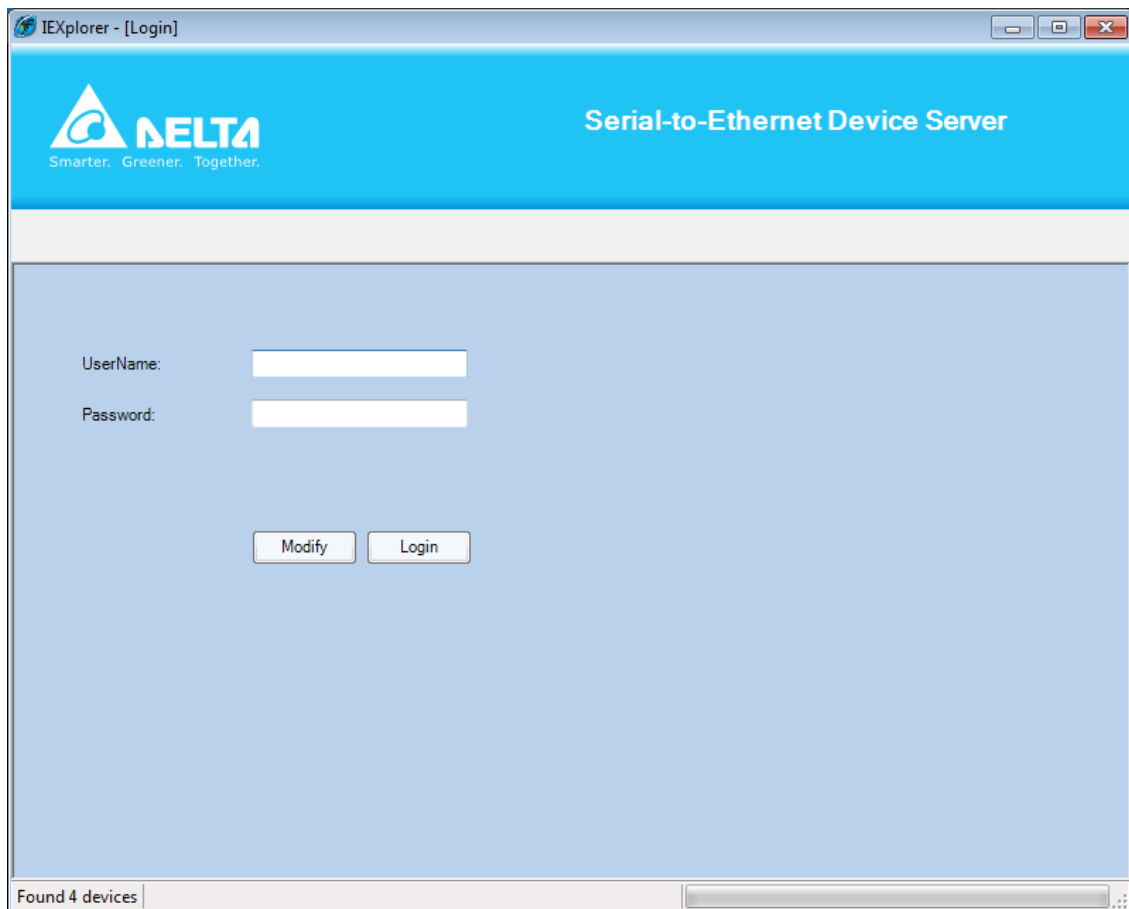
Compatible OS: Windows XP SP2, Windows 7 (32/64 bits), Windows 8(64 bits)or Windows 10 (32/64 bits)

## 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.



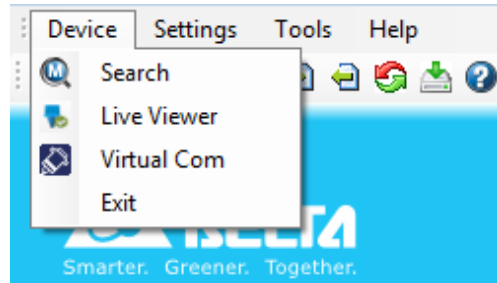
1. After double-clicking the icon, you can see the IEXplorer interface shown below:



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 (\*).

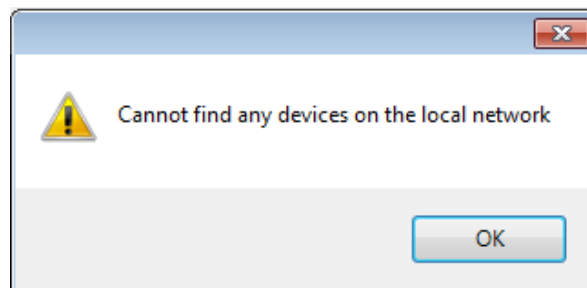
## 4.2 Device

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

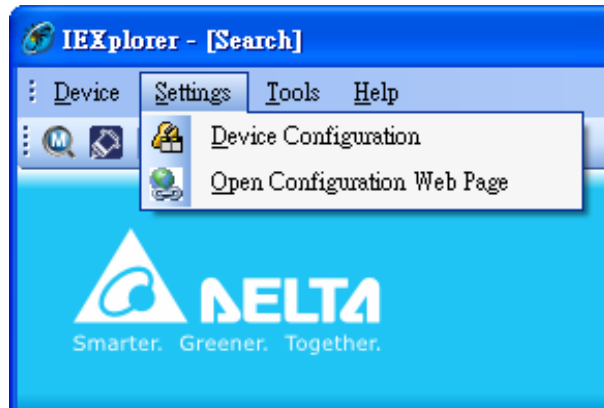
### 4.2.2 Live Viewer

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.

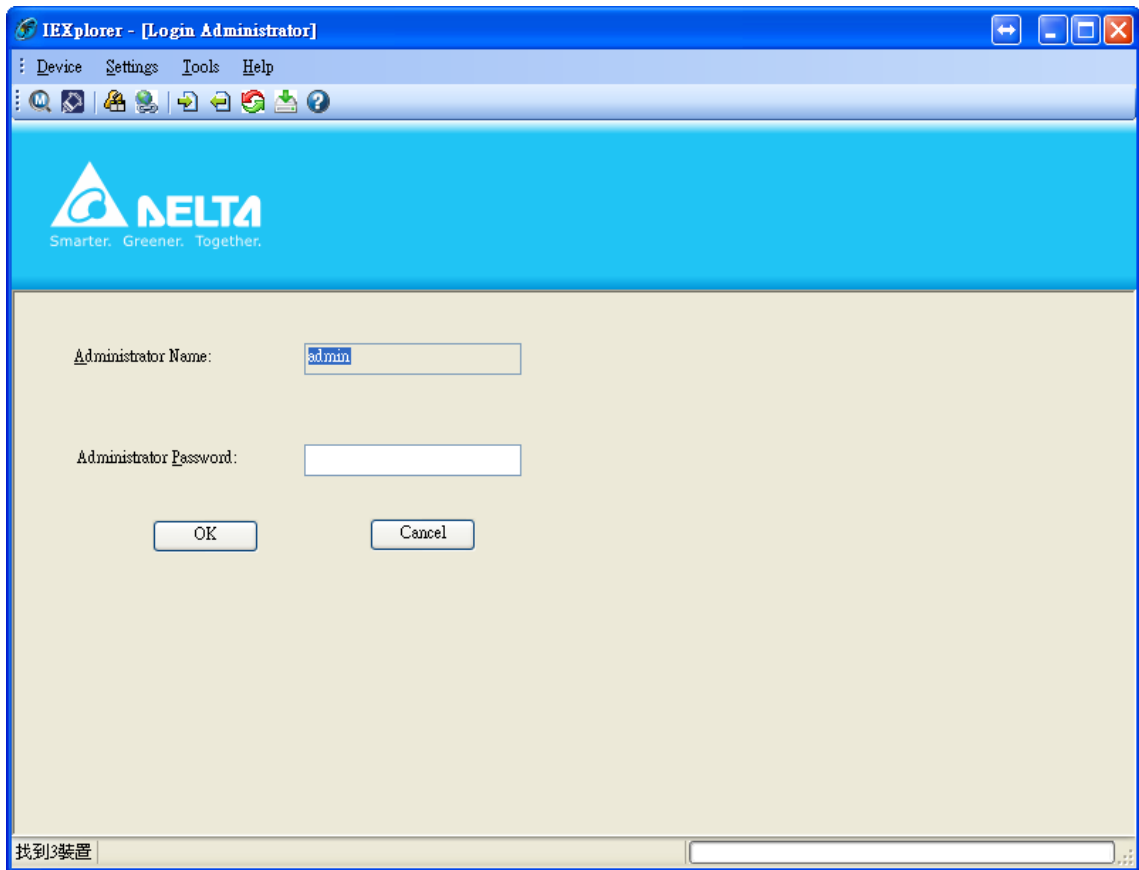
## 4.3 Settings

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.

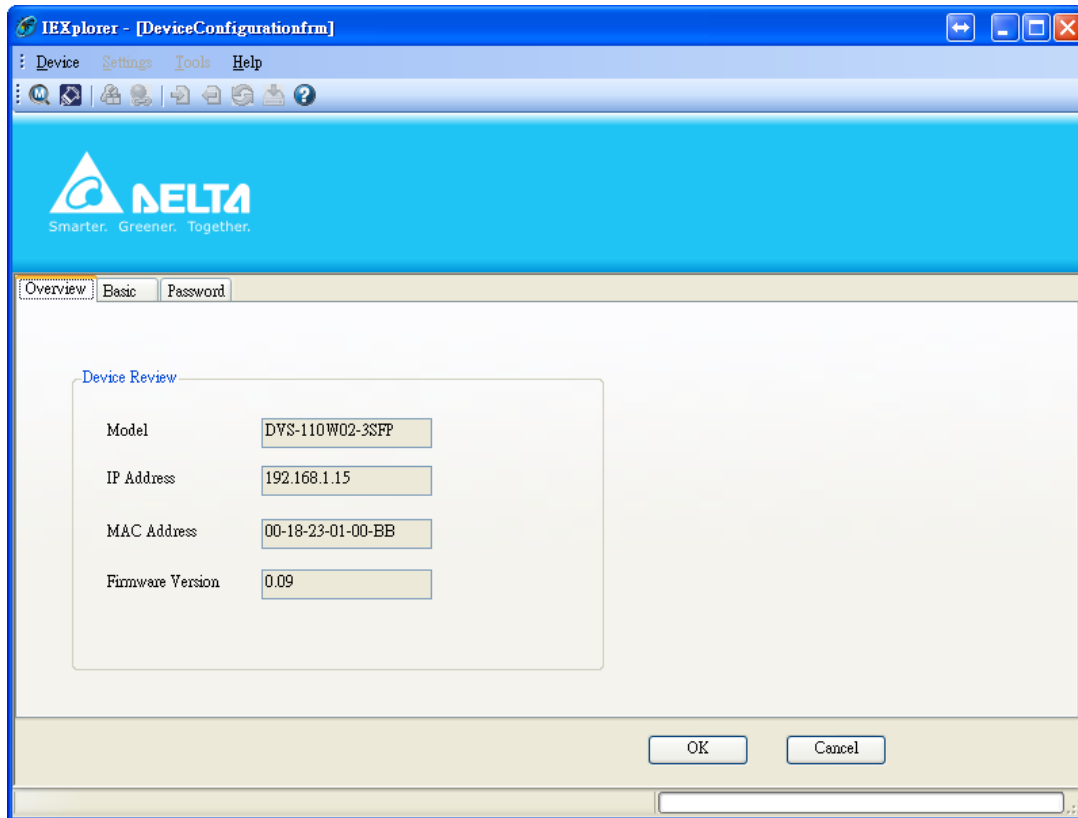


### 4.3.1 Device Configuration

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:

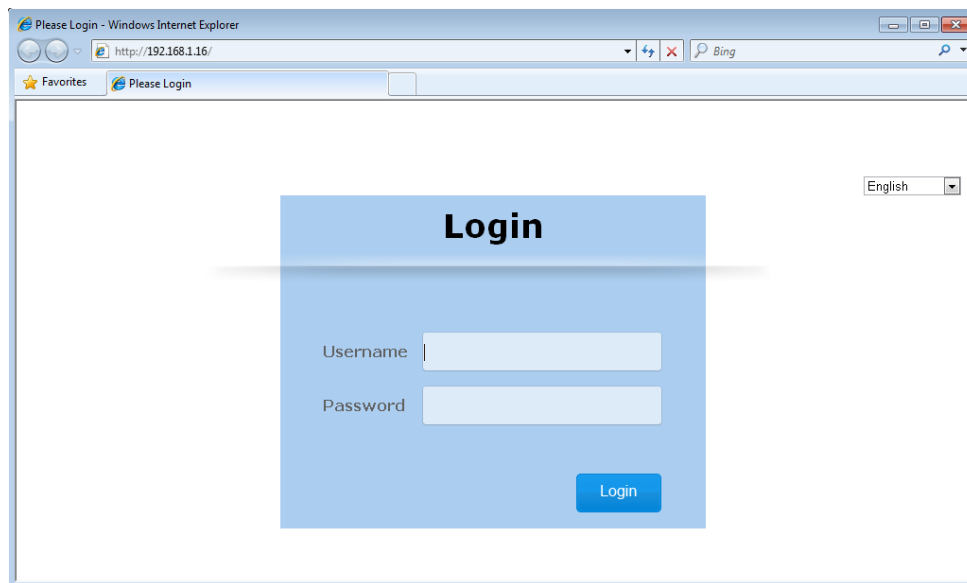


4

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.

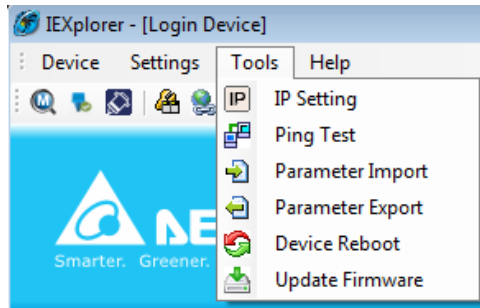


**Note:**

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.

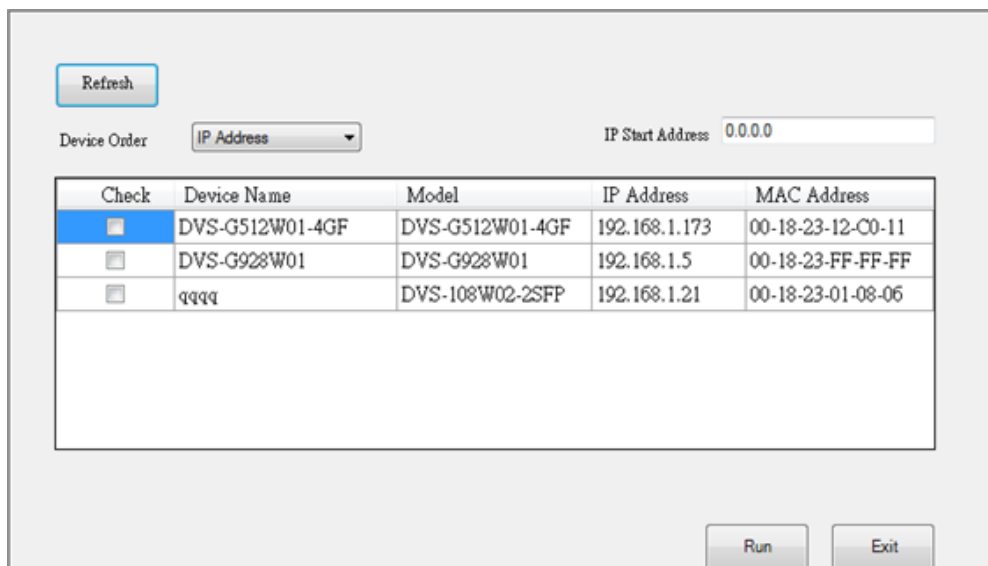
## 4.4 Tools

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.

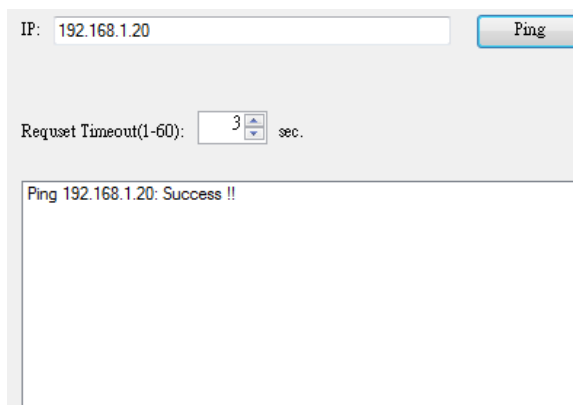


**Note:**

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

### 4.4.2 Ping Test

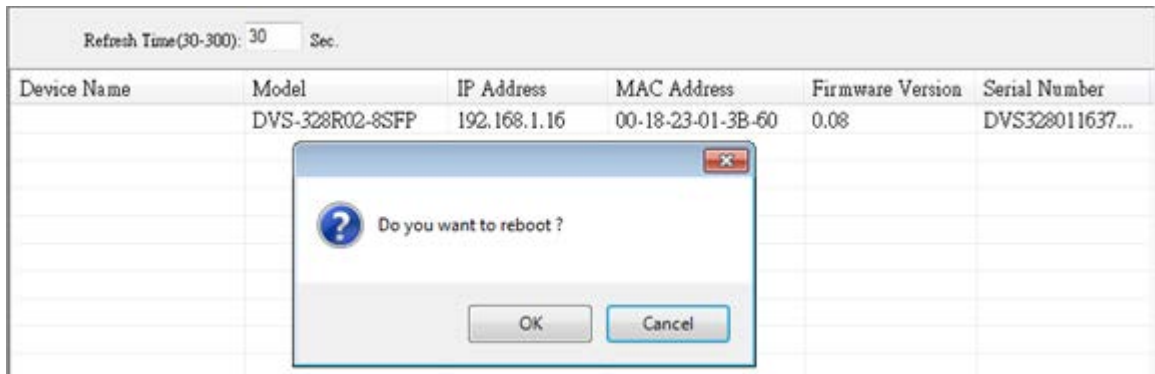
After Ping Test is clicked, you can specify the IP address that you want to ping.





### 4.4.5 Device Reboot

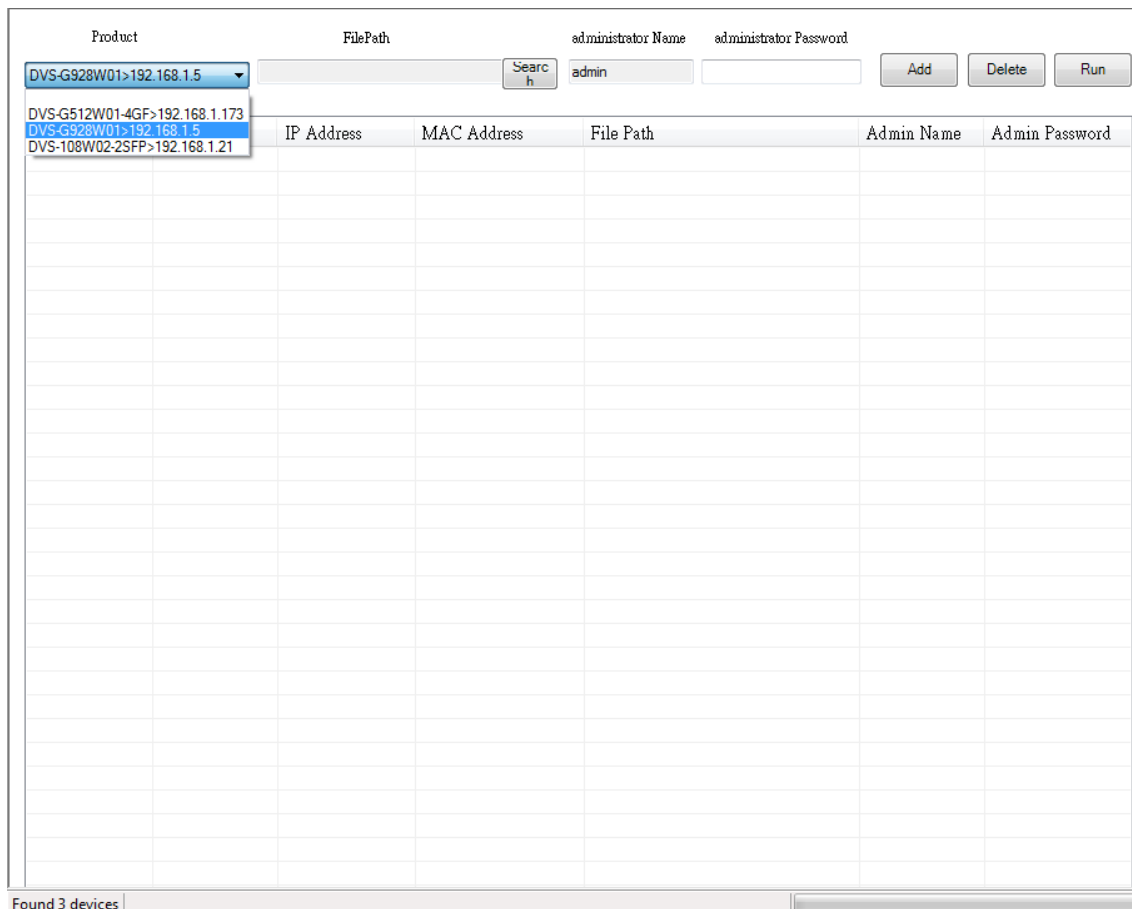
IExplorer allows you to reboot the device via the utility.



### 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.

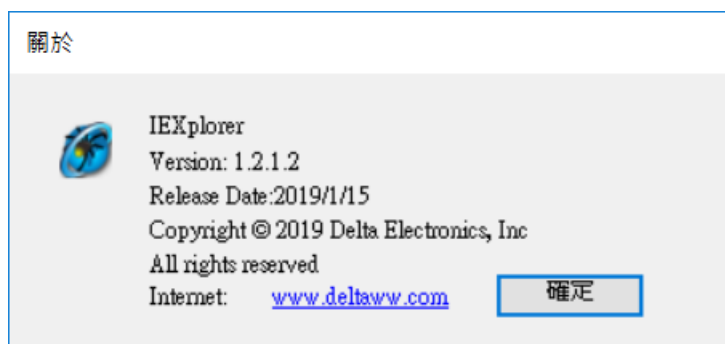
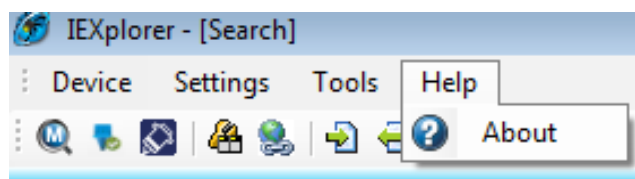


**Note:**

1. If it is update successfully, please wait for 3 minutes to login again.
2. The login ID and the password are the same as the web interface.

## 4.5 Help

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



**MEMO**



---

# Appendix A Private MIB Group

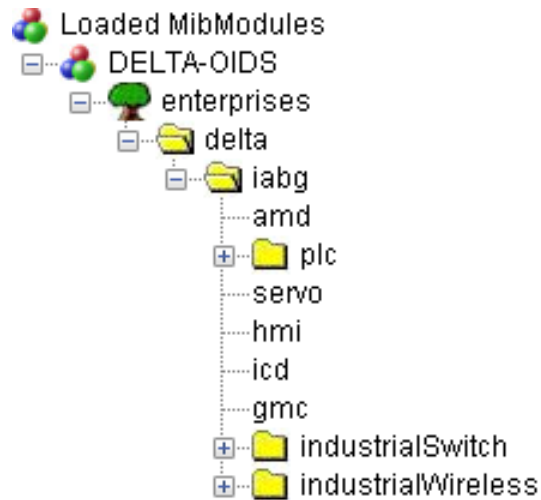
## Table of Contents

A.1	Private MIB Group .....	A-2
-----	-------------------------	-----

## 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.



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

**MEMO**

**A**



---

# Appendix B MODBUS TCP Map

## Table of Contents

**B.1 DVS-G106W02-2GF ..... B-2**  
**B.2 DVS-G112W02-4GF ..... B-8**  
**B.3 DVS-G116W02-4GF ..... B-14**

## B.1 DVS-G106W02-2GF

- Support Function Code 0x03 and 0x04

Address Offset	Data Type	Format	Description	Note
System Information				
0x0001	1 word	HEX	Product Code	Product Code ( 8ABBH )
0x0003	1 word		Firmware Version Hi byte = major Lo byte = minor	Ex: V1.00 High byte = 0x01 Lo byte = 0x00
0x0004	2 word	HEX	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	ASCII	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'
0x0030	20 words	ASCII	Product Name	"DVS-G106W02-2GF" Word 0 Hi byte = 'D' Word 0 Lo byte = 'V' Word 1 Hi byte = 'S' Word 1 Lo byte = '-' Word 2 Hi byte = 'G' Word 2 Lo byte = '1' Word 3 Hi byte = '0' Word 3 Lo byte = '6' Word 4 Hi byte = 'W' Word 4 Lo byte = '0'

				Word 5 Hi byte = '2' Word 5 Lo byte = '-' Word 6 Hi byte = '2' Word 6 Lo byte = 'G' Word 7 Hi byte = 'F' Word 7 Lo byte = '\0'
0x0050	20 words	ASCII	Serial No.	
0x0070	3 words	ASCII	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	HEX	Ethernet IP Address	Ex: IP = 192.168.1.5 Word 0 = 0xC0A8 Word 1 = 0x0105
0x0075	2 words	HEX	Ethernet Netmask	Ex: Mask = 255.255.255.0 Word 0 = 0xFFFF Word 1 = 0xFF00
0x0077	2 words	HEX	Ethernet Gateway IP Address	Ex: IP = 192.168.1.1 Word 0 = 0xC0A8 Word 1 = 0x0101
0x0080	1 word	HEX	Power 1 Status	0x0000: OFF 0x0001: ON
0x0081	1 word	HEX	Power 2 Status	0x0000: OFF 0x0001: ON
0x0090	1 word	HEX	DO 1 Status	0x0000: OFF 0x0001: ON
0x00A0	1 word	HEX	DI 1 Status	0x0000: OFF 0x0001: ON
Port Information				
0x1000 ~ 0x1005	1 word	HEX	Port 1 to 6 Status	0x0000: Link down 0x0001: Link up 0x0002: Disable
0x1100 ~ 0x1105	1 word	HEX	Port 1 to 6 Physical Status	0x0000: 10M,Half 0x0001: 10M,Full 0x0002: 100M,Half 0x0003: 100M,Full 0x0004: 1G,Full
0x1200 ~ 0x1205	1 word	HEX	Port 1 to 6 Flow Control	0x0000: OFF 0x0001: ON
0x1300 ~ 0x1305	1 word	HEX	Port 1 to 6 MDI/MDIX Setting	0x0000: Auto 0x0001: MDI 0x0002: MDIX
0x1500 ~ 0x1505	1 word	HEX	Port 1 to 6 bandwidth overload	0x0000: OFF 0x0001: Port X bandwidth overload

0x1600 ~ 0x1605	1 word	HEX	Port 1 to 6 loopback detection port status	0x0000: OFF 0x0001: loopback detected
0x1A00 ~ 0x1C30	20 words	HEX	Port 1 to 6 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'	Note: 10/100TX,RJ45 10/100/1000TX,RJ45 100/1000,SFP
Packet Information				
0x2000 ~ 0x200B	2 words	HEX	Port 1 to 6 Tx Packets	Ex: Port 1 Tx Packet Amount = 0x33221100 0x2000 = 0x3322 0x2001 = 0x1100
0x2100 ~ 0x210B	2 words	HEX	Port 1 to 6 Rx Packets	Ex: Port 1 Rx Packet Amount = 0x33221100 0x2100 = 0x3322 0x2101 = 0x1100
0x2200 ~ 0x220B	2 words	HEX	Port 1 to 6 Tx Error Packets	Ex: Port 1 Tx Packet Amount = 0x33221100 0x2200 = 0x3322 0x2201 = 0x1100
0x2300 ~ 0x230B	2 words	HEX	Port 1 to 6 Rx Error Packets	Ex: Port 1 Rx Packet Amount = 0x33221100 0x2300 = 0x3322 0x2301 = 0x1100
Redundancy Information ( If the spec for Proprietary Ring is completed, we will add this function )				
0x3000	1 word	HEX	Redundancy Protocol	0x0000: None 0x0001: RSTP/STP
0x3001	1 word	HEX	RSTP Root	0x0000: Not Root 0x0001: Root

**B**

0x3100 ~ 0x3105	1 word	HEX	RSTP Port 1 to 6 Status	0x0000: Port Disable 0x0001: Not RSTP Port 0x0002: Link Down 0x0003: Discarding 0x0004: Learning 0x0005: Forwarding
0x3200	1 word	HEX	RING mode	0x00: None ( Disable ) 0x01: Master 0x02: Slave
0x3201	1 word	HEX	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	HEX	COUPING Mode	0x00: None ( Disable ) 0x01: Head 0x02: Tail
0x3301	1 word	HEX	COUPING State	COUPING mode is disable: 0x00: None 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	HEX	CHAIN Mode	0x00: None ( Disable ) 0x01: Head 0x02: Tail 0x03: Member
0x3401	1 word	HEX	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 ~ 0x4001	1 word	HEX	Port 1 to Port 2 Port No.	

0x4100 ~ 0x4127	20 words	HEX	Port 1 to Port 2 Model Name	SFP DDM Memory Map EEPROM Serial Interface ( 2-Wire Address A0 ) Data Address: 40-55 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	HEX	Port 1 to Port 2 Temperature Word 0 = Temperature MSB Word 1 = Temperature LSB	Real Time Diagnostic ( 2-Wire Address A2h ) Data Address: 96-97
0x4300 ~ 0x4303	2 words	HEX	Port 1 to Port 2 Voltage Word 0 = Vcc MSB Word 1 = Vcc LSB	Real Time Diagnostic ( 2-Wire Address A2h ) Data Address: 99-99
0x4400 ~ 0x4403	2 words	HEX	Port 1 to Port 2 TX Power Word 0 = TX Power MSB Word 1 = TX Power LSB	Real Time Diagnostic ( 2-Wire Address A2h ) Data Address: 102-103
0x4500 ~ 0x4503	2 words	HEX	Port 1 to Port 2 RX Power Word 0 = RX Power MSB Word 1 = RX Power LSB	Real Time Diagnostic ( 2-Wire Address A2h ) Data Address: 104-105
0x4600 ~ 0x4601	1 words	HEX	Port 1 to Port 2 Link Status	0x0000: Link down 0x0001: Link up
Alarm				
0x5000	1 word	HEX	Switch colde start alarm	0x0000: OFF 0x0001: ON 0xFFFF: Disable
0x5001	1 word	HEX	Switch warm start alarm	0x0000: OFF 0x0001: ON
0x5004	1 word	HEX	Power state on alarm	0x0000: OFF 0x0001: ON
0x5005	1 word	HEX	Power state off alarm	0x0000: OFF 0x0001: ON
0x5006	1 word	HEX	DI on alarm	0x0000: OFF 0x0001: ON
0x5007	1 word	HEX	DI off alarm	0x0000: OFF 0x0001: ON

0x5008	1 word	HEX	authentication failure alarm	0x0000: OFF 0x0001: ON
0x5009	1 word	HEX	dot1d Bridge New Root alarm	0x0000: OFF 0x0001: ON
0x500A	1 word	HEX	dot1d Bridge Topology Changed alarm	0x0000: OFF 0x0001: ON
0x500B	1 word	HEX	LLDP Remote Tables Change alarm	0x0000: OFF 0x0001: ON
0x500C	1 word	HEX	Configuartion Changed alarm	0x0000: OFF 0x0001: ON
0x500D	1 word	HEX	Firmware update alarm	0x0000: OFF 0x0001: ON
0x500E	1 word	HEX	IP changed alarm	0x0000: OFF 0x0001: ON
0x500F	1 word	HEX	Passward changed alarm	0x0000: OFF 0x0001: ON
0x5010	1 word	HEX	RING failure	0x0000: OFF 0x0001: ON
0x5011	1 word	HEX	RING backup path is activated	0x0000: OFF 0x0001: ON
0x5012	1 word	HEX	RING returns to health status	0x0000: OFF 0x0001: ON
0x5013	1 word	HEX	CHAIN failure	0x0000: OFF 0x0001: ON
0x5014	1 word	HEX	CHAIN backup path is activated	0x0000: OFF 0x0001: ON
0x5015	1 word	HEX	CHAIN returns to HEALTH status	0x0000: OFF 0x0001: ON
0x5016	1 word	HEX	COUPLING failure	0x0000: OFF 0x0001: ON
0x5017	1 word	HEX	COUPLING backup path is activated	0x0000: OFF 0x0001: ON
0x5018	1 word	HEX	COUPLING returns to HEALTH status	0x0000: OFF 0x0001: ON
0x5100 ~ 0x5101	1 word	HEX	SFP Port 1 to Port 2 DDM Failure - Temp alarm	0x0000: OFF 0x0001: ON
0x5110 ~ 0x5111	1 word	HEX	SFP Port 1 to Port 2 DDM Failure - Voltage	0x0000: OFF 0x0001: ON
0x5120 ~ 0x5121	1 word	HEX	SFP Port 1 to Port 2 DDM Failure - Bias	0x0000: OFF 0x0001: ON
0x5130 ~ 0x5131	1 word	HEX	SFP Port 1 to Port 2 DDM Failure - TX Power	0x0000: OFF 0x0001: ON
0x5140 ~ 0x5141	1 word	HEX	SFP Port 1 to Port 2 DDM Failure - RX Power	0x0000: OFF 0x0001: ON
IABU Internal Data ( 0x2B )				
Device ID Code	Object ID	Length	Description	
0x01	0x00	23 bytes	Vendor Name "Delta Electronics, Inc."	

0x01	32 bytes	Product Name "DVS-G106W02-2GF"	
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"	Length by Firmware Version context

## B.2 DVS-G112W02-4GF

- Support Function Code 0x03 and 0x04

Address Offset	Data Type	Format	Description	Note
System Information				
0x0001	1 word	HEX	Product Code	Product Code ( 8A15H )
0x0003	1 word		Firmware Version Hi byte = major Lo byte = minor	Ex: V1.00 High byte = 0x01 Lo byte = 0x00
0x0004	2 word	HEX	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	ASCII	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'

**B**

0x0030	20 words	ASCII	Product Name	"DVS-G112W02-4GF" Word 0 Hi byte = 'D' Word 0 Lo byte = 'V' Word 1 Hi byte = 'S' Word 1 Lo byte = '.' Word 2 Hi byte = 'G' Word 2 Lo byte = '1' Word 3 Hi byte = '1' Word 3 Lo byte = '2' Word 4 Hi byte = 'W' Word 4 Lo byte = '0' Word 5 Hi byte = '2' Word 5 Lo byte = '.' Word 6 Hi byte = '4' Word 6 Lo byte = 'G' Word 7 Hi byte = 'F' Word 7 Lo byte = '\0'
0x0050	20 words	ASCII	Serial No.	
0x0070	3 words	ASCII	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	HEX	Ethernet IP Address	Ex: IP = 192.168.1.5 Word 0 = 0xC0A8 Word 1 = 0x0105
0x0075	2 words	HEX	Ethernet Netmask	Ex: Mask = 255.255.255.0 Word 0 = 0xFFFF Word 1 = 0xFF00
0x0077	2 words	HEX	Ethernet Gateway IP Address	Ex: IP = 192.168.1.1 Word 0 = 0xC0A8 Word 1 = 0x0101
0x0080	1 word	HEX	Power 1 Status	0x0000: OFF 0x0001: ON
0x0081	1 word	HEX	Power 2 Status	0x0000: OFF 0x0001: ON
0x0090	1 word	HEX	DO 1 Status	0x0000: OFF 0x0001: ON
0x00A0	1 word	HEX	DI 1 Status	0x0000: OFF 0x0001: ON
Port Information				
0x1000 ~ 0x100B	1 word	HEX	Port 1 to 12 Status	0x0000: Link down 0x0001: Link up 0x0002: Disable
0x1100 ~ 0x110B	1 word	HEX	Port 1 to 12 Physical Status	0x0000: 10M,Half 0x0001: 10M,Full 0x0002: 100M,Half 0x0003: 100M,Full 0x0004: 1G,Full

0x1200 ~ 0x120B	1 word	HEX	Port 1 to 12 Flow Control	0x0000: OFF 0x0001: ON
0x1300 ~ 0x130B	1 word	HEX	Port 1 to 12 MDI/MDIX Setting	0x0000: Auto 0x0001: MDI 0x0002: MDIX
0x1500 ~ 0x150B	1 word	HEX	Port 1 to 12 bandwidth overload	0x0000: OFF 0x0001: Port X bandwidth overload
0x1600 ~ 0x160B	1 word	HEX	Port 1 to 12 loopback detection port status	0x0000: OFF 0x0001: loopback detected
0x1A00 ~ 0x1C30	20 words	HEX	Port 1 to 12 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'	Note: 10/100TX,RJ45 10/100/1000TX,RJ45 100/1000,SFP
<b>Packet Information</b>				
0x2000 ~ 0x2017	2 words	HEX	Port 1 to 12 Tx Packets	Ex: Port 1 Tx Packet Amount = 0x33221100 0x2000 = 0x3322 0x2001 = 0x1100
0x2100 ~ 0x2117	2 words	HEX	Port 1 to 12 Rx Packets	Ex: Port 1 Rx Packet Amount = 0x33221100 0x2100 = 0x3322 0x2101 = 0x1100
0x2200 ~ 0x2217	2 words	HEX	Port 1 to 12 Tx Error Packets	Ex: Port 1 Tx Packet Amount = 0x33221100 0x2200 = 0x3322 0x2201 = 0x1100
0x2300 ~ 0x2317	2 words	HEX	Port 1 to 12 Rx Error Packets	Ex: Port 1 Rx Packet Amount = 0x33221100 0x2300 = 0x3322 0x2301 = 0x1100
<b>Redundancy Information ( If the spec for Proprietary Ring is completed, we will add this function )</b>				
0x3000	1 word	HEX	Redundancy Protocol	0x0000: None 0x0001: RSTP/STP

**B**

0x3001	1 word	HEX	RSTP Root	0x0000: Not Root 0x0001: Root
0x3100 ~ 0x310B	1 word	HEX	RSTP Port 1 to 12 Status	0x0000: Port Disable 0x0001: Not RSTP Port 0x0002: Link Down 0x0003: Discarding 0x0004: Learning 0x0005: Forwarding
0x3200	1 word	HEX	RING mode	0x00: None ( Disable ) 0x01: Master 0x02: Slave
0x3201	1 word	HEX	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	HEX	COUPLING Mode	0x00: None ( Disable ) 0x01: Head 0x02: Tail
0x3301	1 word	HEX	COUPLING State	COUPLING mode is disable: 0x00: None COUPLING mode is Head: 0x00: Monitor 0x01: Fault 0x02: Link-Up 0x03: Hold COUPLING mode is Tail 0x00: Discover 0x01: Monitor 0x02: Fault
0x3400	1 word	HEX	CHAIN Mode	0x00: None ( Disable ) 0x01: Head 0x02: Tail 0x03: Member
0x3401	1 word	HEX	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 ~ 0x4003	1 word	HEX	Port 1 to Port 4 Port No.	
0x4100 ~ 0x4127	20 words	HEX	Port 1 to Port 4 Model Name	SFP DDM Memory Map EEPROM Serial Interface ( 2-Wire Address A0 ) Data Address: 40-55 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 ~ 0x4207	2 words	HEX	Port 1 to Port 4 Temperature Word 0 = Temperature MSB Word 1 = Temperature LSB	Real Time Diagnostic ( 2-Wire Address A2h ) Data Address: 96-97
0x4300 ~ 0x4307	2 words	HEX	Port 1 to Port 4 Voltage Word 0 = Vcc MSB Word 1 = Vcc LSB	Real Time Diagnostic ( 2-Wire Address A2h ) Data Address: 99-99
0x4400 ~ 0x4407	2 words	HEX	Port 1 to Port 4 TX Power Word 0 = TX Power MSB Word 1 = TX Power LSB	Real Time Diagnostic ( 2-Wire Address A2h ) Data Address: 102-103
0x4500 ~ 0x4507	2 words	HEX	Port 1 to Port 4 RX Power Word 0 = RX Power MSB Word 1 = RX Power LSB	Real Time Diagnostic ( 2-Wire Address A2h ) Data Address: 104-105
0x4600 ~ 0x4607	1 words	HEX	Port 1 to Port 4 Link Status	0x0000: Link down 0x0001: Link up
<b>Alarm</b>				
0x5000	1 word	HEX	Switch colde start alarm	0x0000: OFF 0x0001: ON 0xFFFF: Disable
0x5001	1 word	HEX	Switch warm start alarm	0x0000: OFF 0x0001: ON
0x5004	1 word	HEX	Power state on alarm	0x0000: OFF 0x0001: ON
0x5005	1 word	HEX	Power state off alarm	0x0000: OFF 0x0001: ON
0x5006	1 word	HEX	DI on alarm	0x0000: OFF 0x0001: ON
0x5007	1 word	HEX	DI off alarm	0x0000: OFF 0x0001: ON

0x5008	1 word	HEX	authentication failure alarm	0x0000: OFF 0x0001: ON
0x5009	1 word	HEX	dot1d Bridge New Root alarm	0x0000: OFF 0x0001: ON
0x500A	1 word	HEX	dot1d Bridge Topology Changed alarm	0x0000: OFF 0x0001: ON
0x500B	1 word	HEX	LLDP Remote Tables Change alarm	0x0000: OFF 0x0001: ON
0x500C	1 word	HEX	Configuartion Changed alarm	0x0000: OFF 0x0001: ON
0x500D	1 word	HEX	Firmware update alarm	0x0000: OFF 0x0001: ON
0x500E	1 word	HEX	IP changed alarm	0x0000: OFF 0x0001: ON
0x500F	1 word	HEX	Password changed alarm	0x0000: OFF 0x0001: ON
0x5010	1 word	HEX	RING failure	0x0000: OFF 0x0001: ON
0x5011	1 word	HEX	RING backup path is activated	0x0000: OFF 0x0001: ON
0x5012	1 word	HEX	RING returns to health status	0x0000: OFF 0x0001: ON
0x5013	1 word	HEX	CHAIN failure	0x0000: OFF 0x0001: ON
0x5014	1 word	HEX	CHAIN backup path is activated	0x0000: OFF 0x0001: ON
0x5015	1 word	HEX	CHAIN returns to HEALTH status	0x0000: OFF 0x0001: ON
0x5016	1 word	HEX	COUPLING failure	0x0000: OFF 0x0001: ON
0x5017	1 word	HEX	COUPLING backup path is activated	0x0000: OFF 0x0001: ON
0x5018	1 word	HEX	COUPLING returns to HEALTH status	0x0000: OFF 0x0001: ON
0x5100 ~ 0x5103	1 word	HEX	SFP Port 1 to Port 4 DDM Failure - Temp alarm	0x0000: OFF 0x0001: ON
0x5110 ~ 0x5113	1 word	HEX	SFP Port 1 to Port 4 DDM Failure - Voltage	0x0000: OFF 0x0001: ON
0x5120 ~ 0x5123	1 word	HEX	SFP Port 1 to Port 4 DDM Failure – Bias	0x0000: OFF 0x0001: ON
0x5130 ~ 0x5133	1 word	HEX	SFP Port 1 to Port 4 DDM Failure - TX Power	0x0000: OFF 0x0001: ON
0x5140 ~ 0x5143	1 word	HEX	SFP Port 1 to Port 4 DDM Failure - RX Power	0x0000: OFF 0x0001: ON
IABU Internal Data ( 0x2B )				
Device ID Code	Object ID	Length	Description	
0x01	0x00	23 bytes	Vendor Name "Delta Electronics, Inc."	
	0x01	32 bytes	Product Name "DVS-G112W02-2GF"	

	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"	Length by Firmware Version context
--	------	---	------------------------------------

### B.3 DVS-G116W02-4GF

- Support Function Code 0x03 and 0x04

Address Offset	Data Type	Format	Description	Note
System Information				
0x0001	1 word	HEX	Product Code	Product Code ( 8A13H )
0x0003	1 word		Firmware Version Hi byte = major Lo byte = minor	Ex: V1.00 High byte = 0x01 Lo byte = 0x00
0x0004	2 word	HEX	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	ASCII	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'

**B**

0x0030	20 words	ASCII	Product Name	"DVS-G116W02-4GF" Word 0 Hi byte = 'D' Word 0 Lo byte = 'V' Word 1 Hi byte = 'S' Word 1 Lo byte = '-' Word 2 Hi byte = 'G' Word 2 Lo byte = '1' Word 3 Hi byte = '1' Word 3 Lo byte = '6' Word 4 Hi byte = 'W' Word 4 Lo byte = '0' Word 5 Hi byte = '2' Word 5 Lo byte = '-' Word 6 Hi byte = '4' Word 6 Lo byte = 'G' Word 7 Hi byte = 'F' Word 7 Lo byte = '0'
0x0050	20 words	ASCII	Serial No.	
0x0070	3 words	ASCII	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	HEX	Ethernet IP Address	Ex: IP = 192.168.1.5 Word 0 = 0xC0A8 Word 1 = 0x0105
0x0075	2 words	HEX	Ethernet Netmask	Ex: Mask = 255.255.255.0 Word 0 = 0xFFFF Word 1 = 0xFF00
0x0077	2 words	HEX	Ethernet Gateway IP Address	Ex: IP = 192.168.1.1 Word 0 = 0xC0A8 Word 1 = 0x0101
0x0080	1 word	HEX	Power 1 Status	0x0000: OFF 0x0001: ON
0x0081	1 word	HEX	Power 2 Status	0x0000: OFF 0x0001: ON
0x0090	1 word	HEX	DO 1 Status	0x0000: OFF 0x0001: ON
0x00A0	1 word	HEX	DI 1 Status	0x0000: OFF 0x0001: ON
Port Information				
0x1000 ~ 0x100B	1 word	HEX	Port 1 to 12 Status	0x0000: Link down 0x0001: Link up 0x0002: Disable
0x1100 ~ 0x110B	1 word	HEX	Port 1 to 12 Physical Status	0x0000: 10M,Half 0x0001: 10M,Full 0x0002: 100M,Half 0x0003: 100M,Full 0x0004: 1G,Full

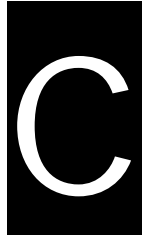
0x1200 ~ 0x120B	1 word	HEX	Port 1 to 12 Flow Control	0x0000: OFF 0x0001: ON
0x1300 ~ 0x130B	1 word	HEX	Port 1 to 12 MDI/MDIX Setting	0x0000: Auto 0x0001: MDI 0x0002: MDIX
0x1500 ~ 0x150B	1 word	HEX	Port 1 to 12 bandwidth overload	0x0000: OFF 0x0001: Port X bandwidth overload
0x1600 ~ 0x160B	1 word	HEX	Port 1 to 12 loopback detection port status	0x0000: OFF 0x0001: loopback detected
0x1A00 ~ 0x1C30	20 words	HEX	Port 1 to 12 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'	Note: 10/100TX,RJ45 10/100/1000TX,RJ45 100/1000,SFP
Packet Information				
0x2000 ~ 0x2017	2 words	HEX	Port 1 to 12 Tx Packets	Ex: Port 1 Tx Packet Amount = 0x33221100 0x2000 = 0x3322 0x2001 = 0x1100
0x2100 ~ 0x2117	2 words	HEX	Port 1 to 12 Rx Packets	Ex: Port 1 Rx Packet Amount = 0x33221100 0x2100 = 0x3322 0x2101 = 0x1100
0x2200 ~ 0x2217	2 words	HEX	Port 1 to 12 Tx Error Packets	Ex: Port 1 Tx Packet Amount = 0x33221100 0x2200 = 0x3322 0x2201 = 0x1100
0x2300 ~ 0x2317	2 words	HEX	Port 1 to 12 Rx Error Packets	Ex: Port 1 Rx Packet Amount = 0x33221100 0x2300 = 0x3322 0x2301 = 0x1100
Redundancy Information ( If the spec for Proprietary Ring is completed, we will add this function )				
0x3000	1 word	HEX	Redundancy Protocol	0x0000: None 0x0001: RSTP/STP

0x3001	1 word	HEX	RSTP Root	0x0000: Not Root 0x0001: Root
0x3100 ~ 0x310B	1 word	HEX	RSTP Port 1 to 12 Status	0x0000: Port Disable 0x0001: Not RSTP Port 0x0002: Link Down 0x0003: Discarding 0x0004: Learning 0x0005: Forwarding
0x3200	1 word	HEX	RING mode	0x00: None ( Disable ) 0x01: Master 0x02: Slave
0x3201	1 word	HEX	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	HEX	COUPING Mode	0x00: None ( Disable ) 0x01: Head 0x02: Tail
0x3301	1 word	HEX	COUPING State	COUPING mode is disable: 0x00: None 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	HEX	CHAIN Mode	0x00: None ( Disable ) 0x01: Head 0x02: Tail 0x03: Member
0x3401	1 word	HEX	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 ~ 0x4003	1 word	HEX	Port 1 to Port 4 Port No.	
0x4100 ~ 0x4127	20 words	HEX	Port 1 to Port 4 Model Name	SFP DDM Memory Map EEPROM Serial Interface ( 2-Wire Address A0 ) Data Address: 40-55 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	HEX	Port 1 to Port 2 Temperature Word 0 = Temperature MSB Word 1 = Temperature LSB	Real Time Diagnostic ( 2-Wire Address A2h ) Data Address: 96-97
0x4300 ~ 0x4303	2 words	HEX	Port 1 to Port 2 Voltage Word 0 = Vcc MSB Word 1 = Vcc LSB	Real Time Diagnostic ( 2-Wire Address A2h ) Data Address: 98-99
0x4400 ~ 0x4403	2 words	HEX	Port 1 to Port 2 TX Power Word 0 = TX Power MSB Word 1 = TX Power LSB	Real Time Diagnostic ( 2-Wire Address A2h ) Data Address: 102-103
0x4500 ~ 0x4503	2 words	HEX	Port 1 to Port 2 RX Power Word 0 = RX Power MSB Word 1 = RX Power LSB	Real Time Diagnostic ( 2-Wire Address A2h ) Data Address: 104-105
0x4600 ~ 0x4601	1 words	HEX	Port 1 to Port 2 Link Status	0x0000: Link down 0x0001: Link up
Alarm				
0x5000	1 word	HEX	Switch colde start alarm	0x0000: OFF 0x0001: ON 0xFFFF: Disable
0x5001	1 word	HEX	Switch warm start alarm	0x0000: OFF 0x0001: ON
0x5004	1 word	HEX	Power state on alarm	0x0000: OFF 0x0001: ON
0x5005	1 word	HEX	Power state off alarm	0x0000: OFF 0x0001: ON
0x5006	1 word	HEX	DI on alarm	0x0000: OFF 0x0001: ON
0x5007	1 word	HEX	DI off alarm	0x0000: OFF 0x0001: ON

0x5008	1 word	HEX	authentication failure alarm	0x0000: OFF 0x0001: ON
0x5009	1 word	HEX	dot1d Bridge New Root alarm	0x0000: OFF 0x0001: ON
0x500A	1 word	HEX	dot1d Bridge Topology Changed alarm	0x0000: OFF 0x0001: ON
0x500B	1 word	HEX	LLDP Remote Tables Change alarm	0x0000: OFF 0x0001: ON
0x500C	1 word	HEX	Configuartion Changed alarm	0x0000: OFF 0x0001: ON
0x500D	1 word	HEX	Firmware update alarm	0x0000: OFF 0x0001: ON
0x500E	1 word	HEX	IP changed alarm	0x0000: OFF 0x0001: ON
0x500F	1 word	HEX	Passward changed alarm	0x0000: OFF 0x0001: ON
0x5010	1 word	HEX	RING failure	0x0000: OFF 0x0001: ON
0x5011	1 word	HEX	RING backup path is activated	0x0000: OFF 0x0001: ON
0x5012	1 word	HEX	RING returns to health status	0x0000: OFF 0x0001: ON
0x5013	1 word	HEX	CHAIN failure	0x0000: OFF 0x0001: ON
0x5014	1 word	HEX	CHAIN backup path is activated	0x0000: OFF 0x0001: ON
0x5015	1 word	HEX	CHAIN returns to HEALTH status	0x0000: OFF 0x0001: ON
0x5016	1 word	HEX	COUPLING failure	0x0000: OFF 0x0001: ON
0x5017	1 word	HEX	COUPLING backup path is activated	0x0000: OFF 0x0001: ON
0x5018	1 word	HEX	COUPLING returns to HEALTH status	0x0000: OFF 0x0001: ON
0x5100 ~ 0x5101	1 word	HEX	SFP Port 1 to Port 2 DDM Failure - Temp alarm	0x0000: OFF 0x0001: ON
0x5110 ~ 0x5111	1 word	HEX	SFP Port 1 to Port 2 DDM Failure - Voltage	0x0000: OFF 0x0001: ON
0x5120 ~ 0x5121	1 word	HEX	SFP Port 1 to Port 2 DDM Failure - Bias	0x0000: OFF 0x0001: ON
0x5130 ~ 0x5131	1 word	HEX	SFP Port 1 to Port 2 DDM Failure - TX Power	0x0000: OFF 0x0001: ON
0x5140 ~ 0x5141	1 word	HEX	SFP Port 1 to Port 2 DDM Failure - RX Power	0x0000: OFF 0x0001: ON
IABU Internal Data ( 0x2B )				
Device ID Code	Object ID	Length	Description	
0x01	0x00	23 bytes	Vendor Name "Delta Electronics, Inc."	
	0x01	32 bytes	Product Name "DVS-G116W02-2GF"	

	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"	Length by Firmware Version context
--	------	--	------------------------------------



---

## Appendix C EtherNet/IP

### Table of Contents

C.1	DVS-G106W02-2GF.....	C-2
C.2	DVS-G112W02-4GF.....	C-13
C.3	DVS-G116W02-4GF.....	C-23

## C.1 DVS-G106W02-2GF

- Support Function Code 0x03 and 0x04

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 ( 8ABBH )
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-G106W02-2GF", 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	Input	<b>Refer to Base Switch Object Attr ID 4</b> <b>Byte 0:</b> Power Source Status (Least Significant Byte) <b>Byte 1:</b> Power Source Status (Most Significant Byte) <b>Refer to Base Switch Object Attr ID 8</b> <b>Byte 2-5:</b> Global Link Status DWORD 0 <b>Byte 6-9:</b> Global Link Status DWORD 1 <b>Byte 10-13:</b> Global Link Status DWORD 2 <b>Byte 14-17:</b> Global Link Status DWORD 3
2	16	Global Admin State	Input	<b>Refer to Base Switch Object Attr ID 7</b> <b>Byte 0-3:</b> Global Admin Status DWORD 0 <b>Byte 4-7:</b> Global Admin Status DWORD 1 <b>Byte 8-11:</b> Global Admin Status DWORD 2 <b>Byte 12-15:</b> Global Admin Status DWORD 3
3	2	Contact Status	Input	<b>Refer to Base Switch Object Attr ID 10</b> <b>Byte 0:</b> Contact Status (Least Significant Byte) <b>Byte 1:</b> Contact Status (Most Significant Byte)
50	16	TBD	Output	TBD
64	76	Device Status	Input	Refer to I/O Assembly - 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.

<b>I/O Assembly</b>				
Direction	Name	Size	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 Status 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 Status DWORD 2 Global Admin Status DWORD 3	
	Contact Status	WORD	Refer to Base Switch Object Attr ID 10	
	AlarmStauts	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 Mode	USINT	Refer to Delta IES Object Attr 19	
	Redundancy - CHAIN Statue	USINT	Refer to Delta IES Object Attr 20	
	Redundancy - COUPING Mode	USINT	Refer to Delta IES Object Attr 21	
Redundancy - COUPING State	USINT	Refer to Delta IES Object Attr 22		
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 Status DWORD 2 Global Admin Status DWORD 3	
<b>Connection Manager Object ( 0x06 )</b>				
<b>Class Attributes</b>				
Attr ID	Access Rule	Name	Data Type	Description of Attribute
1	Get	Revision	UINT	Revision of this object
<b>Instance Attributes</b>				
Attr ID	Access Rule	Name	Data Type	Description of Attribute
<b>Common Services</b>				
Service	Need in Implementation	Service Name	Description of Service	

Code	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 <b>Bit 0: BOOTP Client</b> 1 (TRUE) shall indicate the device is capable of obtaining its network configuration via BOOTP. <b>Bit 1: DNS Client</b> 1 (TRUE) shall indicate the device is capable of resolving host names by querying a DNS server. <b>Bit 2: DHCP Client</b> 1 (TRUE) shall indicate the device is capable of obtaining its network configuration via DHCP. <b>Bit 3: DHCP-DNS Update</b> Shall be 0 <b>Bit 4: Configuration Settable</b> 1 (TRUE) shall indicate the Interface Configuration attribute is settable.
3	Get/Set	Configuration Control	DWORD	Interface control flags <b>Bit 0-3: Configuraiton Method</b> 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. <b>Bit 4: DNS Enable</b> 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).
<b>Common Services</b>				
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
<b>Common Services</b>				
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 <b>Bit 0-1: Power Source 1</b> <b>Bit 2-3: Power Source 2....</b> <b>Bit 14-15: Power Source 8</b> 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 ) <b>DWORD[0]: Port 0 - 31 admin status</b> <b>DWORD[1]: Port 32 - 63 admin status</b> <b>DWORD[2]: Port 64 - 95 admin status</b> <b>DWORD[3]: Port 96 - 127 admin status</b> 0 = Port ( or Interface ) Disabled 1 = Port ( or Interface ) Enabled
8	Get	Global Port Link Status	ARRAY OF DWORD	Port Link Status ( Note: Size of array = attribute 5 ) <b>DWORD[0]: Port 0 - 31 link status</b> <b>DWORD[1]: Port 32 - 63 link status</b> <b>DWORD[2]: Port 64 - 95 link status</b> <b>DWORD[3]: Port 96 - 127 link status</b> 0 = Link inactive ( Down ) 1 = Link Active ( UP )

10	Get	Constact Status	WORD	Switch Contact Closure ( DI ) <b>Bit 0-1: Switch Contact 1 ( DI 1 )</b> <b>Bit 2-3: Switch Contact 2 ( DI 2 )</b> 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 <b>Bit 2-3: Relay Output 2 status</b> Other Reserved ( should be 0 ) 00 = Digital output not support/presed 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 <del>Bit 6: power3 state on-&gt;off</del> <del>Bit 7: power3 state off-&gt;on</del> Bit 8: DI1 state on->off

				<del>Bit 9: DI1 state off-&gt;on</del> <del>Bit 6: DI1 state on-&gt;off</del> <del>Bit 7: DI1 state off-&gt;on</del> <del>Bit 8: DI2 state on-&gt;off</del> <del>Bit 9: DI2 state off-&gt;on</del> 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
14	Get	SFP Failure	ARRAY OF USINT	Support 8 port. <b>Byte 0: SFP port 1 Failure state</b> <b>Byte 1: SFP port 2 Failure state....</b> <b>Byte 7: SFP port 8 Failure state</b> Bit 0: SFP port present 0 = Not present, 1 = present Bit 1: Temp alarm state 0 = ON, 1 = OFF Bit 2: Voltage alarm state 0 = ON, 1 = OFF Bit 3: Bias alarm state 0 = ON, 1 = OFF Bit 4: TX Power state 0 = ON, 1 = OFF Bit 5: RX Power state 0 = ON, 1 = OFF Bit 6-7: Reserved
15	Get	Redundancy Protocol	USINT	0x00: None 0x01: 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 Mode	USINT	0x00: None ( Disable ) 0x01: Head 0x02: Tail 0x03: Member
20	Get	Redundancy - CHAIN State	USINT	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
21	Get	Redundancy - COUPING Mode	USINT	0x00: None ( Disable ) 0x01: Head 0x02: Tail
22	Get	Redundancy - COUPING State	USINT	COUPING mode is disable: 0x00: None 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-G112W02-4GF

- Support Function Code 0x03 and 0x04

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 ( 8A15H )
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-G112W02-4GF", 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	<b>Refer to Base Switch Object Attr ID 4</b> <b>Byte 0:</b> Power Source Status (Least Significant Byte) <b>Byte 1:</b> Power Source Status (Most Significant Byte) <b>Refer to Base Switch Object Attr ID 8</b> <b>Byte 2-5:</b> Global Link Status DWORD 0 <b>Byte 6-9:</b> Global Link Status DWORD 1 <b>Byte 10-13:</b> Global Link Stauts DWORD 2 <b>Byte 14-17:</b> Global Link Status DWORD 3
2	16	Global Admin State	Input	<b>Refer to Base Switch Object Attr ID 7</b> <b>Byte 0-3:</b> Global Admin Status DWORD 0 <b>Byte 4-7:</b> Global Admin Status DWORD 1 <b>Byte 8-11:</b> Global Admin Stauts DWORD 2 <b>Byte 12-15:</b> Global Admin Status DWORD 3
3	2	Contact Status	Input	<b>Refer to Base Switch Object Attr ID 10</b> <b>Byte 0:</b> Contact Status (Least Signficant Byte) <b>Byte 1:</b> Contact Status (Most Signficant Byte)
50	16	TBD	Output	TBD
64	76	Device Status	Input	Refer to I/O Assembly - 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				
Direction	Name	Size	Name	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 Status 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 Status DWORD 2 Global Admin Status DWORD 3
	Contact Status	WORD	Refer to Base Switch Object Attr ID 10
	AlarmStauts	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 Mode	USINT	Refer to Delta IES Object Attr 19
	Redundancy - CHAIN Statue	USINT	Refer to Delta IES Object Attr 20
	Redundancy - COUPING Mode	USINT	Refer to Delta IES Object Attr 21
Redundancy - COUPING State	USINT	Refer to Delta IES Object Attr 22	
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 Status 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	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 <b>Bit 0: BOOTP Client</b> 1 (TRUE) shall indicate the device is capable of obtaining its network configuration via BOOTP. <b>Bit 1: DNS Client</b> 1 (TRUE) shall indicate the device is capable of resolving host names by querying a DNS server. <b>Bit 2: DHCP Client</b> 1 (TRUE) shall indicate the device is capable of obtaining its network configuration via DHCP. <b>Bit 3: DHCP-DNS Update</b> Shall be 0 <b>Bit 4: Configuration Settable</b> 1 (TRUE) shall indicate the Interface Configuration attribute is settable.
3	Get/Set	Configuration Control	DWORD	Interface control flags <b>Bit 0-3: Configuration Method</b> 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. <b>Bit 4: DNS Enable</b> 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
		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)).
<b>Common Services</b>				
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 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
<b>Common Services</b>				
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 <b>Bit 0-1: Power Source 1</b> <b>Bit 2-3: Power Source 2....</b> <b>Bit 14-15: Power Source 8</b> 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 ) <b>DWORD[0]: Port 0 - 31 admin status</b> <b>DWORD[1]: Port 32 - 63 admin status</b> <b>DWORD[2]: Port 64 - 95 admin status</b> <b>DWORD[3]: Port 96 - 127 admin status</b> 0 = Port ( or Interface ) Disabled 1 = Port ( or Interface ) Enabled
8	Get	Global Port Link Status	ARRAY OF DWORD	Port Link Status ( Note: Size of array = attribute 5 ) <b>DWORD[0]: Port 0 - 31 link status</b> <b>DWORD[1]: Port 32 - 63 link status</b> <b>DWORD[2]: Port 64 - 95 link status</b> <b>DWORD[3]: Port 96 - 127 link status</b> 0 = Link inactive ( Down ) 1 = Link Active ( UP )
10	Get	Constact Status	WORD	Switch Contact Closure ( DI ) <b>Bit 0-1: Switch Contact 1 ( DI 1 )</b> <b>Bit 2-3: Switch Contact 2 ( DI 2 )</b> 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 <del>Bit 2-3: Relay Output 2 status</del> Other Reserved ( should be 0 ) 00 = Digital output not support/presed 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 <del>Bit 6: power3 state on-&gt;off</del> <del>Bit 7: power3 state off-&gt;on</del> Bit 8: DI1 state on->off Bit 9: DI1 state off->on <del>Bit 6: DI1 state on-&gt;off</del> <del>Bit 7: DI1 state off-&gt;on</del> <del>Bit 8: DI2 state on-&gt;off</del> <del>Bit 9: DI2 state off-&gt;on</del> 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: passward 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
14	Get	SFP Failure	ARRAY OF USINT	Support 8 port. <b>Byte 0: SFP port 1 Failure state</b> <b>Byte 1: SFP port 2 Failure state....</b> <b>Byte 7: SFP port 8 Failure state</b> Bit 0: SFP port present 0 = Not present, 1 = present Bit 1: Temp alram state 0 = ON, 1 = OFF Bit 2: Voltage alarm state 0 = ON, 1 = OFF Bit 3: Bias alarm state 0 = ON, 1 = OFF Bit 4: TX Power state 0 = ON, 1 = OFF Bit 5: RX Power state 0 = ON, 1 = OFF Bit 6-7: Reserved
15	Get	Redundancy Protocol	USINT	0x00: None 0x01: 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 Mode	USINT	0x00: None ( Disable ) 0x01: Head 0x02: Tail 0x03: Member

20	Get	Redundancy - CHAIN State	USINT	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
21	Get	Redundancy - COUPING Mode	USINT	0x00: None ( Disable ) 0x01: Head 0x02: Tail
22	Get	Redundancy - COUPING State	USINT	COUPING mode is disable: 0x00: None COUPING mode is Head: 0x00: Monitor 0x01: Fault 0x02: Link-Up 0x03: Hold COUPING mode is Tail 0x00: Discover 0x01: Monitor 0x02: Fault
<b>Common Services</b>				
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-G116W02-4GF

- Support Function Code 0x03 and 0x04

<b>Identity Object ( 0x01 )</b>				
<b>Class Attributes</b>				
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
<b>Instance Attributes</b>				
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 ( 8A13H )
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-G116W02-4GF", 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	Input	<b>Refer to Base Switch Object Attr ID 4</b> <b>Byte 0:</b> Power Source Status (Least Significant Byte) <b>Byte 1:</b> Power Source Status (Most Significant Byte) <b>Refer to Base Switch Object Attr ID 8</b> <b>Byte 2-5:</b> Global Link Status DWORD 0 <b>Byte 6-9:</b> Global Link Status DWORD 1 <b>Byte 10-13:</b> Global Link Status DWORD 2 <b>Byte 14-17:</b> Global Link Status DWORD 3
2	16	Global Admin State	Input	Refer to Base Switch Object Attr ID 7 <b>Byte 0-3:</b> Global Admin Status DWORD 0 <b>Byte 4-7:</b> Global Admin Status DWORD 1 <b>Byte 8-11:</b> Global Admin Status DWORD 2 <b>Byte 12-15:</b> Global Admin Status DWORD 3
3	2	Contact Status	Input	Refer to Base Switch Object Attr ID 10 <b>Byte 0:</b> Contact Status (Least Significant Byte) <b>Byte 1:</b> Contact Status (Most Significant Byte)
50	16	TBD	Output	TBD
64	76	Device Status	Input	Refer to I/O Assembly - Input
<b>Common Services</b>				
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.

<b>I/O Assembly</b>			
Direction	Name	Size	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 Status 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
	AlarmStauts	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 Mode	USINT	Refer to Delta IES Object Attr 19
	Redundancy - CHAIN Statue	USINT	Refer to Delta IES Object Attr 20
	Redundancy - COUPING Mode	USINT	Refer to Delta IES Object Attr 21
	Redundancy - COUPING State	USINT	Refer to Delta IES Object Attr 22
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	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	<p>Interface capability</p> <p><b>Bit 0: BOOTP Client</b> 1 (TRUE) shall indicate the device is capable of obtaining its network configuration via BOOTP.</p> <p><b>Bit 1: DNS Client</b> 1 (TRUE) shall indicate the device is capable of resolving host names by querying a DNS server.</p> <p><b>Bit 2: DHCP Client</b> 1 (TRUE) shall indicate the device is capable of obtaining its network configuration via DHCP.</p> <p><b>Bit 3: DHCP-DNS Update</b> Shall be 0</p> <p><b>Bit 4: Configuration Settable</b> 1 (TRUE) shall indicate the Interface Configuration attribute is settable.</p>
3	Get/Set	Configuration Control	DWORD	<p>Interface control flags</p> <p><b>Bit 0-3: Configuration Method</b> 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.</p> <p><b>Bit 4: DNS Enable</b> If 1 (TRUE), the device shall resolve host names by querying a DNS server.</p>
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).
<b>Common Services</b>				
Service	Need in Implementation	Service Name	Description of Service	

Code	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 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 <b>Bit 0-1: Power Source 1</b> <b>Bit 2-3: Power Source 2....</b> <b>Bit 14-15: Power Source 8</b> 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 ) <b>DWORD[0]: Port 0 - 31 admin status</b> <b>DWORD[1]: Port 32 - 63 admin status</b> <b>DWORD[2]: Port 64 - 95 admin status</b> <b>DWORD[3]: Port 96 - 127 admin status</b> 0 = Port ( or Interface ) Disabled 1 = Port ( or Interface ) Enabled
8	Get	Global Port Link Status	ARRAY OF DWORD	Port Link Status ( Note: Size of array = attribute 5 ) <b>DWORD[0]: Port 0 - 31 link status</b> <b>DWORD[1]: Port 32 - 63 link status</b> <b>DWORD[2]: Port 64 - 95 link status</b> <b>DWORD[3]: Port 96 - 127 link status</b> 0 = Link inactive ( Down ) 1 = Link Active ( UP )
10	Get	Constact Status	WORD	Switch Contact Closure ( DI ) <b>Bit 0-1: Switch Contact 1 ( DI 1 )</b> <b>Bit 2-3: Switch Contact 2 ( DI 2 )</b> 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
<b>Instance Attributes</b>				
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 <del>Bit 2-3: Relay Output 2 status</del> Other Reserved ( should be 0 ) 00 = Digital output not support/presed 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 <del>Bit 6: power3 state on-&gt;off</del> <del>Bit 7: power3 state off-&gt;on</del> Bit 8: DI1 state on->off Bit 9: DI1 state off->on <del>Bit 6: DI1 state on-&gt;off</del> <del>Bit 7: DI1 state off-&gt;on</del> <del>Bit 8: DI2 state on-&gt;off</del> <del>Bit 9: DI2 state off-&gt;on</del> 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: passward 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
14	Get	SFP Failure	ARRAY OF USINT	Support 8 port. <b>Byte 0: SFP port 1 Failure state</b> <b>Byte 1: SFP port 2 Failure state....</b> <b>Byte 7: SFP port 8 Failure state</b> Bit 0: SFP port present 0 = Not present, 1 = present Bit 1: Temp alarm state 0 = ON, 1 = OFF Bit 2: Voltage alarm state 0 = ON, 1 = OFF Bit 3: Bias alarm state 0 = ON, 1 = OFF Bit 4: TX Power state 0 = ON, 1 = OFF Bit 5: RX Power state 0 = ON, 1 = OFF Bit 6-7: Reserved
15	Get	Redundancy Protocol	USINT	0x00: None 0x01: 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 Mode	USINT	0x00: None ( Disable ) 0x01: Head 0x02: Tail 0x03: Member

20	Get	Redundancy - CHAIN State	USINT	<p>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</p>
21	Get	Redundancy - COUPING Mode	USINT	<p>0x00: None ( Disable )                      0x01: Head                      0x02: Tail</p>
22	Get	Redundancy - COUPING State	USINT	<p>COUPING mode is disable:                      0x00: None                      COUPING mode is Head:                      0x00: Monitor                      0x01: Fault                      0x02: Link-Up                      0x03: Hold                      COUPING mode is Tail                      0x00: Discover                      0x01: Monitor                      0x02: Fault</p>

**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.....D-2

## 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