

# ForeFront 3210P Series **VDSL2 IP Switch**

---

## *User Manual*



This is a Class A device and is not intended for use in a residential environment.



IMPORTANT

**Important**—The compliance information in this document is pending and subject to change.

Sales Office: +1 (301) 975-1000  
Technical Support: +1 (301) 975-1007  
E-mail: [support@patton.com](mailto:support@patton.com)  
WWW: [www.patton.com](http://www.patton.com)

Part Number: **07MFF3210P-UM**  
Revised: **May 31, 2013**

**Patton Electronics Company, Inc.**

7622 Rickenbacker Drive  
Gaithersburg, MD 20879 USA  
Tel: +1 (301) 975-1000  
Fax: +1 (301) 869-9293  
Support: +1 (301) 975-1007  
Web: [www.patton.com](http://www.patton.com)  
E-mail: [support@patton.com](mailto:support@patton.com)

**Copyright © 2013, Patton Electronics Company. All rights reserved.**

The information in this document is subject to change without notice. Patton Electronics assumes no liability for errors that may appear in this document.

**Important Information**

To use virtual private network (VPN) and/or AES/DES/3DES encryption capabilities with the ForeFront, you may need to purchase additional licenses, hardware, software, network connection, and/or service. Contact [sales@patton.com](mailto:sales@patton.com) or +1 (301) 975-1000 for assistance.

**Warranty Information**

Patton Electronics warrants all ForeFront components to be free from defects, and will—at our option—repair or replace the product should it fail within one year from the first date of the shipment.

This warranty is limited to defects in workmanship or materials, and does not cover customer damage, abuse or unauthorized modification. If the product fails to perform as warranted, your sole recourse shall be repair or replacement as described above. Under no condition shall Patton Electronics be liable for any damages incurred by the use of this product. These damages include, but are not limited to, the following: lost profits, lost savings and incidental or consequential damages arising from the use of or inability to use this product. Patton Electronics specifically disclaims all other warranties, expressed or implied, and the installation or use of this product shall be deemed an acceptance of these terms by the user.

# Table of Contents

Table of Contents.....	3
List of Figures.....	7
List of Tables.....	9
About This Guide .....	10
Audience .....	10
Structure .....	10
Precautions .....	11
Safety When Working with Electricity .....	12
General Observations .....	13
Typographical Conventions Used in this Document .....	13
General Conventions .....	13
<b>1 General Information .....</b>	<b>14</b>
ForeFront 3210P VDSL2 IP Switch Overview .....	15
Network Features .....	15
ForeFront 3210P VDSL2 IP Switch Panels .....	18
LED Indicators .....	18
Reset Button .....	18
Pin Assignment of RJ21 Cable .....	19
<b>2 Web Configuration .....</b>	<b>20</b>
Introduction .....	22
Connecting to the Web Management System .....	22
Administration .....	23
IP Address .....	23
Switch Setting .....	23
Basic .....	24
Module Info .....	24
Misc Config .....	24
Console Port Information .....	25
Port Configuration .....	25
Port Controls .....	26
Port Sniffer .....	27
Protected Port .....	27
VDSL Port Status .....	28
SNMP Configuration .....	29
System Options .....	29
Community Strings .....	29
Trap Manager .....	30
SNMPv3 Group .....	30
SNMPv3 View .....	30
SNMPv3 Access .....	31

SNMPv3 USM-user .....	31
Syslog Setting .....	32
Alarm Configuration .....	33
Temperature & Fan Status .....	33
Firmware Update .....	33
Configuration Backup .....	34
TFTP Restore Configuration .....	34
TFTP Backup Configuration .....	34
SNTP Settings .....	35
L2 Features .....	35
VLAN Configuration .....	36
Static VLAN .....	36
GVRP VLAN .....	38
QinQ VLAN .....	39
Trunking .....	41
Aggregator Setting .....	41
Aggregator information .....	42
Static Activity .....	42
Forwarding & Filtering .....	43
Dynamic MAC Table .....	43
Static MAC Table .....	44
MAC Filtering .....	44
IGMP Snooping .....	44
Spanning Tree .....	45
System Configuration .....	46
PerPort Configuration .....	47
Instance .....	48
Interface .....	48
DHCP Relay & Opt. 82 .....	48
DHCP Option 82 .....	49
DHCP Relay .....	49
DHCP Option 82 Router Port .....	49
DHCP Opt. 82 Port Table .....	49
ACL (Access Control List) .....	50
IPv4 .....	51
Non-IPv4 .....	52
Binding .....	52
QoS VoIP .....	53
Security .....	53
Security Manager .....	53
MAC Limit .....	54
Configure MAC Limit .....	54
MAC Limit Port Status .....	54
802.1x Configuration .....	54

System Configuration .....	55
PerPort Configuration .....	55
Misc Configuration .....	56
QoS .....	57
QoS Configuration .....	57
QoS Configuration - Priority Queue Service .....	57
PerPort Configuration .....	57
ToS/DSCP .....	58
Monitoring .....	59
Port Status .....	59
Port Statistics .....	60
VDSL .....	61
Configuration .....	61
Profile Table .....	62
Reset System .....	62
Reboot .....	63
<b>3 Configuration Via Console .....</b>	<b>64</b>
Introduction .....	65
Login to the Console .....	65
General Information of Commands .....	66
Configuration .....	67
Command Descriptions .....	69
System Commands .....	69
Switch Static Configuration .....	69
Trunk Commands .....	71
LACP Commands .....	71
VLAN Mode & Commands .....	72
GVRP Commands .....	73
QinQ Commands .....	75
Misc Configuration .....	75
Administration .....	76
Port Mirroring .....	77
QoS .....	77
Commands for MAC .....	78
MAC Limits .....	79
Protocol Related Commands .....	79
STP/RSTP .....	79
MSTP .....	81
SNMP .....	84
IGMP .....	87
802.1x .....	88
DHCP Relay & Option82 .....	89
Syslog .....	90

SSH .....	90
Reboot Switch .....	90
TFTP Function .....	90
Access Control List .....	91
IPv4 ACL commands .....	91
Non-IPv4 ACL commands .....	93
SIP/SMAC Binding .....	93
<b>4 Contacting Patton for Assistance .....</b>	<b>96</b>
Introduction .....	97
Contact Information .....	97
Patton Support Headquarters in the USA .....	97
Alternate Patton Support for Europe, Middle East, and Africa (EMEA) .....	97
Warranty Service and Returned Merchandise Authorizations (RMAs) .....	97
Warranty Coverage .....	97
Out-of-warranty service .....	98
Returns for credit .....	98
Return for credit policy .....	98
RMA Numbers .....	98
Shipping instructions .....	98
<b>A Compliance Information .....</b>	<b>99</b>
Compliance .....	100
EMC .....	100
Low-Voltage Directive (Safety) .....	100
Radio and TV Interference .....	100
CE Declaration of Conformity .....	100
Authorized European Representative .....	100
<b>B Specifications .....</b>	<b>101</b>
Interfaces .....	102
LED Indicators .....	102
Standards Support .....	102
Protocol Support .....	102
Security .....	102
Device Management .....	103
Physical .....	103

## List of Figures

1	ForeFront 3210P VDSL2 IP Switch	15
2	Web Management System home page	22
3	Administration navigation	23
4	IP Address Setting	23
5	Switch Setting > Basic	24
6	Switch Setting > Module Info	24
7	Switch Setting > Misc Config	24
8	Console Information	25
9	Port Configuration > Port Control	26
10	Port Configuration > Port Sniffer	27
11	Port Configuration > Protected Port Setting	27
12	Port Configuration > VDSL Port Status	28
13	Detailed VDSL Port Status	28
14	SNMP Configuration	29
15	SNMP Configuration > System Options	29
16	SNMP Configuration > Community Strings	29
17	SNMP Configuration > Trap Managers	30
18	SNMP Configuration > SNMPv3 Group	30
19	SNMP Configuration > SNMPv3 View	31
20	SNMP Configuration > SNMPv3 Access	31
21	SNMP Configuration > SNMPv3 USM-user	32
22	Syslog Setting	32
23	Alarm Configuration	33
24	Temperature and Fan Information	33
25	Firmware Update	33
26	Configuration Restore	34
27	Configuration Restore > TFTP Restore Configuration	34
28	Configuration Restore > TFTP Backup Configuration	34
29	SNTF Settings	35
30	VLAN Configuration	36
31	VLAN Configuration > Static VLAN	36
32	VLAN Configuration > Static VLAN > Basic	37
33	VLAN mode	37
34	Create a VLAN group	37
35	VLAN Configuration > Static VLAN > VLAN filters	38
36	VLAN filter table	38
37	VLAN Configuration > GVRP Configuration	38
38	VLAN Configuration > GVRP Configuration > GVRP Settings	39
39	VLAN Configuration > QinQ Configuration	39
40	VLAN Configuration > QinQ Configuration > QinQ Port Setting	40
41	VLAN Configuration > QinQ Configuration > QinQ Tunnel Setting	40
42	Trunking	41
43	Trunking > Aggregator Setting	41
44	Trunk Group Table	42
45	Trunking > Static Activity	42
46	Forwarding and Filtering	43
47	Forwarding and Filtering > Dynamic MAC Table	43

48	Forwarding and Filtering > Static MAC Table	44
49	Forwarding and Filtering > MAC Filtering	44
50	IGMP Snooping	45
51	Configure Spanning Tree Parameters	46
52	Spanning Tree > System Configuration	46
53	Spanning Tree > PerPort Configuration	47
54	Spanning Tree > Instance	48
55	Spanning Tree > Interface	48
56	DHCP Relay & Option 82	49
57	DHCP Option 82 > Relay IP	50
58	Access Control List	50
59	Access Control List > IPv4	51
60	Access Control List > Non-IPv4	52
61	Access Control List > Binding	52
62	Access Control List > QoS VoIP	53
63	QoS VoIP Options	53
64	Security Manager	54
65	MAC Limit	54
66	802.1x Configuration	55
67	802.1x Configuration > PerPort Configuration	56
68	802.1x Configuration > Misc Configuration	56
69	QoS Configuration	57
70	QoS Configuration > PerPort Configuration	58
71	ToS/DSCP Configuration	58
72	Left-side panel navigation	59
73	Port Status	59
74	Port Statistics	60
75	Profile Setting > Configuration	61
76	Profile Setting > Profile Table	62
77	Reset System	62
78	Reboot Switch System	63
79	Login screen	65
80	Login complete	66
81	Help information screen	66
82	Configuration mode	67



## List of Figures

---

1	General conventions .....	13
2	FF3210P Connectors .....	18
3	LED Indicators .....	18
4	Pin Assignment .....	19
5	L4 Protocol .....	52
6	Port Status Options .....	59
7	Port Statistics Options .....	60
8	VDSL Profile Options .....	61
9	Profile Setting Options .....	62
10	Default Settings .....	65
11	Major Commands .....	66
12	Configurations .....	67

# About This Guide

---

This guide describes the ForeFront 3210P VDSL2 IP Switch hardware, installation and basic configuration.

## Audience

---

This guide is intended for the following users:

- Operators
- Installers
- Maintenance technicians

## Structure

---

This guide contains the following chapters and appendices:

- [Chapter 1](#) on page 14 provides information about the ForeFront 3210P features and capabilities
- [Chapter 2](#) on page 20 provides information about configuring the ForeFront for the web
- [Chapter 3](#) on page 56 provides information about configuring the ForeFront for a console
- [Chapter 4](#) on page 96 provides information on contacting Patton technical support for assistance
- [Appendix A](#) on page 99 provides compliance information for the ForeFront 3210P
- [Appendix B](#) on page 101 provides specifications for ForeFront 3210P

For best results, read the contents of this guide *before* you install the ForeFront 3210P.

## Precautions

Notes, cautions, and warnings, which have the following meanings, are used throughout this guide to help you become aware of potential problems. *Warnings* are intended to prevent safety hazards that could result in personal injury. *Cautions* are intended to prevent situations that could result in property damage or impaired functioning.

**Note** A note presents additional information or interesting sidelights.



IMPORTANT

The alert symbol and IMPORTANT heading calls attention to important information.



CAUTION

The alert symbol and CAUTION heading indicate a potential hazard. Strictly follow the instructions to avoid property damage.



CAUTION

The shock hazard symbol and CAUTION heading indicate a potential electric shock hazard. Strictly follow the instructions to avoid property damage caused by electric shock.



CAUTION

**The alert symbol and WARNING heading indicate a potential safety hazard. Strictly follow the warning instructions to avoid personal injury.**



CAUTION

**The shock hazard symbol and WARNING heading indicate a potential electric shock hazard. Strictly follow the warning instructions to avoid injury caused by electric shock.**

## Safety When Working with Electricity



- Do not open the device when the power cord is connected. For systems without a power switch and without an external power adapter, line voltages are present within the device when the power cord is connected.
- For devices with an external power adapter, the power adapter shall be a listed *Limited Power Source*. The mains outlet that is utilized to power the device shall be within 10 feet (3 meters) of the device, shall be easily accessible, and protected by a circuit breaker in compliance with local regulatory requirements.
- For AC powered devices, ensure that the power cable used meets all applicable standards for the country in which it is to be installed.
- For AC powered devices which have 3 conductor power plugs (L1, L2 & GND or Hot, Neutral & Safety/Protective Ground), the wall outlet (or socket) must have an earth ground.
- For DC powered devices, ensure that the interconnecting cables are rated for proper voltage, current, anticipated temperature, flammability, and mechanical serviceability.
- WAN, LAN & PSTN ports (connections) may have hazardous voltages present regardless of whether the device is powered ON or OFF. PSTN relates to interfaces such as telephone lines, FXS, FXO, DSL, xDSL, T1, E1, ISDN, Voice, etc. These are known as "hazardous network voltages" and to avoid electric shock use caution when working near these ports. When disconnecting cables for these ports, detach the far end connection first.
- Do not work on the device or connect or disconnect cables during periods of lightning activity



**This device contains no user serviceable parts. This device can only be repaired by qualified service personnel.**



In accordance with the requirements of council directive 2002/96/EC on Waste of Electrical and Electronic Equipment (WEEE), ensure that at end-of-life you separate this product from other waste and scrap and deliver to the WEEE collection system in your country for recycling.



Always follow ESD prevention procedures when removing and replacing cards.

Wear an ESD-preventive wrist strap, ensuring that it makes good skin contact. Connect the clip to an unpainted surface of the chassis frame to safely channel unwanted ESD voltages to ground.

To properly guard against ESD damage and shocks, the wrist strap and cord must operate effectively. If no wrist strap is available, ground yourself by touching the metal part of the chassis.

### General Observations

- Clean the case with a soft slightly moist anti-static cloth
- Place the unit on a flat surface and ensure free air circulation
- Avoid exposing the unit to direct sunlight and other heat sources
- Protect the unit from moisture, vapors, and corrosive liquids


## Typographical Conventions Used in this Document

This section describes the typographical conventions and terms used in this guide.

### General Conventions

The procedures described in this manual use the following text conventions:

Table 1. General conventions

Convention	Meaning
Garamond blue type	Indicates a cross-reference hyperlink that points to a figure, graphic, table, or section heading. Clicking on the hyperlink jumps you to the reference. When you have finished reviewing the reference, click on the <b>Go to Previous View</b> button  in the Adobe® Acrobat® Reader toolbar to return to your starting point.
<b>Futura bold type</b>	Commands and keywords are in <b>boldface</b> font.
<b><i>Futura bold-italic type</i></b>	Parts of commands, which are related to elements already named by the user, are in <b>boldface italic</b> font.
<i>Italicized Futura type</i>	Variables for which you supply values are in <i>italic</i> font
Futura type	Indicates the names of fields or windows.
<b>Garamond bold type</b>	Indicates the names of command buttons that execute an action.
< >	Angle brackets indicate function and keyboard keys, such as <SHIFT>, <CTRL>, <C>, and so on.
[ ]	Elements in square brackets are optional.
{ a   b   c }	Alternative but required keywords are grouped in braces ( { } ) and are separated by vertical bars (   )
screen	Terminal sessions and information the system displays are in <i>screen</i> font.
<b>node</b>	The leading IP address or nodename of a BODi rS is substituted with <b>node</b> in <b>boldface italic</b> font.
<b>SN</b>	The leading <b>SN</b> on a command line represents the nodename of the BODi rS
#	An hash sign at the beginning of a line indicates a comment line.

# Chapter 1 **General Information**

## **Chapter contents**

ForeFront 3210P VDSL2 IP Switch Overview .....	15
Network Features .....	15
ForeFront 3210P VDSL2 IP Switch Panels .....	18
LED Indicators .....	18
Reset Button .....	18
Pin Assignment of RJ21 Cable .....	19

## ForeFront 3210P VDSL2 IP Switch Overview

Patton's ForeFront 3210P VDSL2 IP Switch presents the ideal and efficient solution for Telecom, ISP (Internet Service Provider), or SI (System Integration) with 24-port VDSL2 and 2-port gigabit Ethernet combo interfaces (TP and SFP) in the 1.5U height design. The ForeFront 3210P VDSL2 IP Switch offers the benefits of high speed connectivity with an efficient management system, robust layer 2 features with advanced security system, and reliable hardware design with monitoring system.



Figure 1. ForeFront 3210P VDSL2 IP Switch

### Network Features

The ForeFront 3210P VDSL2 IP Switch includes the following key features:

- 24 10/100BaseX Ethernet ports and 2 10/100/1000BaseX Ethernet ports Ethernet switch controller
- Supports SMII or SS-SMII for 10/100BaseX ports
- Supports GMII/MII/TBI for 10/100/1000BaseX ports
- All packet buffer and control data memory embedded
- Flow control support
  - 802.3x pause frame used for full-duplex ports
  - Collision-based back-pressure for half-duplex ports, carrier-based back-pressure not supported
- Half- and full-duplex operations
  - Full-duplex operation supported on 10/100/1000 Mbps ports
  - Half-duplex operation supported on 10/100 Mbps ports only
- Supports 802.1D bridge self-learning, storing up to 8K+ 256 unicast or multicast addresses
- Supports automatic age-out period between 1 to 1,000,000 seconds
- Broadcast storm filtering based on ingress port bandwidth
- HOL blocking prevention
- Deadlock relief
- Auto-polling via MDC/MDIO management interface for auto-configuration of speed, duplex mode, and flow control capability of all Ethernet ports
- 9K+ jumbo packets supported on per port and per VLAN basis
- Supports layer 2 source filtering
- Supports 802.1D Spanning Tree Algorithm and Protocol, and 802.1w Rapid Reconfiguration

- Flexible per-port VLAN classification option supports port-based VLAN domain and 802.1Q VLAN domain simultaneously
- Supports Independent VLAN Learning (IVL) and Shared VLAN Learning (SVL)
- Supports 802.1X Port-based Network Access Control
- Supports 802.3ad Aggregation of Multiple Link Segments
  - Statistical load-balancing algorithm may be configured to be function of source and destination MAC addresses, ingress port ID, source and destination IP addresses, and TCP/UDP source and destination ports
- Supports BPDU, LACP, EAPOL suppression based on per port configuration
- Supports 64 VLAN-dependent Spanning Trees
- Supports IP multicast and snooping of IGMP and IP multicast routing protocol PDU
  - Including IGMP, CBT, OSPF, and PIM v2
- IP multicast packets may be forwarded within single VLAN or across multiple VLANs
  - Cross-VLAN mode allows each egress port to have its own tag rule and VID for IP multicast packets
- Port mirroring
- Supports 802.1p Traffic Priority
- ToS-to-802.1p priority mapping is enabled on per-VLAN basis
- Flexible per-port prioritization option
  - The prioritization result can be made available to other switches in the network by replacing priority field in VLAN tag
- Four priority egress queues per port
- Scheduling algorithms: strict priority or weighted round robin
- Four RMON groups (1,2,3,9)
- Supports MIB of RFC1213, 1573, 1757, 1643, 2233
- Programmable LED output provides
  - Serial LED output provides basic status of all Ethernet ports, or
  - Port 24/25 link status and broadcast storm indicator
- MAC address table synchronization assistance
- Asymmetric VLAN membership for better network security
  - Distinguish ingress VLAN member and egress VLAN member
  - Prevents a station to sneak in VLANs set up for common servers
- Improved VLAN ingress rules may specify
  - Filtering untagged packets or VLAN tagged packets



- Filtering packets received on non-ingress VLAN member ports
- Supports insertion of 2nd tag with different TPID to VLAN-tagged packets
- Port-based ingress rate policing and egress rate pacing
- Supports Layer 2/3/4 (Layer 2+) classification
  - Standard-length IPv4 packets can use layer 2 VLAN-tag ID, IP protocol, Source IP, Destination IP, TCP/UDP Destination Port and Source Port, and TCP SYN field for classification
  - Non-standard or non-IPv4 packets use part of layer 2/3 header for classification
  - Up to 256 different classification rules supported
  - Each classification rule is associated with an action code
  - Packet and byte counters for all classification rules to record match statistics
- Supports Layer 2+ based VLAN classification scheme
  - IP subnet based and Protocol-based VLAN achievable by means of layer 2+ classification
  - May override VID in VLAN-tag
- Supports filtering, redirecting, and/or mirroring of packets based on Layer 2+ classification result
  - Redirects IPv6 packets to IPv6-capable network devices
- SMAC/SIP bindings for IPv4 packets can be implemented
- Layer 2+ packet classification result may be used to define packet priority
- Priority adjustment based on per port profile and per VLAN property
  - Priority of a packet can be upgraded or downgraded based on setting of the ingress port and VLAN
- Supports protected port, protected port group, and unprotected port group
- VID in transmitted packets can be replaced by a fixed VID associated with the egress port
  - The VID to be swapped in by egress port can be different than the default VID for untagged ingress packets
- CPU interface: alternatively
  - 32-bit 33 MHz PCI interface
  - 16-bit PIO interface with three DMA controllers
- Programmable byte-swap capability for MIB counter memory access
- Programmable event triggered interrupts allowing software to respond to or ignore an array of exceptions
- 332-ball PBGA package
- 1.8V core and SRAM voltage, and 3.3V pad voltage

## ForeFront 3210P VDSL2 IP Switch Panels

Table 2. FF3210P Connectors

LED	Description
<b>Power</b>	The connector is for 100V ~ 240V AC power inputs (50Hz~60Hz, 1.5A).
<b>GE1 &amp; GE2</b>	For connecting Gigabit Ethernet, ForeFront 3210P provide Gigabit Ethernet combo interfaces, TP and SPF. <b>TP:</b> 10/100/1000 BaseT copper (RJ-45 connector). <b>SFP:</b> 1000 Base-SX/LX mini-GBIC slot.
<b>Console</b>	Users are able to access ForeFront 3210P locally with <b>CONSOLE</b> port. Via <b>CONSOLE</b> , users are able to configure ForeFront 3210P with menu-driven interface with any terminal emulation program, such as, Hyperterminal and Teraterm. (115200, 8, None, 1, None)
<b>Alarm</b>	For alarm inputs and outputs.
<b>Line</b>	Line is for connecting 24 VDSL2 ports with a Telco-50/RJ-21 cable.
<b>Pots</b>	Includes 24 build-in splitters, POTS, with a Telco-50/RJ-21 cable for telephone services.

### LED Indicators

Table 3. LED Indicators

LED	Blinking	On	Off
<b>VDSL Link (1 ~ 24)</b>	VDSL2 Link is active (transmitting data or training)	VDSL2 Link is ready	Link is down
<b>Run/Alarm</b>	Indicates system boot-up	Green: Alarm is detected Red: Alarm	
<b>GE1/ GE2</b>	Transmitting data	10/100/1000Mbps	Link is down
<b>Link/ ACT</b>	Transmitting data	10/100/1000Mbps	Link is down
<b>Speed</b>	Transmitting data	10/100/1000Mbps	Link is down

### Reset Button

The reset button allows users to reboot the VDSL2 IP Switch or load the default setting. Press and hold the reset button for one to five seconds to reboot the IP Switch. Press and hold the reset button for over five seconds to load the default settings.

**Note** All user settings will be lost after restoring the factory default settings. Backing up the configuration regularly is strongly recommended.

## Pin Assignment of RJ21 Cable

Table 4. Pin Assignment

Pin	Color	Port	Pin	Color	Port	Pin	Color	Port
1	Black	P24	9	White	P16	17	White	P8
26	Orange		34	Brown		42	Gray	
2	Black	P23	10	White	P15	18	Red	P7
27	Blue		35	Green		43	Blue	
3	Red	P22	11	White	P14	19	Red	P7
28	Gray		36	Orange		44	Orange	
4	Red	P21	12	White	P13	20	Red	P5
29	Brown		37	Blue		45	Green	
5	Red	P20	13	White	P12	21	Red	P4
30	Green		38	Blue		46	Brown	
6	Red	P19	14	White	P11	22	Red	P3
31	Orange		29	Orange		47	Gray	
7	Red	P18	15	White	P10	23	Black	P2
62	Blue		40	Green		48	Blue	
8	White	P17	16	White	P9	24	Black	P1
33	Gray		41	Brown		49	Orange	

## Chapter 2 **Web Configuration**

### **Chapter contents**

Introduction .....	22
Connecting to the Web Management System .....	22
Administration .....	23
IP Address .....	23
Switch Setting .....	23
Basic .....	24
Module Info .....	24
Misc Config .....	24
Console Port Information .....	25
Port Configuration .....	25
Port Controls .....	26
Port Sniffer .....	27
Protected Port .....	27
VDSL Port Status .....	28
SNMP Configuration .....	29
System Options .....	29
Community Strings .....	29
Trap Manager .....	30
SNMPv3 Group .....	30
SNMPv3 View .....	30
SNMPv3 Access .....	31
SNMPv3 USM-user .....	31
Syslog Setting .....	32
Alarm Configuration .....	33
Temperature & Fan Status .....	33
Firmware Update .....	33
Configuration Backup .....	34
TFTP Restore Configuration .....	34
TFTP Backup Configuration .....	34
SNTP Settings .....	35
L2 Features .....	35
VLAN Configuration .....	36
Static VLAN .....	36
GVRP VLAN .....	38
QinQ VLAN .....	39
Trunking .....	41
Aggregator Setting .....	41
Aggregator information .....	42
Static Activity .....	42

Forwarding & Filtering .....	43
Dynamic MAC Table .....	43
Static MAC Table .....	44
MAC Filtering .....	44
IGMP Snooping .....	44
Spanning Tree .....	45
System Configuration .....	46
PerPort Configuration .....	47
Instance .....	48
Interface .....	48
DHCP Relay & Opt. 82 .....	48
DHCP Option 82 .....	49
DHCP Relay .....	49
DHCP Option 82 Router Port .....	49
DHCP Opt. 82 Port Table .....	49
ACL (Access Control List) .....	50
IPv4 .....	51
Non-IPv4 .....	52
Binding .....	52
QoS VoIP .....	53
Security .....	53
Security Manager .....	53
MAC Limit .....	54
Configure MAC Limit .....	54
MAC Limit Port Status .....	54
802.1x Configuration .....	54
System Configuration .....	55
PerPort Configuration .....	55
Misc Configuration .....	56
QoS .....	57
QoS Configuration .....	57
QoS Configuration - Priority Queue Service .....	57
PerPort Configuration .....	57
ToS/DSCP .....	58
Monitoring .....	59
Port Status .....	59
Port Statistics .....	60
VDSL .....	61
Configuration .....	61
Profile Table .....	62
Reset System .....	62
Reboot .....	63

## Introduction

The contents of this chapter explain how to manage and change configuration options for the ForeFront 3210P VDSL2 IP Switch using your web browsers. Users are able to login to the **Web Management System** with any standard web browser, such as Internet Explorer, Firefox, etc.

## Connecting to the Web Management System

To login to the **Web Management System**:

1. Start a web browser on a computer that is connected to the VDSL2 IP Switch.
2. Enter the following default IP address in the address field of the web browser: **http://192.168.0.100**
3. Enter the username **admin** and password **admin** to login to the Web Management System. This is the default username and password of the VDSL2 IP Switch.
4. After successfully logging in, the **Home Page** of the Web Management System displays as the following:



Figure 2. Web Management System home page

**Note** Verify that the IP address is correct once the IP of the management website is changed.

## Administration

This section allows users to manage the VDSL2 IP Switch, including the IP address, switch settings, etc. Navigate to the **Administration** section from the Menu box on the left-hand side of your screen.

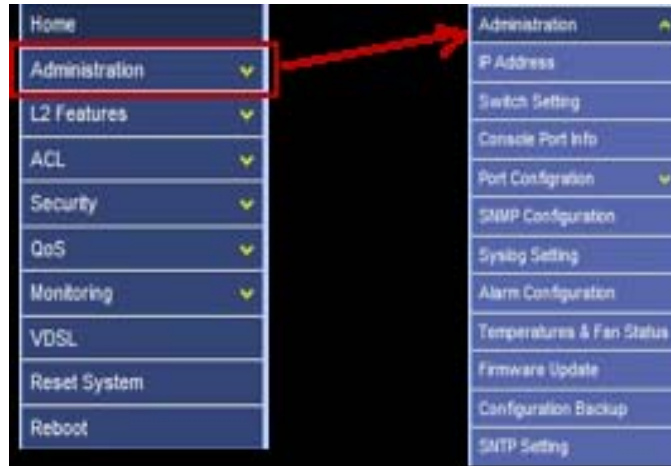


Figure 3. Administration navigation

### IP Address

The IP Address Setting includes four configuration options:

- DHCP mode
  - Disable or enable DHCP mode. The value of this mode will decide whether the IP address is a static IP address or a dynamic IP address.
- IP address
- Subnet mask
- Default gateway

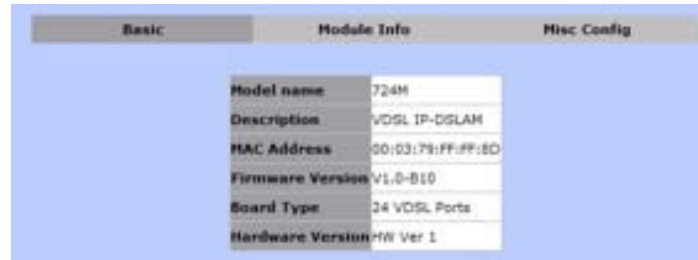
Figure 4. IP Address Setting

### Switch Setting

The Switch Setting presents information of the switch in the following sub-functions.

### Basic

The Basic tab includes the following information: model name, description, MAC address, firmware version, board type and hardware version.



Model name	724M
Description	VDSL IP-DGLAM
MAC Address	00:03:19:FF:FF:8D
Firmware Version	V1.0-B10
Board Type	24 VDSL Ports
Hardware Version	HW Ver 1

Figure 5. Switch Setting > Basic

### Module Info

The Module Info tab includes the uplinks, Gigabit Ethernet 1 and Gigabit Ethernet 2. (These two uplinks will be called Module1 and Module2.)



TYPE	DESCRIPTION
Module1	GIGA COMBO
Module2	GIGA COMBO

Figure 6. Switch Setting > Module Info

### Misc Config

The Misc Config tab is the only section which allows users to change the settings of the switch.



Figure 7. Switch Setting > Misc Config

- **MAC address age-out time:** This value sets up how many seconds that an inactive MAC address remains.



- **Turn on port interval:** This value sets up the time interval to enable the CPU port after flooding attacks (0 means never enable the CPU port).
- **Broadcast storm filter mode:** This feature sets up the threshold value of broadcast traffic for ports.
  - Options: off, 1/2, 1/4, 1/8 or 1/16 (the value is the percentage of the port's ingress bandwidth used by broadcast traffic).
- **Broadcast storm filter packets select:** This option allows users to choose the type of target packet for broadcast storm filter mode.
  - If no type is chosen, the broadcast storm filter mode is off.
  - Options: broadcast packets, IP multicast, control packets, and flooded unicast/multicast packets.
- **Collisions retry forever:** This function allows users to choose how many times the IP switch should retry when a packet meets a collision.
  - Disable, 16, 32 or 48 collision number; when the function is disabled, the IP switch will retry six times before packets are dropped. Otherwise, it will retry continuously until the packet is sent successfully.
- **Hash algorithm:** This option is for choosing a hash algorithm for the MAC address table.
  - CRC-Hash or DirectMap.
- **IP/MAC binding:** This feature allows users to enable or disable the IP/MAC binding function.
- **802.1x protocol:** Enable or disable 802.1x protocol via this option.

**Note** Users are able to save the modified settings by clicking **Apply**, or restore the default settings by clicking **Default**. Clicking **Help** will open another window with information about the features.

### Console Port Information

This section allows users to review the settings of the Console port. Users can connect and manage the VDSL2 IP switch in Command Line Interface (CLI) mode.



Figure 8. Console Information

### Port Configuration

The Port Configuration includes the following four functions of the VDSL2 ports and Gigabit Ethernet ports.

## Port Controls

Port	State	Negotiation	Speed	Duplex	Flow Control	Rate Control (Max: 128Kbps)	Security BSF	Jumbo Frame
Mod1	On	Auto	1000	Full	On	Off	On	On

Figure 9. Port Configuration > Port Control

Users can set up the details of Gigabit Ethernet ports and trunking ports (if trunking ports exist). The following configuration options are available:

- **State:** This option will enable or disable the selected port.
  - Disable will turn off the selected port; therefore, no traffic will be going through this port.
- **Negotiation:** Users can decide whether Gigabit Ethernet ports should be auto-negotiable or not.
  - Options: auto or force. (If *force* mode is selected, users must provide the *Speed* and *Duplex*.)
- **Speed:** Users can set up the speed of Gigabit Ethernet ports in this function.
  - 10, 100 or 1000
- **Duplex:** Half or Full
- **Flow Control**
  - Enable: sends a *PAUSE* signal to the sender and halts traffic for a period of time.
  - Disable: drops the extra packets when there are too many packets to process.
- **Rate Control:** Users can set up the specific rate for both ingress and egress ports. Therefore, the VDSL2 IP switch will control the rate to meet the specified rate. (The valid rate range is 0-8000, and the unit is 128Kbps.)
- **Security:** This function decides whether the IP switch will forward all incoming packets from both secure MAC addresses and unknown MAC addresses.
  - Enable: only packets from secured MAC addresses will be forwarded.
  - Disable: all packets will be forwarded.
- **BSF (*Broadcast Storm Filtering*):** Users can enable or disable this function by port.
- **Jumbo Frame:** Users can choose whether the IP switch forwards jumbo frame packets or not.

### Port Sniffer

The Port Sniffer function monitors a target port by mirroring or copying the data of the port and forwarding to an assigned port.



Figure 10. Port Configuration > Port Sniffer

1. In the **Sniffer Type** drop-down menu, choose which type of data to monitor: **Disable**, **Rx**, **Tx**, or **Both**.
2. In the **Analysis Port** drop-down menu, assign which port should receive the data. (The analysis port will accept only copied packets from the monitored port.)
3. Choose which port to monitor by clicking the circle in the **Monitor** column with the corresponding **Port** number.

### Protected Port

This function isolates a protected port from its neighbor ports and other ports in different protected groups. However, protected ports can communicate with other unprotected ports. Setting up protected ports ensures that there is no traffic (such as unicast, broadcast, or multicast) between protected ports on the VDSL2 IP Switch.



Figure 11. Port Configuration > Protected Port Setting

Users may select from two protected port groups and assign ports to either **Group 1** or **Group 2**. Click on the corresponding checkbox and radial button to select which ports are **Protected** and their **Group**.

### VDSL Port Status

This status allows users to monitor current information of each VDSL port, such as status, upstream rate, downstream rate, SNR margins for upstream and downstream and firmware version.

Figure 12. Port Configuration > VDSL Port Status

To view detailed information for a specific port, click on **Advance** in the corresponding row to open the following window:

Figure 13. Detailed VDSL Port Status

## SNMP Configuration

SNMP, or *Simple Network Management Protocol*, is a standard protocol for managing network devices. SNMP is commonly used in Network Management Systems (also known as NMS) to monitor network devices. In addition, MIBs (Management Information Bases) is a file which is used to store all data of managed network devices in NMS according to SNMP standard protocols.

Figure 14. SNMP Configuration

VDSL2 IP Switch supports three versions of SNMP: SNMPv1, SNMPv2c and SNMPv3. In the SNMP Configuration page, the following sections are included.

### System Options

System Options includes the **name** and **location** of the VDSL2 IP Switch, the **contact** information of a person or organization and the **SNMP Status** enable/disable function.

Figure 15. SNMP Configuration > System Options

### Community Strings

Follow these instructions to set up the password for accessing the SNMP system.

1. View the existing password strings in the **Current Strings** column.
2. In the **New Community String** column, enter a new **String** (password).
3. Choose the **RO** (read only) or **RW** (read and write) option.
4. Click **Add** to add the new information to the community list.
5. Click **Remove** to remove a password from the community list.

Figure 16. SNMP Configuration > Community Strings

### Trap Manager

Follow these instructions to add or remove a New Trap Manager.

1. View the existing SNMP servers in the **Current Managers** column.
2. Add new trap manager information in the **New Manager** column.
3. Enter the **IP Address** and the **Community** (password for accessing the trap manager) of the new trap manager.
4. Click **Add** to add the new manager
5. Click **Remove** to remove information of an existing manager.



Figure 17. SNMP Configuration > Trap Managers

### SNMPv3 Group

Follow these instructions to add or remove SNMPv3 groups.

1. View the current list of SNMPv3 groups in the **Current Strings** column.
2. Add a new group in the **SNMP Group** column
3. Enter the **Group Name**, the security model (**V1/V2/USM**) and the **Security Name** of the group.
4. Click **Add** to add the new SNMPv3 Group.
5. Click **Remove** to remove an existing SNMPv3 Group.



Figure 18. SNMP Configuration > SNMPv3 Group

### SNMPv3 View

Follow these instructions to offer or deny access of the complete or partial features of the VDSL2 IP Switch.

1. View the current SNMPv3 accesses in the **Current Strings** column.
2. Add a new SNMPv3 View in the **SNMP View** column.
3. Enter the **View Name**; whether the OID should be **Included/Excluded** from the SNMP view; the **Sub-tree** of this view; and the subnet **Mask** of this view.
4. Click **Add** to add the new SNMPv3 View.

- Click **Remove** to remove a selected SNMPv3 View from the **Current Strings** table.



Figure 19. SNMP Configuration > SNMPv3 View

### SNMPv3 Access

The SNMPv3 Access section is for managing SNMPv3 access control, which is different from the access control defined by SNMPv1 and SNMPv2. SNMPv3 access sets up SNMP access levels based on contexts, groups and users, rather than on IP addresses and community strings.



Figure 20. SNMP Configuration > SNMPv3 Access

Follow these instructions to add or remove SNMPv3 access.

- View the current SNMPv3 access list in the **Current Strings** column.
- Add new SNMPv3 access controls in the **SNMP Access** column.
- Enter the **Group Name** of the new SNMPv3 access group.
- In the **V1/V2c/USM** drop-down menu, choose a security model. **V1** is reserved for SNMPv1, **V2c** is reserved for SNMPv2c and **USM** is a user-based security model.
- In the **SNMP Access** drop-down menu, choose a security model (*NoAuth/Auth/Authpriv*). **NoAuth** permits no authentication and no privacy; **Auth** permits authentication and no privacy; and **Authpriv** permits both authentication and privacy.
- Choose whether this access group will have **Read View**, **Write View** and **Notify View**.
- Click **Add** to add the new SNMPv3 access group.
- Click **Remove** to remove an access from the **Current Strings** list.

### SNMPv3 USM-user

The SNMPv3 USM-user section is for setting up the details of the USM (User-based Security Model). The USM provides different types of security levels using various authentication and privacy protocols.

Follow these instructions to add or remove a new USM user.

1. View the current SNMPv3 USM-user in the **Current Strings** column.
2. Add a new USM user in the **SNMP USM-user** column.
3. Enter the **SNMP User Name** of the new USM user, the **Auth Type** (none or md5), the **Auth Key** password of the USM user and the **Private Key** password for the privacy protocol type.
4. Click **Add** to add the new SNMPv3 USM-user.
5. Click **Remove** to remove a SNMPv3 USM-user from the current list.

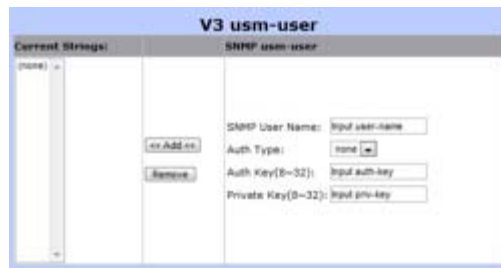


Figure 21. SNMP Configuration > SNMPv3 USM-user

### Syslog Setting

The Syslog function is supported in this VDSL2 IP Switch system. The system will send logs to a remote log system, and then three events will be reported to the remote log system—**cold start**, **warm start** and **link change**. To connect to the remote syslog server, the following information must be entered:

- **Syslog server IP:** The IP address of the remote syslog server IP.
- **Log level options**
  - **None:** never send syslog message to syslog server.
  - **Major:** only send major syslog message to syslog server.
    - Link up or down
    - System warm start or cold start
  - **All:** send all syslog messages to syslog server.



Figure 22. Syslog Setting



## Alarm Configuration

Alarm Configuration is distinguished into two tables—Configure Alarm Information and Alarm Information. Users are able to set up alarms and monitor each alarm status.

Alarm Item	Admin	Security	Title
Alarm1	Enable	Minor	
Alarm2	Disable	Critical	
Alarm3	Disable	Critical	

Alarm Item	Admin	Security	Title	Status
Alarm1	Enable	Minor		Clear
Alarm2	Disable	Critical		
Alarm3	Disable	Critical		

Figure 23. Alarm Configuration

- **Alarm Item:** There are a total of four alarms that can be set in the VDSL2 IP Switch
- **Admin:** Option to disable or enable
- **Security:** The level of the alarm
- **Title:** The name of the alarm

## Temperature & Fan Status

The Temperatures & Fan Status allows the user to monitor the real-time information of the VDSL2 IP Switch temperature and fan speed.

Temperature Local	54 C
Temperature Remote 1	51 C
Temperature Remote 2	53 C
Fan1 Status	Medium Speed
Fan2 Status	Medium Speed
Fan3 Status	Medium Speed

Figure 24. Temperature and Fan Information

## Firmware Update

This function allows users to upgrade firmware through TFTP or HTTP.

Figure 25. Firmware Update

## Configuration Backup

Users can load or backup configurations by using the **Configuration Restore** function, which includes two tabs for performing this function.

Figure 26. Configuration Restore

### TFTP Restore Configuration

This tab allows the user to upload the settings from a configuration file by TFTP or HTTP.

Figure 27. Configuration Restore > TFTP Restore Configuration

### TFTP Backup Configuration

This tab allows users to download the current configuration through TFTP or HTTP.

Figure 28. Configuration Restore > TFTP Backup Configuration

## SNTP Settings

The SNTP, or *Simple Network Time Protocol*, is a system for synchronizing the clocks of network computer systems. By enabling this function, users are able to configure this switch to send time synchronization requests to the assigned servers' IP addresses.



Figure 29. SNTP Settings

Follow these instructions to enable this function:

1. In the SNTP section, choose **Enable** from the drop-down menu.
2. Enter the **IP address** of the assigned SNTP server in the **SNTP Server IP** section.
3. Choose the time zone via the **UTC Type**.
  - **After-UTC:** UTC plus hh (hours); for example, Taipei (UTC+08) choose After-UTC.
  - **Before-UTC:** UTC minus hh (hours); for example, San Francisco (UTC-08) choose Before-UTC
4. Enter a numerical hour in the **Time Range** field for setting up the hour data for the UTC-hh/UTC+hh.
  - For example, UTC-08, choose Before-UTC and 8 in the Time Range field.
5. The **Time** section displays the current time once the switch is connected to the assigned NTP server.

## L2 Features

This section outlines the VDSL2 IP Switch flexible L2 features, which are outlined as the following features:

- VLAN Configuration
- Trunking
- Forwarding & Filtering
- IGMP Snooping
- Spanning Tree
- DHCP Relay & Opt.82

## VLAN Configuration

The Virtual Local Area Network, or virtual LAN is a concept of separating and grouping LAN segments by a common set of requirements. VLAN presents benefits such as, simplifying network design, enhancing bandwidth performance and improving, etc.



Figure 30. VLAN Configuration

The VDSL2 IP Switch supports three types of VLAN Algorithms, which are each described in the sections below.

### Static VLAN

The Static function allows users to setup and manage VLAN groups manually.



Figure 31. VLAN Configuration > Static VLAN

- The VLAN Operation Mode has three options:
  1. Choose **No VLAN** to disable VLAN mode
  2. Choose **Port-Based VLAN** to setup VLAN groups by ports
  3. Choose **802.1Q VLAN** to setup VLAN groups by 802.1Q VLAN tags

- The **Basic** tab contains the VLAN Information, which displays all VLAN groups currently stored. Follow these instructions to manage VLAN groups.



Figure 32. VLAN Configuration > Static VLAN > Basic

**Note** The VLAN mode of VLAN operation mode is the global setting of *Basic* and *VLAN Filter*.

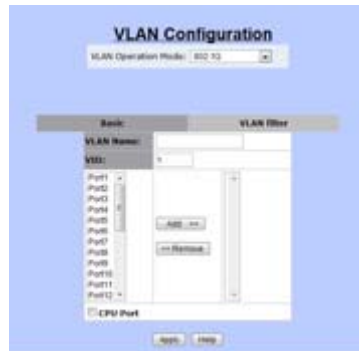


Figure 33. VLAN mode

1. Click **Add** to create a new VLAN group.
2. The group must include a **VLAN Name**, **VLAN ID (VID)**, **VLAN Members (Ports)** and whether to check the **CPU Port** box to choose this VLAN group as the management group of this VDSL2 IP Switch.
3. Click **Apply** to set up tag mode for each **TagMember** (Port).



Figure 34. Create a VLAN group

4. Choose **Edit** to change the settings of an existing VLAN group.
5. Choose **Delete** to remove an existing VLAN group.
6. Choose **PrePage** to move to the previous page of VLAN information table.

7. Choose **NextPage** to move to the following page of VLAN information table.
  8. Choose **Help** to open an FAQ page of VLAN configuration.
- The **VLAN filter tab** allows the user to set and define the filtering rules for each port. Follow these instructions to define and manage each port.

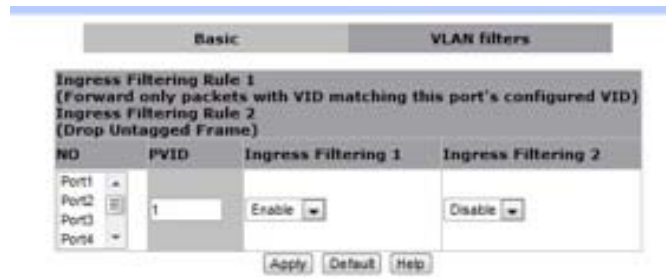


Figure 35. VLAN Configuration &gt; Static VLAN &gt; VLAN filters

1. Locate the list of available ports in the **NO** column. Click on the **port** to change the details; a new table will open.

NO	PVID	Ingress Filtering 1	Ingress Filtering 2
Hw01	1	ENABLE	DISABLE

Figure 36. VLAN filter table

2. In this table, the **PVID** column displays the VLAN ID of ingress packets. (Two filtering rules are available in the VLAN Filtering function of this VDSL2 IP Switch.)
3. **Enable** the **Ingress Filtering 1** function to only allow these ingress packets with an assigned VLAN ID to pass through this port. Choose **Disable** to stop the filtering function.
4. **Enable** the **Ingress Filtering 2** function to drop all untagged packets and only allow packets with the assigned VLAN ID to pass through this port. Choose **Disable** to accept all packets.

### GVRP VLAN

The Generic Attribute Registration Protocol (GVRP) method follows IEEE 802.1Q specification and defines tagging frames with VLAN configuration data. This allows VDSL2 IP switch to exchange VLAN configuration information with other network devices dynamically.

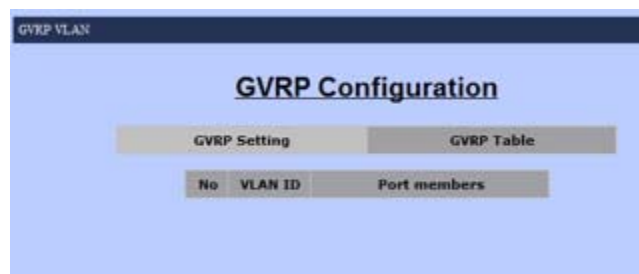


Figure 37. VLAN Configuration &gt; GVRP Configuration

Follow these instructions to set up GVRP configurations:

1. The **GVRP Setting** tab allows the user to configure settings.



Figure 38. VLAN Configuration > GVRP Configuration > GVRP Settings

2. Choose to **Enable** or **Disable** the GVRP function
3. Choose the corresponding checkbox of the **Port** to choose as a **GVRP** group member.
4. Click **Apply** to save the modifications, or **Default** to restore the default settings.
5. Click **Help** to open the FAQ page of the GVRP VLAN.
6. The **GVRP Table** tab displays the current VLAN ID and its group member information. The GVRP will learn this information automatically (see [Figure 37](#)).

### QinQ VLAN

This function allows users or service providers to separate traffic service for different customers by adding service provider VLAN tags and customer VLAN IDs. In this function, the settings are divided into two parts—QinQ Port Settings and QinQ Tunnel Settings.



Figure 39. VLAN Configuration > QinQ Configuration

- **QinQ Port Setting** tab is for setting up QinQ mode, TPID and group members. Follow these instructions to manage the QinQ Port settings:

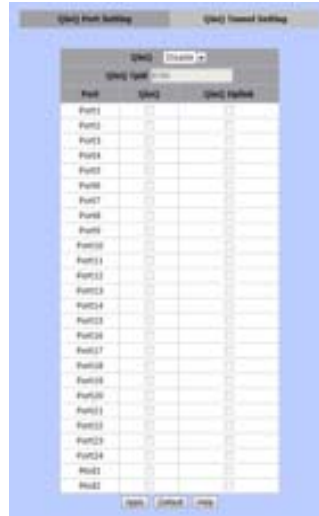


Figure 40. VLAN Configuration > QinQ Configuration > QinQ Port Setting

1. **Enable** or **Disable** the QinQ function.
2. Enter the **QinQ TPID** (Tag Protocol Identifier) number.
  - TPID is the Ethertype value for 802.1Q encapsulation
  - Standard Ethertype value: 0x8100 (default value)
  - Range: 0x0800 - 0xFFFF (hexadecimal value)
3. Choose which port should be enabled with **QinQ** mode by clicking the corresponding checkbox.
4. Choose which port should be set up with a **QinQ Uplink** port of this QinQ group by clicking the corresponding checkbox.

- **QinQ Tunnel Setting** tab is for service providers who carry traffic of multiple customers across their networks and are required to maintain VLAN and Layer 2 protocol configurations for each customer. This requires a **Tunnel ID**, **Tunnel VID** and choosing a **Port List** (user port and uplink port).



Figure 41. VLAN Configuration > QinQ Configuration > QinQ Tunnel Setting



## Trunking

The Trunking, or Link Aggregation, function allows users to combine several ports or connections to create one single connection with a higher and faster connection speed. Two trunking techniques are available in this VDSL2 IP Switch—Static Trunk and LACP.



Figure 42. Trunking

### Aggregator Setting

The Aggregator Setting tab allows users to set up trunking groups and their details. The following information must be included to set up a trunk group:

- **LACP** (checkbox): enable or disable LACP algorithm
- **System Priority**: this value identifies the active LACP of this VDSL2 IP Switch (the lowest value presents the highest priority)
- Trunk Group Table (see [Figure 44](#))

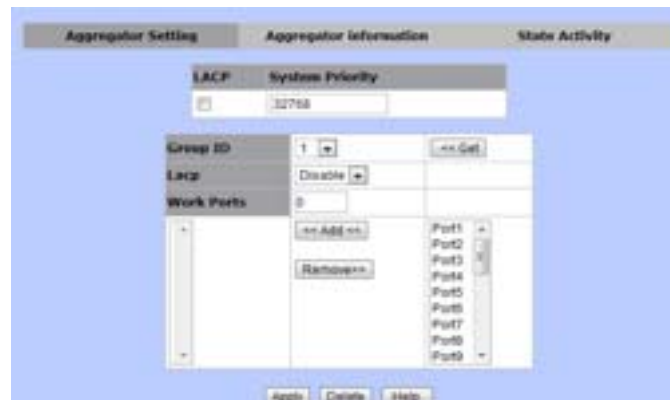


Figure 43. Trunking > Aggregator Setting

Follow these instructions to set up a **Trunk Group**:

1. Choose a **Group ID** (1-13)
2. **Enable** or **Disable** the LACP algorithm for this trunk group

- Choose the total port number (**Work Ports**) of the group; select the group number from the port list.

Figure 44. Trunk Group Table

### Aggregator information

The Aggregator information tab allows users to review trunk information, which includes the **Group Key** (trunk group ID) and the **Port number** of this trunk group.

### Static Activity

The Static Activity tab allows the user to set up LACP mode as an active or passive port.

- **Active Ports** will send LACP packets automatically
- **Passive Ports** will not send LACP packets, but will respond if it receives LACP packets from the other end.

Port	LACP	State Activity	Port	LACP	State Activity
1	N/A		2	N/A	
3	Active		4	Active	
5	N/A		6	N/A	
7	N/A		8	N/A	
9	N/A		10	N/A	
11	N/A		12	N/A	
13	N/A		14	N/A	
15	N/A		16	N/A	
17	N/A		18	N/A	
19	N/A		20	N/A	
21	N/A		22	N/A	
23	N/A		24	N/A	
25	N/A		26	N/A	

Figure 45. Trunking &gt; Static Activity

## Forwarding & Filtering

This function allows users to set up rules about packets. There are three ways to set up these rules—Dynamic MAC Table, Static MAC Table and MAC Filtering.



Figure 46. Forwarding and Filtering

### Dynamic MAC Table

The VDSL2 IP Switch will learn the device's MAC addresses dynamically and record these addresses into the MAC address table.

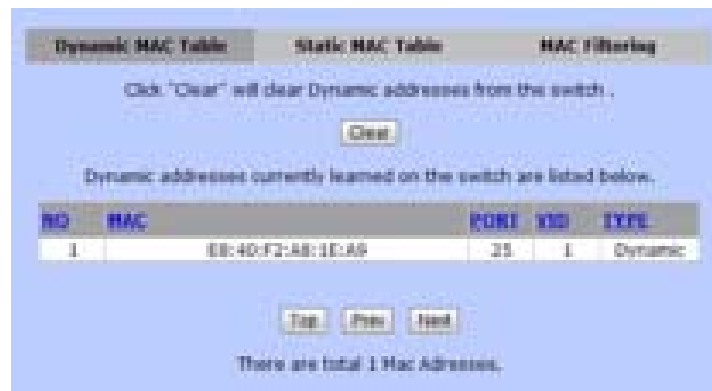


Figure 47. Forwarding and Filtering > Dynamic MAC Table

- **Clear** will delete the dynamic MAC address table
- **Top** will show the first page of the MAC address table
- **Prev** will go to the previous page of the MAC address table
- **Next** will go to the next page of the MAC address table

### Static MAC Table

Users are able to fill the MAC addresses of devices connected to the switch. By adding a static MAC address, the switch will save the information permanently and will not attend to learn the MAC address of this device when the device is online.



Figure 48. Forwarding and Filtering > Static MAC Table

### MAC Filtering

This function allows users to define and drop unwanted traffic.



Figure 49. Forwarding and Filtering > MAC Filtering

### IGMP Snooping

Internet Group Management Protocol allows hosts and routers to build multicast group memberships. IGMP snooping presents the process of IGMP network traffic listening. With this feature, VDSL2 IP Switch is able to

listen to IGMP conversations between hosts and routers. The switch is able to maintain a relation map of links and IP multicast streams.



Figure 50. IGMP Snooping

The following settings are needed in order to allow IGMP snooping work properly:

- **IGMP Protocol:** to enable or disable IGMP function
- **IGMP Fastleave:** to enable or disable IGMP Fastleave mode
- **IGMP Querier:** to enable or disable IGMP Querier mode
- **Multicast Group:** the multicast group list table

### Spanning Tree

Spanning Tree (STP) is a network protocol which is defined by IEEE 802.1 D standards for preventing bridge loops and broadcast radiation. In addition, STP allows redundant links to provide automatic backups. Most commonly known STP algorithms are STP (**Spanning Tree Protocol**), RSTP (**Rapid Spanning Tree Protocol**) and MSTP (**Multiple Spanning Tree Protocol**). This VDSL2 IP Switch supports both STP and MSTP. In addition, in this Switch, users are able to set up STP either for the whole system of the Switch or for each individual port (see [Figure 51](#) on the following page).

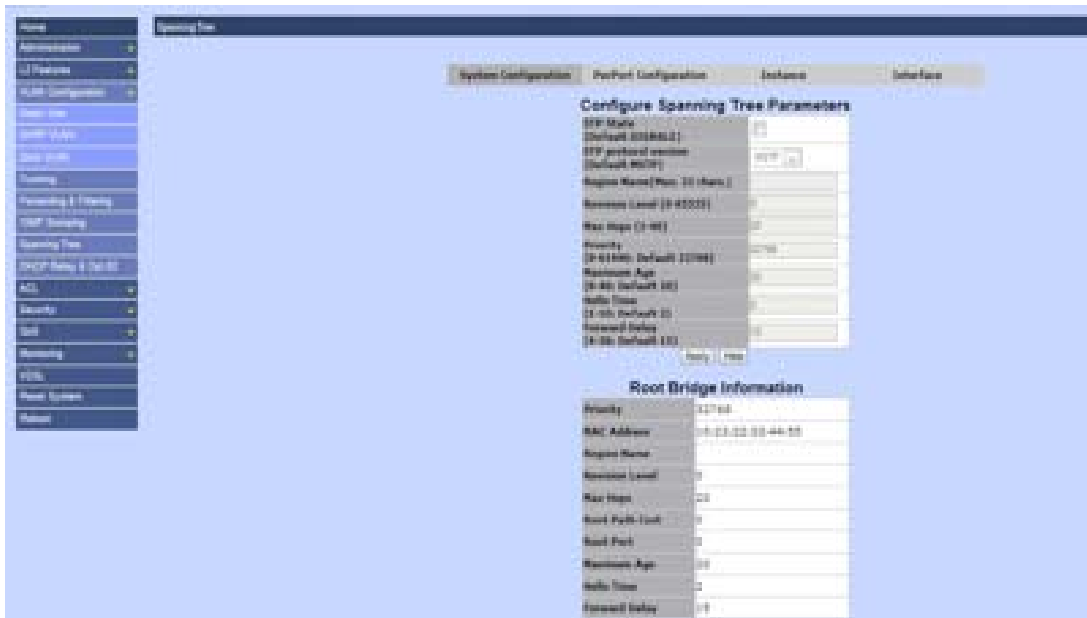


Figure 51. Configure Spanning Tree Parameters

In the Spanning Tree function, there are four major set up pages, explained on the following pages.

### System Configuration

This allows users to set up the details of STP function. In addition, the information of the root node of the STP will be displayed in this page.



Figure 52. Spanning Tree &gt; System Configuration

Follow these instructions to configure the Spanning Tree Parameters:

1. Check the box to **Enable** or **Disable** the STP State.

**Note** To enable the STP function, users must click on the checkbox and click **Apply**. After the saving process is complete, users are able to fill in the remaining information.

2. Choose **STP** or **MSTP** from the drop-down menu to select the **STP protocol version**
3. Enter a **Region Name** of the STP tree (32 characters)
4. Enter the **Revision Level** of the STP tree (0-65535)
5. Enter the number of **Max Hops** to be performed (1-40)
6. Enter a number for the **Priority** (0-61440)
7. Enter the **Maximum Age**, or waiting time, in seconds before the switch attempts to reconfigure (6-40)
8. Enter the **Hello Time** in seconds that the switch will send BPDU packets to check STP current status (1-10)
9. Enter the **Forward Delay** time (4-30)

The Root Bridge Information will display the Priority, MAC Address, Region Name, Revision Level, Max Hops, Root Path Cost, Maximum Age, Hello Time and Forward Delay for the STP function.

### PerPort Configuration

This function allows the user to set up Spanning Tree mode for each individual port.

The screenshot shows the 'Spanning Tree' configuration page. The top navigation bar includes 'System Configuration', 'PerPort Configuration', 'Instance', and 'Interface'. The main heading is 'Configure Spanning Tree Port Parameters'. Below this, there are several input fields for 'Port Number', 'Path Cost', 'Priority', 'Admin Edge', 'Admin Non-STP', 'Admin RSTP', and 'Migration Check'. Below the input fields is an 'Apply' button. The bottom section is titled 'STP Port Status' and contains a table with the following columns: PortName, PathCost, Priority, PortState, PortEdge, PortNonSTP, PortRSTP, and Migration Check. The table lists 20 ports (Port1 through Port20) with consistent values: PathCost 200000, Priority 128, PortState Disabled, PortEdge NO, PortNonSTP NO, PortRSTP NO, and Migration Check NO.

PortName	PathCost	Priority	PortState	PortEdge	PortNonSTP	PortRSTP	Migration Check
Port1	200000	128	Disabled	NO	NO	NO	NO
Port2	200000	128	Disabled	NO	NO	NO	NO
Port3	200000	128	Disabled	NO	NO	NO	NO
Port4	200000	128	Disabled	NO	NO	NO	NO
Port5	200000	128	Disabled	NO	NO	NO	NO
Port6	200000	128	Disabled	NO	NO	NO	NO
Port7	200000	128	Disabled	NO	NO	NO	NO
Port8	200000	128	Disabled	NO	NO	NO	NO
Port9	200000	128	Disabled	NO	NO	NO	NO
Port10	200000	128	Disabled	NO	NO	NO	NO
Port11	200000	128	Disabled	NO	NO	NO	NO
Port12	200000	128	Disabled	NO	NO	NO	NO
Port13	200000	128	Disabled	NO	NO	NO	NO
Port14	200000	128	Disabled	NO	NO	NO	NO
Port15	200000	128	Disabled	NO	NO	NO	NO
Port16	200000	128	Disabled	NO	NO	NO	NO
Port17	200000	128	Disabled	NO	NO	NO	NO
Port18	200000	128	Disabled	NO	NO	NO	NO
Port19	200000	128	Disabled	NO	NO	NO	NO
Port20	200000	128	Disabled	NO	NO	NO	NO

Figure 53. Spanning Tree > PerPort Configuration

*Instance*

Figure 54. Spanning Tree &gt; Instance

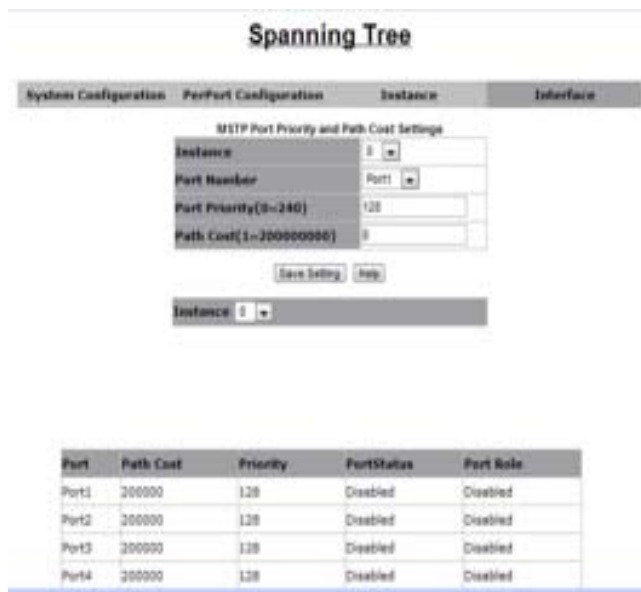
*Interface*

Figure 55. Spanning Tree &gt; Interface

**DHCP Relay & Opt. 82**

Dynamic Host Configuration Protocol is a network protocol for configuring network devices dynamically, so these devices can communicate on an IP network. It is a service that runs at the application layer of TCP/IP protocol stack to assign IP addresses to its clients dynamically.



*DHCP Relay* will forward DHCP broadcasts to multiple DHCP servers in different subnets using unicasts. By doing so, DHCP clients on subnets not directly served by DHCP servers can communicate with DHCP servers. In addition, *DHCP Relay Information Options 82* is defined in RFC 3046 and RFC 3993, and allows a DHCP Relay agent to insert circuit specific information to a request which is forwarded to a DHCP server.

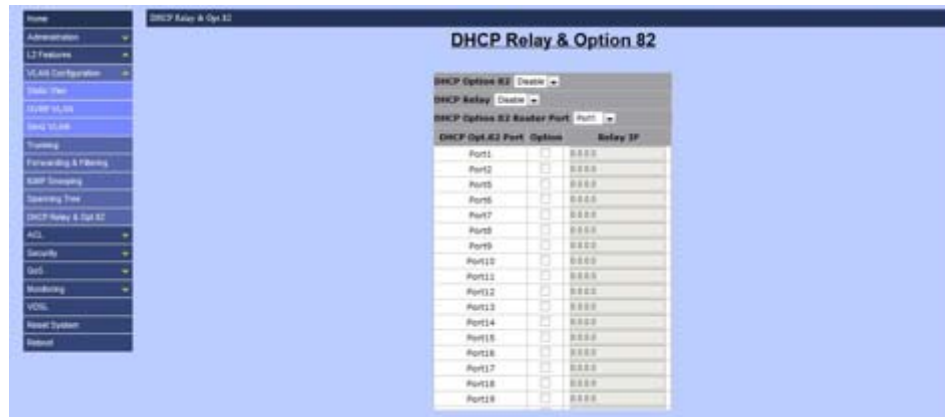


Figure 56. DHCP Relay & Option 82

### *DHCP Option 82*

Users are allowed to enable or disable DHCP Option 82 by choosing the options in the drop-down menu. To setup DHCP Option 82 for this switch, users are required to enable this option first.

### *DHCP Relay*

DHCP Relay is for enabling or disabling DHCP Relay function.

### *DHCP Option 82 Router Port*

DHCP Option 82 Router Port allows users to choose the relay port for DHCP Option 82 feature. Users are able to specify one port between Port1 to Port24 or Mod1 to Mod2.

### *DHCP Opt. 82 Port Table*

This section is for defining DHCP Option 82 and port information.

- **Option:** Enable or disable DHCP Relay Information Option 82 function
- **Relay IP:** Assign the IP address of the port

DHCP Opt. 82 Port#	Options	Relay IP
Port1	<input type="checkbox"/>	0.0.0.0
Port2	<input type="checkbox"/>	0.0.0.0
Port3	<input type="checkbox"/>	0.0.0.0
Port4	<input type="checkbox"/>	0.0.0.0
Port5	<input type="checkbox"/>	0.0.0.0
Port6	<input type="checkbox"/>	0.0.0.0
Port7	<input type="checkbox"/>	0.0.0.0
Port8	<input type="checkbox"/>	0.0.0.0
Port9	<input type="checkbox"/>	0.0.0.0
Port10	<input type="checkbox"/>	0.0.0.0
Port11	<input type="checkbox"/>	0.0.0.0
Port12	<input type="checkbox"/>	0.0.0.0
Port13	<input type="checkbox"/>	0.0.0.0
Port14	<input type="checkbox"/>	0.0.0.0
Port15	<input type="checkbox"/>	0.0.0.0
Port16	<input type="checkbox"/>	0.0.0.0
Port17	<input type="checkbox"/>	0.0.0.0
Port18	<input type="checkbox"/>	0.0.0.0
Port19	<input type="checkbox"/>	0.0.0.0

Figure 57. DHCP Option 82 &gt; Relay IP

## ACL (Access Control List)

Packets can be forwarded or dropped by ACL rules, including IPv4 or non-IPv4. The switch can be used to block packets by maintaining a table of packet fragments indexed by source and destination IP address, protocol, and so on.

The screenshot displays the 'Access Control List' configuration page. It includes a sidebar with navigation options like Home, Administration, L2 Features, ACL, ACL Control List, Security, QoS, Monitoring, VDSL, Reset System, and Reboot. The main content area is titled 'Access Control List' and contains several sections:

- Group ID:** A dropdown menu set to '(1-200)'.
- Action:** A dropdown menu set to 'Permit'. A note below states: 'QoS Value (QoS mode "All High Buffer Lim" is required in QoS webpage)'. There is also a checkbox for 'QoS Value'.
- VLAN:** A dropdown menu set to 'Any'. A note below states: '(=4094, Any means VID=0 if use binding)'. There is also a checkbox for 'VLAN'.
- Packet Type / Binding:** Radio buttons for 'IPv4' (selected) and 'Non-IPv4'. Under 'Binding', there are radio buttons for 'SIP' (selected) and 'SMAC-Port'. There are input fields for 'MAC Address' and 'Port ID'.
- Src IP Address:** A dropdown menu set to 'Any' and an input field for 'IP Address' set to '0.0.0.0'. There is also a checkbox for 'Src IP'.
- Dst IP Address:** A dropdown menu set to 'Any' and an input field for 'IP Address' set to '0.0.0.0'. There is also a checkbox for 'Dst IP'.
- Fragment:** A dropdown menu set to 'Uncheck'.
- L4 Protocol:** A dropdown menu set to 'Any'. There are checkboxes for 'TCR' and 'QoS Value'.
- QoS Value:** A table with columns for 'Protocol', 'Value (Hex,0-FF)', and 'Mask (Hex,0-FF)'. Rows include 'Protocol', 'Source Port', and 'Destination Port'.
- Port ID:** A dropdown menu set to '(=0:0:0:0:0:0)'. There is also a checkbox for 'Port ID'.
- Control List:** A list box containing one entry.

At the bottom, there are buttons for 'Add', 'Del', 'Enable', 'Disable', 'Reset No Count', and 'Help'.

Figure 58. Access Control List

There are two main ACL rule types to setup—Packet Type (IPv4 and Non-IPv4) and Binding (SIP-SMAC-Port). The following describes the three main sections of this page:

- Section 1
  - **Group ID:** the ID of this Access Control List (1-200)
  - **Action:** Permit or Deny access
  - **VLAN:** Any or VID (a specific VLAN ID)

- Section 2
  - **Port ID:** the target port of this access control list should be applied to this section (0-10)
- Section 3
  - **Current List:** the current list of all access control lists

## IPv4

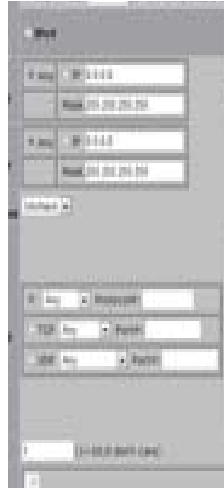


Figure 59. Access Control List > IPv4

The following describes the options within the section:

- Packet Type/Binding
  - The option *IPv4* is selected
- SRC IP Address
  - Options: Any or a specific IP address
  - The rule should be applied on these packets from an IP address or any IP address.
- DST IP Address
  - Options: Any or a specific IP address
  - The rule should be applied on these packets with an assigned destination IP address or any IP address.
- IP Fragment
  - Options: Uncheck or Check
  - To decide whether IP fragment should be checked or not
- L4 Protocol
  - Options are included in the following table:

Table 5. L4 Protocol

L4 Protocol Type	Options	Data
Any	Any, ICMP, IGMP	Protocol No.
TCP	Any, FTP, HTTP	Port No.
UDP	Any, DHCP, TFTP, NetBIOS	Port No.

**Non-IPv4**

Choose the Ether Type as **Any**, **ARP** or **IPX** for this section.



Figure 60. Access Control List > Non-IPv4

**Binding**

Enter the Mac Address, IP Address and Port ID (1-10) for this section.



Figure 61. Access Control List > Binding

## QoS VoIP



Figure 62. Access Control List > QoS VoIP

If the QoS VoIP check box is selected, the following information must be provided.

- The Priority of QoS VoIP (0-7)
- The Port ID number for the Value and Mask (Hex, 0-1F)
- The Protocol number for the Value and Mask (Hex, 0-FF)
- The Source Port number for the Value and Mask (0-FFFF)
- The Destination Port number for the Value and Mask (0-FFFF)

QoS VoIP	Priority#	7	
	PortID#	Value (Hex, 0-1F)	Mask (Hex, 0-1F)
	Protocol#	Value (Hex, 0-FF)	Mask (Hex, 0-FF)
	Source Port#	Value (Hex, 0-FFFF)	Mask (Hex, 0-FFFF)
	Destination Port#	Value (Hex, 0-FFFF)	Mask (Hex, 0-FFFF)

Figure 63. QoS VoIP Options

**Note** All values are in HEX format.

## Security

This section allows users to enhance the security level of this VDSL2 IP Switch, which includes the following functions.

### Security Manager

This function allows users to change the user name and password for login purposes. Only one set of user name and password is stored in the Switch. The following information must be included:

- User Name (default name is admin)
- Assign/Change Password (default password is admin)
- Reconfirm Password



Figure 64. Security Manager

## MAC Limit

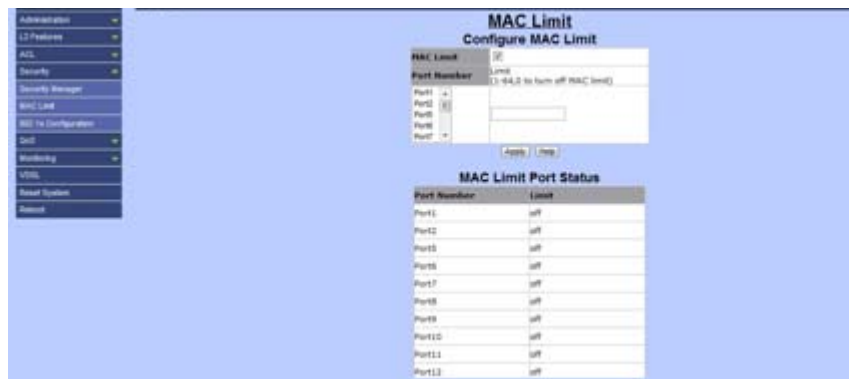


Figure 65. MAC Limit

The MAC limit allows users to set a maximum number of MAC addresses to be stored in the MAC address table. The MAC addresses chosen to be stored are the result of first-come-first-save policy. Once a MAC address is stored in the MAC address table, it stays until it is aged out. When an “opening” is available, the switch stores the first new MAC address in that opening. All packets from MAC addresses not in the MAC address table should be blocked. There are two sections in the MAC Limit page:

### Configure MAC Limit

This section allows users to set up MAC limit rules for each port by providing the following information:

- **MAC Limit:** Enable or disable MAC limit function.
- **Limit:** The maximum number of MAC addresses should be blocked.

### MAC Limit Port Status

This section allows users to review the status of ports and MAC limits.

## 802.1x Configuration

This section makes use of the physical access characteristics of IEEE 802 LAN infrastructures. These infrastructures provide a means of authenticating and authorizing devices attached to a LAN port with point-to-

point connection characteristics, and prevents access to that port in cases which the authentication and authorization process fails.



Figure 66. 802.1x Configuration

**Note** The default 802.1x setup is disabled, preventing access to the 802.1x Configuration page which is shown. To enable the 802.1x protocol field, go to **Administration > Switch setting > Misc Configs**. After enabling this function, the 802.1x configuration page will be visible.

### System Configuration

This section allows the user to configure the 802.1x parameters.

- **Radius Server IP:** the IP address of the authentication server
- **Server Port:** the UDP port number used by the authentication server to authenticate (default: 1812)
- **Accounting Port:** the UDP port number used by the authentication server to retrieve accounting information (default: 1813)
- **Shared Key:** the password between the switch and the authentication server
- **NAS, Identifier:** the name of this switch

### PerPort Configuration

This section allows users to setup the authorization mode of 802.1x for each port and review the authorization status of each port. The VDSL2 IP Switch allows users to setup four authorization modes:

- **FU:** force the specific port to be unauthorized
- **EA:** force the specific port to be authorized
- **AU:** the state of the selected port was determined by the outcome of the authentication
- **NO:** the selected port did not support the 802.1x function



Figure 67. 802.1x Configuration &gt; PerPort Configuration

### Misc Configuration

This section allows users to change miscellaneous setups of 802.1x function.

- **Quiet Period:** defines periods of time during which it will not attempt to acquire a supplicant (default time: 60 seconds).
- **Tx Period:** determines when an EAPOL PDU is to be transmitted (Default value is 30 seconds).
- **Supplicant Timeout:** determines timeout conditions in the exchanges between the supplicant and authentication server (default value: 30 seconds).
- **Server Timeout:** determines timeout conditions in the exchanges between the authenticator and authentication server (default value: 30 seconds).
- **ReAuthMax:** determines the number of re-authentication attempts that are permitted before the specific port becomes unauthorized (default value: 2 times).
- **Reauth Period:** determines a nonzero number of seconds between periodic re-authentication of the supplicants (default value: 3600 seconds).

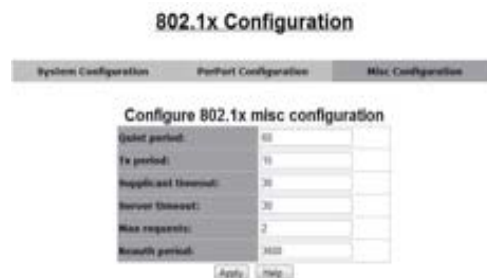


Figure 68. 802.1x Configuration &gt; Misc Configuration



## QoS

This switch provides quality of service (QoS) to prioritize the packet forwarding when traffic congestion occurs. This switch supports two QoS functions—port-based (4-level output queue) and 802.1p (8-level priority to 4-level queue mapping). In addition, Strict and Weight Round Robin (WRR) QoS modes are supported.

### QoS Configuration

This page includes two sections to complete the QoS Configuration.



Figure 69. QoS Configuration

#### QoS Configuration - Priority Queue Service

There are four QoS Modes supported in this switch:

- **First Come First Service:** The sequence of packets sent is dependent on arriving orders; this mode can be regarded as QoS disabled.
- **All High before Low:** High priority packets are sent before low priority packets.
- **WRR (Weighted Round Robin):** Select the preference given to packets in the switch's high-priority queue. These options represent the number of higher priority packets sent before one lower priority packet is sent. For example, 8 Highest: 4 second-high means that the switch sends 8 highest-priority packets before sending 4 second-high priority packets.
- **802.1p priority:** The switch supports 8 802.1p priority queues with 4 priority levels (Highest, Second-High, Second-Low, and Lowest). This section is for setting up the maps of priority queues and priority levels.

#### PerPort Configuration

This section allows users to set up the priority level for each port. Users are able to set up QoS algorithm with Port-Based algorithm in this page. The Port Priority table (see [Figure 69](#)) includes the option to disable or choose a priority number for each port (0-7).

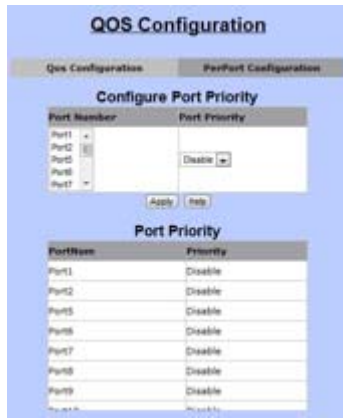


Figure 70. QoS Configuration > PerPort Configuration

### ToS/DSCP

The ToS (Type of Service)/DSCP page allows users to set up priority algorithm for each queue and packets. In IPv4 packet header, there is a ToS byte, and ToS algorithm uses the first 3 bits for priority level. However, for DSCP algorithm, it will take the first 6 bits for priority level.

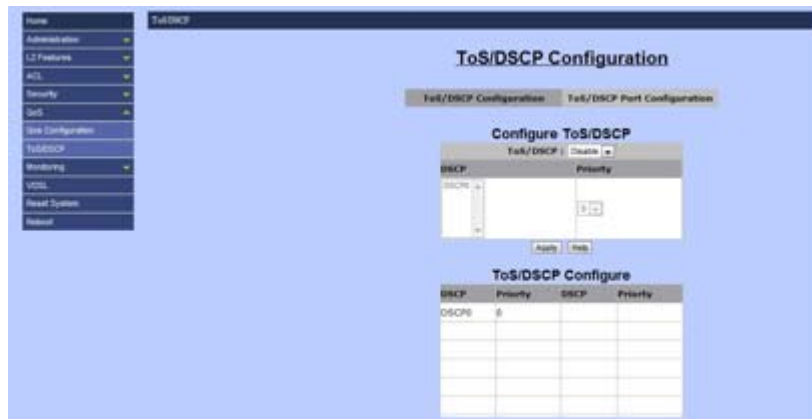


Figure 71. ToS/DSCP Configuration

## Monitoring

This function allows users to review current status and statistics of each port (Port1 ~ Port24, Mod1 and Mod2).

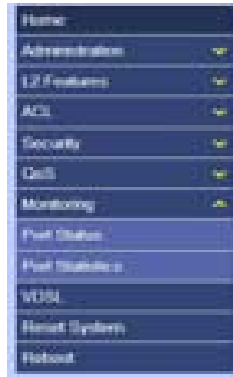


Figure 72. Left-side panel navigation

### Port Status

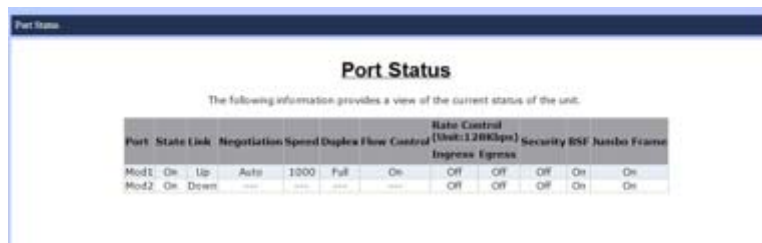


Figure 73. Port Status

The Port Status displays the current status of linked ports, and is for review only. The information will be shown as the following:

Table 6. Port Status Options

Item	Data
<b>Port</b>	Port No.
<b>State</b>	On (Only linked ports will be shown)
<b>Link</b>	Up / Down
<b>Negotiation</b>	Auto / Force
<b>Speed</b>	10/100 Mbps (Port1-Port24) 10/100/1000 Mbps (Mod1-Mod2)
<b>Duplex</b>	Full / Half
<b>Rate Control (Ingress and Egress)</b>	On / Off
<b>Security</b>	On / Off
<b>BSF</b>	On / Off

Table 6. Port Status Options

Item	Data
Jumbo Frame	On / Off

**Port Statistics**

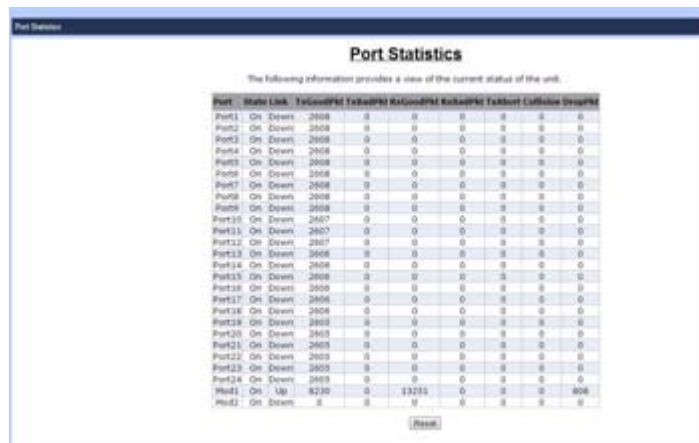


Figure 74. Port Statistics

This section allows users to review the statistics data of each port with the following details:

Table 7. Port Statistics Options

Item	Data
Port	Port No.
State	On / Down
Link	On / Down
TxGoodPkt	Total bytes of good packets that were transmitted
TxBadPkt	Total bytes of bad packets that were transmitted
RxGoodPkt	Total bytes of good packets that were received
RxBadPkt	Total bytes of bad packets that were received
TxAbort	Total bytes of packets that were aborted
Collision	Collision
DropPkt	Total bytes of packets dropped

## VDSL

This page allows users to set up and review VDSL profiles. Navigate the this page by using the Left-side panel navigation.

### Configuration



Figure 75. Profile Setting > Configuration

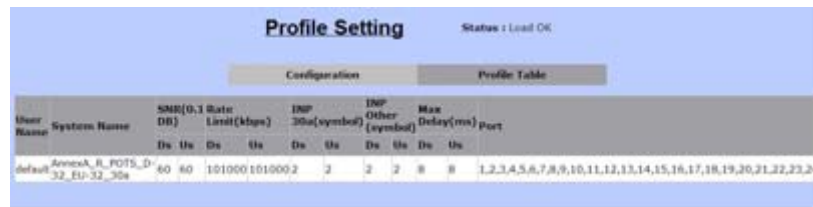
This section allows users to set up VDSL profiles and store these profiles into the system. The following describes the details available to set up each VDSL profile.

**Note** There are 21 pre-defined profiles. These names are not changeable, but users are allowed to save new profiles.

Table 8. VDSL Profile Options

Item	Description
<b>User Profile Name</b>	The name of user-defined profile
<b>New Profile Name</b>	New Profile name (up to 64 characters)
<b>System Profile Name</b>	This option is for setting up VDSL band profile. Different profile results in different connection statuses of data rate and distance
<b>SNR</b>	SNR values for both downstream and upstream (6dB-24dB)
<b>Rate Limit Ds Us</b>	The data rates for both downstream and upstream
<b>INP 30a</b>	INP levels for VDSL2 profile 30a for both downstream and upstream
<b>INP no 30a</b>	INP level for other VDSL2 profiles (8a, 8b, 8c, 8d, 12a, 12b and 17a) for both downstream and upstream
<b>Max Delay</b>	The maximum delay time for both downstream and upstream Options: No limit, No delay, 1 ms-63ms
<b>Port</b>	For assigning which ports should be applied to which profile.

## Profile Table



User Name	System Name	SNR(0,1 State DB)		Rate Limit(kbps)		INP 30a(symbol)		INP Other(symbol)		Max Delay(ms)	Port
		Ds	Us	Ds	Us	Ds	Us	Ds	Us		
default	Annex_8_POTS_D-32_EU-32_30a	60	60	101000	101000	2	2	2	8	8	1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24

Figure 76. Profile Setting > Profile Table

This section allows users to review the details of existing profiles and the following options.

Table 9. Profile Setting Options

Item	Description
<b>User Name</b>	Profile Name
<b>System Name</b>	VDSL2 Band profile
<b>SNR (Ds / Us)</b>	SNR value
<b>Rate Limit (Ds / Us)</b>	Data rate
<b>INP 30a (Ds / Us)</b>	INP level for VDSL2 profile 30a
<b>INP Other (Ds / Us)</b>	INP level for the other VDSL2 profiles
<b>Max Delay</b>	Maximum delay
<b>Port</b>	Port members of this profile

## Reset System

This function is for restoring all configurations back to the default factory configurations. All the settings will be changed back to the original state.



Figure 77. Reset System

## Reboot

---

This function allows users to reboot the switch without turning off the power.



Figure 78. Reboot Switch System

## Chapter 3 **Configuration Via Console**

### **Chapter contents**

Introduction .....	65
Login to the Console .....	65
General Information of Commands .....	66
Configuration .....	67
Command Descriptions .....	69
System Commands .....	69
Switch Static Configuration .....	69
Trunk Commands .....	71
LACP Commands .....	71
VLAN Mode & Commands .....	72
GVRP Commands .....	73
QinQ Commands .....	75
Misc Configuration .....	75
Administration .....	76
Port Mirroring .....	77
QoS .....	77
Commands for MAC .....	78
MAC Limits .....	79
Protocol Related Commands .....	79
STP/RSTP .....	79
MSTP .....	81
SNMP .....	84
IGMP .....	87
802.1x .....	88
DHCP Relay & Option82 .....	89
Syslog .....	90
SSH .....	90
Reboot Switch .....	90
TFTP Function .....	90
Access Control List .....	91
IPv4 ACL commands .....	91
Non-IPv4 ACL commands .....	93
SIP/SMAC Binding .....	93



## Introduction

This chapter describes setting up the ForeFront 3210P VDSL2 IP Switch support with a console instead of a web browser. The Command Line Interface allows users to access the switch with any terminal emulation program, such as, Hyperterminal or teraterm, etc.

The table below shows the default settings of the serial port to connect to the switch.

Table 10. Default Settings

Baud Rate	115200
Data Bit	8
Parity	None
Stop Bit	1
Flow Control	None

## Login to the Console

After connecting the switch with a PC, or laptop together, users are able to login with a terminal emulation program, such as Hyperterminal. The following window will be visible while the switch is booting.

```

Tera Term Web 11 - COM4 VT
File Edit Setup Web Control Window Help
Initiate Ethernet switch driver v1.28
Giga PHY type MARVELL 88E1111
*****
24 + 2 Switch Module Slot Information
*****
Gigabit Port 1 Yes
Gigabit Port 2 Yes
*****

Initializing switch functions ...
SNMP files ..... OK
Modules ..... OK
LACP ..... OK
Trunk ..... OK
GVRP ..... OK
VLAN ..... OK
System ..... OK
QinQ ..... OK
Forwarding ..... OK
IP Mcast ..... OK
IGMP ..... OK
STP/RSTP/HSTP

```

Figure 79. Login screen



Table 11. Major Commands

show	Show information
configure	Configuration
disable	Turn off privileged mode command <ul style="list-style-type: none"> <li>• This will turn off the privilege of setting system configurations</li> <li>• Enable will be shown if the user disables the privilege</li> </ul>

## Configuration

Navigate to the configuration mode by typing **config** in Switch# and **enter/return**. This will allow users to configure the settings of VDSL2 IP Switch.

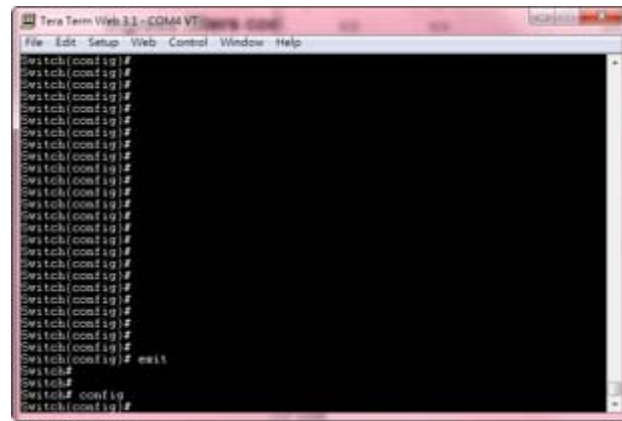


Figure 82. Configuration mode

The following table displays the available configurations of the switch.

Table 12. Configurations

exit	Exit current mode and change to the previous mode
logout	Log out of the system
help	Show the description of a command
history	Set the number of history commands
no	Negate a command or set its defaults'
show	Show running system information
hostname	Set up the switch's network name
disable	Turn off privileged mode (disable configuration mode)
password	Password information
timeout	Set up the timeout for the current CLI
syslog-server	Set up the information of syslog server
broadcast	Set up Broadcast storm filter mode
collision-retry	Set up the settings of collision-retry function
mac-age-time	Enable MAC address age-out function

Table 12. Configurations

mac-hash	Set up MAC hash algorithm
mirror-port	Port monitoring information
qos	QoS information
tosport	ToS/DSCP port status information
tosdscp	ToS/DSCP information
clear	Clear values in destination protocol
mac-address-table	MAC address table information
smac-address-table	MAC address table information
filter	Filter destination MAC address information
mac-limit	MAC limit
port	Port information
boot	Reboot the switch
copy	Copy configurations
dhcp	DHCP information
erase	Erase configuration
ip	IP information
ping	Send ICMP ECHO_REQUEST to network hosts
dhcp-options82	Enable DHCP option 82 feature
dhcp-relay	Enable DHCP relay feature
qinq	QinQ information
trunk	Trunking information
vlan	VLAN information
dot1x	802.1x information
radius-server	Radius server information
garp	GARP information
gvrp	GVRP information
igmp	IGMP information
lacp	LACP information
snmp	SNMP information
sntp	Start SNTP service
spanning-tree	Spanning Tree Protocol
acl	ACL information
enable	Enable privileged command mode
bind	Enable SIP/SMAC binding
dslcli	Run DSL CLI
interface	Commands for interfaces
profiles	Commands for profiles
util	Commands for VDSL utility

## Command Descriptions

---

### System Commands

- **show running-config**: Show the running configuration of the switch.
- **copy running-config startup-config**: Backup the configurations of the switch.
- **erase startup-config**: Reset to default factory configurations the following reboot time.
- **clear arp [ip-address]**: Clear entries in the ARP cache in the selected IP address.
- **show arp**: Show IP ARP translation table.
- **ping ip-addr [<1...999>]**: Send ICMP ECHO\_REQUEST to the selected IP address.  
 <1...999>: the number of repetitions. If there is no value in this area, it will continuously ping until users press <Ctrl>+C to stop.
- **no per-vlan-flooding-portmask**: Enable or disable per VLAN default flooding port mask.
- **per-vlan-flooding-portmask <unicast | multicast> <vlan-id> <port-list>**: Set unicast or multicast per VLAN default flooding port mask.
- **show per-vlan-flooding-portmask**: Display unicast and multicast per VLAN default flooding port mask table.

### Switch Static Configuration

- **port state <on | off> [<port-list>]**

Turn on or turn off the port state.

The <port-list> command specifies the ports to be turned on or off. If there is no <port-list> value, all ports will be turned on or turned off.

**Note** Where **<port-list>** is listed in the configurations below, this command is used to specify the ports to be set, unless stated otherwise. If no value is entered, all ports will be set.

- **port nego <force | auto > [<port-list>]**  
Set port negotiation mode.
- **port speed <10 | 100 | 1000> <full | half> [<port-list>]**  
Set port speed (mbps) and duplex.
- **port flow <enable | disable> <enable | disable> [<port-list>]**  
Enable or disable port flow control.  
 1st <enable | disable>: enables or disables flow control in full duplex mode.  
 2nd <enable | disable>: enables or disables flow control in half duplex mode.
- **port rate <ingress | egress> <0..8000> [<port-list>]**  
Set port effective ingress or egress rate.  
 <0...8000>: specifies the ingress or egress rate. (0...8000)

- **port security <on | off> [<port-list>]**  
Set port security. When port security is on, the port will stop MAC address learning and forward only packets with MAC addresses in the static MAC address table.
- **port protected group <1-2> <port-list>**  
Set protected port group member.  
The <port-list> command specifies the group member ports.
- **port protected <port-list>**  
Set protected port list.  
The <port-list> command specifies the protected port list.
- **port priority <disable | low | high> [<port-list>]**  
Set port priority.
- **port jumboframe <enable | disable> [<port-list>]**  
Set port jumbo frame. When the port jumbo frame is enabled, the port forward jumbo frame packet
- **port interval <0-3600>:**  
While flooding the CPU port at the speed of 4MB/s or larger, the system will close the relative port. The system will open this port using the interval value .0 represents the system will never enable this after closing for flooding the CPU.
- **show port status**  
Show port status, including port State, Link, Trunking, VLAN, Negotiation, Speed, Duplex, Flow control, Rate control, Priority, Security and BSF control.
- **show port statistics <port-id>**  
Show port statistics, including TxGoodPkt, TxBadPkt, RxGoodPkt, RxBadPkt, TxAbort, Collision and DropPkt.  
The <port-id> command specifies the port to be shown.
- **show port protection**  
Show protected port information.

### Trunk Commands

- **show trunk**  
Show trunking information.
- **trunk add <trunk-id> <lacp | no-lacp> <port-list> <active-port-list>**  
Add a new trunk group.  
The command <trunk-id> specifies the trunk group to be added.  
The command <lacp> specifies the added trunk group to be LACP enabled.  
The command <no-lacp> specifies the added trunk group to be LACP disabled.  
The command <port-list> specifies the ports to be set.  
The command <active-port-list> specifies the ports to be set to LACP active.
- **no trunk <trunk-id>**  
Delete an existing trunk group.  
The command <trunk-id> specifies the trunk group to be deleted.

### LACP Commands

- **[no] lacp**  
Enable/disable LACP.
- **lacp system-priority <1..65535>**  
Set LACP system priority.  
Parameters: <1..65535> specifies the LACP system priority.
- **no lacp system-priority**  
Set LACP system priority to the default value 32768.
- **show lacp status**  
Show LACP enable/disable status and system priority.
- **show lacp**  
Show LACP information.
- **show lacp agg <trunk-id>**  
Show LACP aggregator information.  
The <trunk-id> command specifies the trunk group to be shown.
- **show lacp port <port-id>**  
Show LACP information by port.  
The <port-id> command specifies the port to be shown.

**Note** If VLAN group exists, all members of the static trunk group must be in same VLAN group.

### VLAN Mode & Commands

In VLAN Mode port-based command, packets can only go among members of the same VLAN group. Note all unselected ports are treated as belonging to another single VLAN. If the port-based VLAN is enabled, the VLAN-tagging is ignored.

In VLAN Mode: 802.1Q command, if a trunk group exists, you can see it (e.g. TRUNK1, TRUNK2...) after port 24, and configure it to be a member of the VLAN group. In this setting, the port is set to Untagged if devices underneath this port do not support VLAN-tagging. This allows the switch to send untagged frames to this port. Consequently, devices that do not support VLAN-tagging or do not enable VLAN-tagging can still successfully fetch the incoming frames and communicate with the device that transferred the tagged frames, and vice versa.

In Advanced 802.1Q VLAN Setting command, ingress filters configure when a packet is received on a port; users can govern the switch to drop it or not if it is an untagged packet. Furthermore, if the received packet is tagged but not belonging to the same VLAN group of the receiving port, users can also control the switch to forward or drop the packet. The example below configures the switch to drop the packets not belonging to the same VLAN group and forward the packets not containing VLAN tags.

- **show vlan mode**

Display the current VLAN mode.

- **vlan mode (disabled|port-based|dot1q)**

Change VLAN mode.

Parameters: (disabled|port-based|dot1q) specifies the VLAN mode.

**Note** Change the VLAN mode every time; users must restart the switch for valid values.

- **show vlan mode**

Display the current VLAN mode.

- **vlan mode (disabled|port-based|dot1q)**

Change VLAN mode.

Parameters: (disabled|port-based|dot1q) specifies the VLAN mode.

**Note** Change the VLAN mode every time; users must restart the switch for valid values.

- **vlan add <1-4094> <NAME> <cpu-port|no-cpu-port> <LIST> [<LIST>]**

Add or edit VLAN entry.

The <1-4094> command specifies the VLAN id or Group id (if port based VLAN mode)

The <NAME> command specifies the VLAN group name.

The <cpu-port|no-cpu-port> command specifies the CPU port belonging to this VLAN group.

1st <LIST> specifies the ports to be set to VLAN members.



2nd [<LIST>] specifies which ports will be set to tagged members. If not entered, all members are set to untagged.

e.g. `vlan add 1 vlan1 cpu-port 1-4` . This VLAN entry has four members (from port1 to port4) and all members are untagged.

- **no vlan <1-4094>**

Delete VLAN entry.

Parameters: <1-4094> specifies the VLAN id or group id (if port based VLAN). e.g. `no vlan 1`

- **show vlan [<1-4094>]**

Show VLAN entry information.

The [<1-4094>] command specifies the VLAN id, null means all valid entries. e.g. `show vlan 1`

- **show vlan static**

Show static VLAN entry information.

- **vlan pvid <LIST> <1-4094>**

Set port default VLAN id.

The <LIST> command specifies the ports to be set.

The <1-4094> command specifies the port VLAN id.

- **show vlan pvid [<LIST>]**

Show port default VLAN id.

Parameters: [<LIST>] specifies the ports to be shown. If not entered, all ports' PVID will be shown.

- **vlan filter <enable|disable> <enable|disable> <LIST>**

Set ingress filter rules.

1st <enable|disable> specifies if the non-members' packet will be forwarded or not. If enabled, it will forward only packets with VID matching this port's configured VID.

2nd <enable|disable> specifies if the untagged frame will be dropped or not. If enabled, it will drop the untagged frame.

The <LIST> command specifies the port or trunk list (eg. 3, 6-8, Trk2).

- **show vlan filter [<LIST>]**

Show VLAN filter setting

The [<LIST>] command specifies the ports to be shown. If not entered, all ports' filter rules will be shown.

## GVRP Commands

- **[no] gvrp**

Enable or disable GVRP.

- **show gvrp status**

Show GVRP enable or disable status.

- **[no] port gvrp <LIST>**  
Enable or disable GVRP by port.  
The <LIST> command specifies the port or trunk list to be set.
- **show port gvrp**  
Show GVRP status by port.
- **garp timer <join | leave | leave-all> <0..65535>**  
Set GARP timer.  
The commands, <join | leave | leave-all> specifies a timer (Join, Leave, or Leave-All) to be set; <0..65535> specifies the timer in seconds.
- **show garp timer**  
Show GARP timer.
- **show gvrp db**  
Show GVRP DB.
- **show gvrp gip**  
Show GVRP GIP.
- **show gvrp machine**  
Show GVRP machine.
- **clear gvrp statistics <LIST>**  
Clear GVRP statistics by port.  
The <LIST> command specifies the port or trunk list to be set.
- **show gvrp statistics <LIST>**  
Show GVRP statistics by port.  
The <LIST> command specifies the port or trunk list to be set.
- **[no] gvrp debug [<sys | err | pdu | db | gen | garp | gvrp | vlan>]**  
Enable/disable GVRP debugging output.

### **QinQ Commands**

- **qinq enable**  
Enable QinQ.
- **[no] qinq**  
Disable QinQ.
- **qinq tpid <TPIDVAL>**  
Set QinQ tpid.  
The <TPIDVAL> command specifies QinQ tpid value (Hex, 1-FFFF).
- **qinq userport <enable|disable> <LIST>**  
A port configured to support the client end of a QinQ tunnel is called a QinQ user-port. Use this command to enable/disable a QinQ user-port to specified port(s).
- **qinq uplinkport <enable|disable> <LIST>**  
A port configured to support the network end of a QinQ tunnel is called a QinQ uplink-port. Use this command to enable/disable a QinQ uplink-port to specified port(s).
- **qinq tunnel add <1-25> <1-4094> <LIST>**  
Add QinQ tunnel.  
<1-25> specifies the tunnel ID.  
<1-4094> specifies the VLAN ID.  
The <LIST> command specifies the ports to be set to QinQ tunnel.
- **qinq tunnel delete <1-25>**  
Delete QinQ tunnel.  
<1-25> specifies the tunnel ID.
- **show qinq configuration**  
Show QinQ global and portal configuration.
- **show qinq tunnel**  
Show QinQ tunnel information.

### **Misc Configuration**

- **[no] mac-age-time**  
Enable or disable MAC address age-out.
- **mac-age-time <6..1572858>**  
Set MAC address age-out time.  
<6..1572858> specifies the MAC address age-out time. The value must be divisible by 6; type the number of seconds that an inactive MAC address remains in the switch's address table.
- **show mac-age-time**  
Show MAC address age-out time.

- **broadcast mode <off | 1/2 | 1/4 | 1/8 | 1/16>**  
Set broadcast storm filter mode to off, 1/2, 1/4, 1/8, 1/16.
- **broadcast select <unicast/multicast | control packet | ip multicast | broadcast>**  
Select the Broadcast storm filter packet type:
  - Unicast/Multicast: Flood unicast/multicast filter
  - Control Packets: Control packets filter
  - IP multicast: Ip multicast packets filter
  - Broadcast Packets: Broadcast Packets filter
- **Collision-Retry <off | 16 | 32 | 48>**  
Parameters:  
<off|16|32|48> In half duplex, collision-retry maximum is 16, 32 or 48 times, and the packet will be dropped if collisions still occur. In default (off), if collisions occur, it will retry forever.
- **Hash <crc-hash | direct-map>**  
Set hash algorithm to CRC-Hash or DirectMap.

## Administration

- **hostname <name-str>**  
Set switch name.  
  
The <name-str> command specifies the switch name. If you would like to have spaces within the name, use quotes (“”) around the name.  
  
-no hostname: Reset the switch name to factory default setting.
- **[no] password <manager | operator | all>**  
Set or remove username and password for manager or operator. The manager username and password is also used by the web UI.
- **ip address <ip-addr> <ip-mask>**  
Set IP address and subnet mask.
- **ip default-gateway <ip-addr>**  
Set the default gateway IP address.
- **show ip**  
Show IP address, subnet mask and the default gateway.
- **show info**  
Show basic information, including system info, MAC address and firmware version.
- **dhcp**  
Set switch as dhcp client, it will get ip from dhcp server

**Note** If this command is set, the switch will reboot.

- **show dhcp**

Show dhcp enable/disable.

### Port Mirroring

Port monitoring is a feature to redirect the traffic occurring on every port to a designated monitoring port on the switch. With this feature, the network administrator can monitor and analyze the traffic on the entire LAN segment. In the switch, users can specify one port to be the monitoring port and any single port to be the monitored port. Users can also specify the direction of the traffic to be monitored. After properly configured, packets with the specified direction from the monitored ports are forwarded to the monitoring port.

#### Note

- The default Port Monitoring setting is disabled.
  - The analysis port is dedicated as a mirroring port with duplicated traffic flow from the mirrored port. The ordinary network traffic is not available for the analysis port.
  - Any trunk group and member port is not available for this function.
- **mirror-port <rx | tx | both> <port-id> <port-list>**

Set port monitoring information. (RX only|TX only|both RX and TX)

-rx specifies monitoring rx only.

-tx specifies monitoring tx only.

-both specifies monitoring both rx and tx.

The <port-id> command specifies the analysis port ID. This port receives traffic from all monitored ports.

The <port-list> command specifies the monitored port list.

- **show mirror-port**

Show port monitoring information.

### QoS

- QoS Mode:
  - **First Come First Service:** The sequence of packets sent is dependent on order of arrival.
  - **All High before Low:** High priority packets are sent before low priority packets.
  - **WRR (Weighted Round Robin):** Select the preference given to packets in the switch's high-priority queue. These options represent the number of higher priority packets sent before one lower priority packet is sent. For example, 8 Highest: 4 second-high means that the switch sends 8 highest-priority packets before sending 4 second high priority packets.
- **Qos Level:** 0-7 priority level can map to highest, second-high, second-low and lowest queue.

- **qos priority <first-come-first-service | all-high-before-low | weighted-round-robin> [<highest-weight>][<sechighweight>][<sec low -weight>] [<lowest-weight>]**  
Set 802.1p priority.  
e.g. qos priority weighted-round-robin 8,4,2,1
- **qos level < highest | second-high | second-low | lowest > <level-list>**  
Set priority levels to highest, second-high, second-low and lowest.  
The <level-list> command specifies the priority levels, set as high or low; the level must be between 1 and 7.  
e.g. qos level highest 7  
e.g. qos level lowest 4
- **show qos**  
Show QoS configurations, including 802.1p priority, priority level. e.g. show qos.
  - QoS mode: first come first service  
Highest weight: 8  
Second High weight: 4  
Second Low weight: 2  
Lowest weight: 1
  - 802.1p priority [0-7]: Lowest Lowest SecLow SecLow SecHigh SecHigh Highest Highest
- **port priority <disable | [0-7]> [<port-list>]**  
Set port priority.  
The [<port-list>] command specifies the ports to be set. If not entered, all ports are set, e.g. port priority disable 1-5.

### Commands for MAC

- **clear mac-address-table**  
Clear all dynamic MAC address table entries.
- **mac-address-table static <mac-addr> <vlan-id> <port-id | port-list>**  
Set static unicast or multicast MAC address. If a multicast MAC address (address beginning with 01:00:5E) is supplied, the last parameter must be a port-list. Otherwise, it must be a port-id.
- **no mac-address-table static <mac-addr> <vlan-id>**  
Delete static unicast or multicast MAC address table entries.
- **show mac-address-table**  
Display MAC address table entries.
- **show mac-address table static**  
Display static MAC address table entries.
- **show mac-address-table multicast**

Display multicast related MAC address table.

- **smac-address-table static <mac-addr> <vlan-id> <port-id | port-list>**

Set static unicast or multicast MAC address in a secondary MAC address table. If a multicast MAC address (address beginning with 01:00:5E) is supplied, the last parameter must be a port-list. Otherwise, it must be a port-id.

- **show smac-address-table**

Display secondary MAC address table entries.

- **show smac-address-table multicast**

Display multicast related secondary MAC address table.

- **[no] filter <mac-addr> <vlan-id>**

Set MAC address filter. The packets will be filtered if both the destination MAC address and the VLAN tag match the filter entry. If the packet does not have a VLAN tag, then it matches an entry with VLAN ID 1.

- **show filter**

Display filter MAC address table.

### MAC Limits

MAC limit allows users to set a maximum number of MAC addresses to be stored in the MAC address table. The MAC addresses chosen to be stored in the MAC address table is the result of first-come-first-save policy. Once a MAC address is stored in the MAC address table, it stays until it is aged out. When an “opening” is available, the first new MAC address is automatically stored in that opening by the switch. All packets from the MAC addresses not in the MAC address table should be blocked. Users can configure the MAC limit setting and fill in the new value.

- **mac-limit**

Enable MAC limit.

- **no mac-limit**

Disable MAC limit.

- **Mac-limit <port-list> <1-64>**

Set port MAC limit value, enter 0 to turn off the MAC limit of the port.

- **show mac-limit**

Show MAC limit information, including MAC limit enable/disable and per-port MAC limit setting.

### Protocol Related Commands

#### STP/RSTP

- **[no] spanning-tree**

Enable or disable spanning-tree.

- **spanning-tree forward-delay <4-30>**

Set spanning tree forward delay used, in seconds.

The <4-30> command specifies the forward delay, in seconds. Default value is 15.

**Note** The parameters must enforce the following relationships:

- $2 * (\text{hello-time} + 1) \leq \text{maximum-age} \leq 2 * (\text{forward-delay} - 1)$

- **spanning-tree hello-time <1-10>**

Set spanning tree hello time, in seconds.

The <1-10> command specifies the hello time, in seconds. Default value is 2.

**Note** The parameters must enforce the following relationships:

- $2 * (\text{hello-time} + 1) \leq \text{maximum-age} \leq 2 * (\text{forward-delay} - 1)$

- **spanning-tree maximum-age <6-40>**

Set spanning tree maximum age, in seconds.

The <6-40> command specifies the maximum age, in seconds. Default value is 20.

**Note** The parameters must enforce the following relationships:

- $2 * (\text{hello-time} + 1) \leq \text{maximum-age} \leq 2 * (\text{forward-delay} - 1)$

- **spanning-tree priority <0-61440>**

Set spanning tree bridge priority.

The <0-61440> command specifies the bridge priority. The value must be in steps of 4096.

- **spanning-tree port path-cost <1-200000000> [<port-list>]**

Set spanning tree port path cost.

<1-200000000> specifies the port path cost.

The [<port-list>] command specifies the ports to be set; null means all ports.

- **spanning-tree port priority <0-240> [<port-list>]**

Set spanning tree port priority.

The <0-240> command specifies the port priority. The value must be in steps of 16.

The [<port-list>] command specifies the ports to be set; null means all ports.

- **show spanning-tree**

Show spanning-tree information.

- **show spanning-tree port [<port-list>]**

Show spanning tree per port information.

The [<port-list>] command specifies the port to be shown. Null means all ports.



The remaining commands in this section are only for a system with RSTP (rapid spanning tree, 802.1w) capability.

- **spanning-tree protocol-version <stp | rstp>**  
Change spanning tree protocol version.  
stp specifies the original spanning tree protocol (STP,802.1d)  
rstp specifies rapid spanning tree protocol (RSTP,802.1w)
- **[no] spanning-tree port mcheck [<port-list>]**  
Force the port to transmit RST BPDUs. No format means do not force the port to transmit RST BPDUs.  
The [<port-list>] command specifies the ports to be set; null means all ports.
- **[no] spanning-tree port edge-port [<port-list>]**  
Set the port to be an edge connection; no format means the port is set as a non-edge connection.  
The [<port-list>] command specifies the ports to be set; null means all ports.
- **[no] spanning-tree port non-stp [<port-list>]**  
Disable or enable spanning tree protocol on this port.  
The [<port-list>] command specifies the ports to be set; null means all ports.
- **spanning-tree port point-to-point-mac <auto | true | false> [<port-list>]**  
Set the port to be point to point connection.  
auto specifies point to point link auto connection  
true specifies point to point link is true  
false specifies point to point link is fals.  
The [<port-list>] command specifies the ports to be set; null means all ports.

### MSTP

- **[no] spanning-tree**  
Enable or disable multiple spanning tree.
- **[no] spanning-tree debug**  
Enable or disable multiple spanning tree debugging information.
- **spanning-tree forward-delay <4-30>**  
Set spanning tree forward delay of CIST, in seconds.  
<4-30> specifies the forward delay, in seconds. Default value is 15.

**Note** The parameters must enforce the following relationships:

- $2 * (\text{hello-time} + 1) \leq \text{maximum-age} \leq 2 * (\text{forward-delay} - 1)$

- **spanning-tree hello-time <1-10>**

Set spanning tree hello time of CIST, in seconds.

<1-10> specifies the hello time, in seconds. Default value is 2.

**Note** The parameters must enforce the following relationships:

- $2 * (\text{hello-time} + 1) \leq \text{maximum-age} \leq 2 * (\text{forward-delay} - 1)$

- **spanning-tree maximum-age <6-40>**

Set spanning tree maximum age of CIST, in seconds.

<6-40> specifies the maximum age, in seconds. Default value is 20.

**Note** The parameters must enforce the following relationships:

- $2 * (\text{hello-time} + 1) \leq \text{maximum-age} \leq 2 * (\text{forward-delay} - 1)$

- **spanning-tree priority <0-61440>**

Set spanning tree bridge priority of CIST and all MSTIs.

<0-61440> specifies the bridge priority. The value must be in steps of 4096. Default value is 32768.

- **spanning-tree protocol-version { stp | mstp }**

Set spanning tree protocol version of CIST.

stp specifies the original spanning tree protocol (STP,802.1d)

mstp specifies the multiple spanning tree protocol (MSTP,802.1s)

- **spanning-tree max-hops <1-40>**

Set spanning tree bridge maximum hops of CIST and all MSTIs.

<1-40> specifies the bridge maximum hops. Default value is 20.

- **spanning-tree name [<name-string>]**

Set spanning tree bridge name of CIST.

The [<name-string>] command specifies the bridge name. Default name is null.

- **spanning-tree revision <1-65535>**

Set spanning tree bridge revision of CIST.

<1-65535> specifies the bridge revision. Default value is 0.

**Note** Where [<port-list>] is listed in the configurations below, this command is used to specify the ports to be set, unless stated otherwise. Null means all ports.

- **spanning-tree port path-cost <1-200000000> [<port-list>]**

Set spanning tree port path cost of CIST.

<1-200000000> specifies port path cost.

- **spanning-tree port priority <0-240> [<port-list>]**

Set spanning tree port priority of CIST.

<0-240> specifies the port priority. The value must be in steps of 16.

- **[no] spanning-tree port mcheck [<port-list>]**

Force the port of CIST to transmit MST BPDUs. No format means not force the port of CIST to transmit MST BPDUs.

- **[no] spanning-tree port edge-port [<port-list>]**

Set the port of CIST to be edge connection. No format means set the port of CIST to be non-edge connection.

- **[no] spanning-tree port non-stp [<port-list>]**

Disable or enable spanning tree protocol on the CIST port.

- **spanning-tree port point-to-point-mac <auto | true | false> [<port-list>]**

Set the port of CIST to be point to point connection.

-auto specifies point to point link auto connection.

-true specifies point to point link true.

-false specifies point to point link false.

- **spanning-tree mst <0-15> priority <0-61440>**

Set spanning tree bridge priority of MSTI.

<0-15> specifies the MSTI instance ID.

<0-61440> specifies the MSTI bridge priority. The value must be in steps of 4096. Default value is 32768.

- **spanning-tree mst <0-15> vlan [<vlan-list>]**

Set MSTI to map VLAN list.

<0-15> specifies the MSTI instance ID.

The [<vlan-list>] command specifies the mapped VLAN list. Null means all VLANs.

- **spanning-tree mst <0-15> port path-cost <1-200000000> [<port-list>]**

Set spanning tree port path cost of MSTI.

<1-200000000> specifies port path cost.

- **spanning-tree mst <0-15> port priority <0-240> [<port-list>]**

Set spanning tree port priority of MSTI.

<0-240> specifies the port priority. The value must be in steps of 16.

- **no spanning-tree mst <0-15>**

Delete the specific MSTI.

<0-15> specifies the MSTI instance ID.

- **show spanning-tree**  
Show spanning-tree information of CIST.
- **show spanning-tree port [<port-list>]**  
Show spanning tree port information of CIST.
- **show spanning-tree mst configuration**  
Show MST instance map.
- **show spanning-tree mst <0-15>**  
Show MST instance information.  
<0-15> specifies the MSTI instance ID.
- **show spanning-tree mst <0-15> port <1-26>**  
Show specific port information of MST instance.  
<0-15> specifies the MSTI instance ID.  
<1-26> specifies port number.
- **show vlan spanning-tree**  
Show per VLAN per port spanning tree status.

## SNMP

- **snmp /no snmp**  
Enable or disable SNMP.
- **show snmp status**  
Show enable or disable status of SNMP.
- **snmp system-name <name-str>**  
Set agent system name string.  
The <name-str> command specifies the system name string.  
e.g. snmp system-name SWITCH
- **snmp system-location <location-str>**  
Set agent location string.  
The <location-str> command specifies the location string.  
e.g. snmp system-location office
- **snmp system-contact <contact-str>**  
Set agent system contact string.  
The <contact-str> command specifies the contact string.  
e.g. snmp system-contact abc@sina.com
- **show snmp system**

Show SNMP system information.

- **snmp community <read-sysinfo-only | read-all-only | read-write-all> <community-str>**

Set SNMP community string.

The <community-str> command specifies the community string.

e.g. snmp community read-all-only public

- **no snmp community <community-str>**

Delete SNMP community string.

The <community-str> command specifies the community string.

e.g. no snmp community public

- **show snmp community**

Show SNMP community strings.

- **snmp trap <ip-addr> [<community-str>] [<1...65535>]**

Set SNMP trap receiver IP address, community string and port number.

The <ip-addr> command specifies the IP address.

The <community-str> command specifies the community string.

<1...65535> specifies the trap receiver port number.

e.g. snmp trap 192.168.200.1 public

- **no snmp trap <ip-addr> [<1...65535>]**

Remove trap receiver IP address and port number.

The <ip-addr> command specifies the IP address.

<1...65535> specifies the trap receiver port number.

e.g. no snmp trap 192.168.200.1

- **show snmp trap**

Show all trap receivers.

- **snmp group <group-name> <v1 | v2c | usm> <security-name>**

Join a group.

The <group-name> command specifies the group name.

The <v1 | v2c | usm> command specifies the security model.

The <security-name> command specifies the security name.

e.g. snmp group test usm testuser

- **no snmp group <v1 | v2c | usm> <security-name>**

Leave a group.

The <v1 | v2c | usm> command specifies the security model.

The <security-name> command specifies the security name.

e.g. no snmp group usm testuser

- **show snmp group**

Show group list.

- **snmp view <view-name> <included | excluded> <view-subtree> <view-mask>**

Add a view.

The <view-name> command specifies the view name.

The <included | excluded> command specifies the view type.

The <view-subtree> command specifies the view subtree (e.g. .1.3.6.1.2.1).

The <view-mask> command specifies the view mask, in hexadecimal digits.

e.g. snmp view testview included 1.3.6.1.2.1 0xff

- **no snmp view <view-name>**

Delete a view.

The <view-name> command specifies the view name.

e.g. no snmp view system

- **show snmp view**

Show view list.

- **snmp access <group-name> <v1 | v2c | usm> <noauth | auth | authpriv> <read-name> <write-name> <notify-name>**

Add an access control.

The <group-name> command specifies the group name.

The <v1 | v2c | usm> command specifies the security model.

The <noauth | auth | authpriv> command specifies the security level.

The <read-name> command specifies the access read view name.

The <write-name> command specifies the access write view name.

The <notify-name> command specifies the access notify view name.

e.g. snmp access test usm testauth all all all

- **no snmp access <group-name> <v1 | v2c | usm> <noauth | auth | authpriv>**

Delete an access control.

The <group-name> command specifies the group name.

The <v1 | v2c | usm> command specifies the security model.

The <noauth | auth | authpriv> command specifies the security level.

e.g. no snmp access test usm auth

- **show snmp access**  
Show access list.
- **snmp engine-id <enterprise-id> <engine-id>**  
Setup SNMPv3 engine ID.  
The <engine-id> command specifies the engine ID, in the format of text string.  
e.g. snmp engine-id 123456789123456789123456
- **show snmp engine-id**  
Show SNMPv3 engine ID.
- **snmp usm-user <user-name> [<md5 | none>]**  
Add SNMPv3 USM user.  
The <user-name> command specifies the user name.  
The <md5 | none> command specifies the authentication type.  
e.g. Create a user name as testuser and password as 12345678, use auth md5 then enter CLI command:
- **snmp usm-user testuser md5 <cr>**  
New password for authentication (8<=length<=32): 12345678<cr>  
Retype new password: 12345678<cr>
- **no snmp usm-user <user-name>**  
Delete SNMPv3 USM user.  
The <user-name> command specifies the user name.  
e.g. no snmp usm-user testuser
- **show snmp usm-user**  
Show all SNMPv3 USM users.

## IGMP

- **[no] igmp**  
Enable/disable IGMP snooping.
- **[no] igmp fastleave**  
Enable/disable IGMP snooping fast leave. If enabled, the switch will fast delete members who send a leave report, or else wait one second.
- **[no] igmp querier**  
Enable/disable IGMP snooping querier.
- **[no] igmp CrossVLAN**  
Enable/disable IGMP snooping CrossVLAN
- **[no] igmp debug**

Enable/disable IGMP snooping debugging output.

- **show igmp <status | router | groups | table>**

Show IGMP snooping information.

-**status** specifies IGMP snooping status and statistics information.

-**router** specifies IGMP snooping router's IP address.

-**groups** specifies IGMP snooping multicast group list.

-**table** specifies IGMP snooping IP multicast table entries.

- **igmp clear\_statistics**

Clear IGMP snooping statistics counters.

## 802.1x

This switch supports IEEE 802.1x standard, which provides port-based access control by validating the end user's authorization through an authentication (RADIUS) server. EAP- MD5/TLS/PEAP authentication types are supported for this switch.

- **[no] dot1x**

Enable or disable 802.1x.

- **radius-server host <ip-addr> <1024..65535> <1024..65535>**

Set radius server IP, port number and accounting port number.

The <ip-addr> command specifies server's IP address.

1st <1024..65535> specifies the server port number.

2nd <1024..65535> specifies the accounting port number.

- **radius-server key <key-str>**

Set 802.1x shared key.

The <key-str> command specifies shared key string.

- **radius-server nas <id-str>**

Set 802.1x NAS identifier.

The <id-str> command specifies NAS identifier string.

- **show radius-server**

Show radius server information, including radius server IP, port number, accounting port number, shared key and NAS identifier.

- **dot1x timeout quiet-period <0..65535>**

Set 802.1x quiet period (default: 60 seconds).

<0..65535> specifies the quiet period, in seconds.

- **dot1x timeout tx-period <0..65535>**



Set 802.1x Tx period (default: 15 seconds).

<0..65535> specifies the Tx period, in seconds.

- **dot1x timeout supplicant <1..300>**

Set 802.1x supplicant timeout (default: 30 seconds).

<1..300> specifies the supplicant timeout, in seconds.

- **dot1x timeout radius-server <1..300>**

Set radius server timeout (default: 30 seconds).

<1..300> specifies the radius server timeout, in seconds.

- **dot1x max-req <1..10>**

Set 802.1x maximum request retries (default: 2 times).

<1..10> specifies the maximum request retries.

- **dot1x timeout re-authperiod <30..65535>**

Set 802.1x re-auth period (default: 3600 seconds).

<30..65535> specifies the re-auth period, in seconds.

- **show dot1x**

Show 802.1x information, quiet period, Tx period, supplicant timeout, server timeout, maximum requests and re-auth period.

- **dot1x port <fu | fa | au | no> <port-list>**

Set 802.1x per port information.

-fu specifies forced unauthorized.

-fa specifies forced authorized.

-au specifies authorization.

-no specifies disable authorization.

The <port-list> command specifies the ports to be set.

- **show dot1x port**

Show 802.1x per port information.

### **DHCP Relay & Option82**

- **[no] dhcp-option82**

Enable/disable DHCP option82 function.

- **[no] dhcp-relay**

Enable/disable DHCP relay function.

- **dhcp-option82 <enable | disable> <LIST>**

Enable/disable port-based option82 function.

- **dhcp-relay <enable | disable> <LIST> <IP address>**  
Enable/disable port-based DHCP relay function.
- **dhcp router <LIST>**  
Set DHCP router port.
- **show dhcp configuration**  
Show DHCP configuration information.

### Syslog

- **syslog-server <server-ip> <logging-level>**  
Setting the syslog server and logging level.  
The <server-ip> command specifies the syslog server IP.  
The <logging-level> command specifies the logging level (0: none; 1: major; 2: all).
- **show syslog-server**  
Display the syslog server IP and logging level.

### SSH

- **ssh <v1 | v2 | all>**  
Enable ssh function.  
The <v1 | v2 | all> command specifies which ssh version to support.
- **no ssh**  
Disable ssh function.

### Reboot Switch

- **erase startup-config**  
Reset configurations to default factory settings at next boot time.
- **boot**  
Restart/Reboot (warm-start) the switch.

### TFTP Function

- TFTP Firmware Update  
copy tftp firmware <ip-addr> <remote-file>  
Download firmware from TFTP server.  
The <ip-addr> command specifies the IP address of the TFTP server.  
The <remote-file> command specifies the file to be downloaded from the TFTP server.
- Restore Configure File

```
copy tftp <running-config | flash> <ip-addr> <remote-file>
```

Retrieve configuration from the TFTP server. If the remote file is the text file of CLI commands, use the keyword `running-config`. If the remote file is the configuration flash image of the switch instead, use the keyword `flash`.

The `<ip-addr>` command specifies the IP address of the TFTP server.

The `<remote-file>` command specifies the file to be downloaded from the TFTP server.

- Backup Configure File

```
copy <running-config | flash> tftp <ip-addr> <remote-file>
```

Send configuration to the TFTP server. To save as a text file of CLI commands, use the keyword `running-config`. To save as a flash image instead, use the keyword `flash`.

The `<ip-addr>` command specifies the IP address of the TFTP server.

The `<remote-file>` command specifies the file to be backed up to the TFTP server.

### Access Control List

Packets that can be forwarded or dropped by ACL rules include IPv4 or non-IPv4 packets. This switch can be used to block packets by maintaining a table of packet fragments indexed by source and destination IP address, protocol, and so on.

**Note** This function is available only in the 802.1q VLAN enabled environment.

#### IPv4 ACL commands

- **no acl <group id>**

Delete ACL group.

The `<group id>` command specifies the group id (1-220).

e.g. `no acl 1`

- **no acl count <group id>**

Reset the ACL group count.

The `<group id>` command specifies the group id (1-220).

- **Enable/Disable acl <group id>**

Reset the ACL group count.

The `<group id>` command specifies the group id (1-220).

- **Enable/Disable acl <group id>**

Reset the ACL group count.

The `<group id>` command specifies the group id (1-220).

- **show acl [<group id>]**

Show all or ACL group information by group id.

The <group id> command specifies the group id, null means all valid groups.

e.g. show acl 1

Group Id : 1

-----

Action : Permit

Rules:

Vlan ID : Any

IP Fragment : Uncheck

Src IP Address : Any

Dst IP Address : Any

L4 Protocol : Any

Port ID : Any

Hit Octet Count : 165074

Hit Packet count : 472

- **acl (add|edit) <group id> (permit|deny) <0-4094> ipv4 <0-255> A.B.C.D A.B.C.D A.B.C.D A.B.C.D (check|unCheck) <0- 65535> <0-26>**

Add or edit ACL group for IPv4 packets.

(add|edit) specifies the operation.

The <group id> command specifies the group id (1~220).

(permit|deny) specifies the action. permit: permit packet cross switch; deny: drop packet.

<0-4094> specifies the VLAN id; 0 means don't care.

<0-255> specifies the IP protocol; 0 means don't care.

1st A.B.C.D specifies the Source IP address; 0.0.0.0 means don't care.

2nd A.B.C.D specifies the Mask; 0.0.0.0 means don't care, 255.255.255.255 means compare all.

3rd A.B.C.D specifies the Destination IP Address; 0.0.0.0 means don't care.

4th A.B.C.D specifies the Mask; 0.0.0.0 means don't care, 255.255.255.255 means compare all.

(check|unCheck) specifies the IP Fragment. check: Check IP fragment field; unCheck: Not check IP fragment field.

<0-65535> specifies the Destination port number if TCP or UDP; 0 means don't care.

<0-26> specifies the Port id; 0 means don't care.

e.g. acl add 1 deny 1 ipv4 0 192.168.1.1 255.255.255.255 0.0.0.0 0.0.0.0 unCheck 0 0

This ACL rule will drop all packets from IP 192.168.1.1 with VLAN id=1 and IPv4.

- **acl (add|edit) <group id> (qosvoip) <0-4094> <0-7> <0-1F> <0-1F> <0-FF> <0-FF> <0-FFFF> <0-FFFF> <0-FFFF> <0-FFFF>**

Add or edit ACL group for Ipv4.

(add|edit) specifies the operation.

The <group id> command specifies the group id (1-220).

(qosvoip) specifies the action, do qos voip packet adjustment.

<0-4094> specifies the VLAN id; 0 means don't care.

<0-1F> specifies the port ID value.

<0-1F> specifies the port ID mask.

<0-FF> specifies the protocol value.

<0-FF> specifies the protocol mask.

<0-FFFF> specifies the source port value.

<0-FFFF> specifies the source port mask.

<0-FFFF> specifies the destination port value.

<0-FFFF> specifies the destination mask.

e.g. acl add 1 qosvoip 1 7 1 1 0 0 0 0 0

#### *Non-IPv4 ACL commands*

- **no acl <group id> and show acl [<group id>]**

The commands are the same as in Ipv4 ACL commands.

- **acl (add|edit) <1-220> (permit|deny) <0-4094> nonipv4 <0-65535>**

Add or edit ACL group for non-Ipv4.

(add|edit) specifies the operation.

The <group id> command specifies the group id (1-220).

(permit|deny) specifies the action, permit: permit packet cross switch; deny: drop packet.

<0-4094> specifies the VLAN id; 0 means don't care.

<0-65535> specifies the Ether Type; 0 means don't care.

e.g. acl add 1 deny 0 nonipv4 2054

This ACL rule will drop all packets for ether type 0x0806 and non-IPv4.

#### **SIP/SMAC Binding**

Source IP (SIP) / Source MAC (SMAC) address binding is another type of ACL rule to provide secured access to the switch. Only traffic that matches all criteria of the specified source IP address, source MAC address, VLAN ID and port number can be allowed to access to the switch. This function is also called IP-MAC lock.

- **bind**

Enable binding function.

- **no bind**

Disable binding function.

- **no bind <group id>**

Delete Binding group.

The <group id> command specifies the group id (1-220).

e.g. no bind 1

- **show bind [<group id >]**

Show Binding group information.

The <group id> command specifies the group id (1-220); null means all valid groups.

e.g. show bind 1

- **bind add < group id > A:B:C:D:E:F <0-4094> A.B.C.D <1-26>**

Add Binding group.

The < group id > command specifies the group id (1-220).

1st A.B.C.D specifies the MAC address.

<0-4094> specifies the VLAN id; 0 means don't care.

2nd A.B.C.D specifies the Source IP address; 0.0.0.0 means don't care.

3rd A.B.C.D specifies the IP Address.

<1-26> specifies the Port id.

e.g. bind add 1 00:11:22:33:44:55 0 192.168.1.1 1. This Binding rule will permit all packet cross switch from device's IP is

192.168.1.1 and MAC is 00:11:22:33:44:55 and this device connect to switch port id=1.



## Chapter 4 **Contacting Patton for Assistance**

### **Chapter contents**

Introduction .....	97
Contact Information .....	97
Patton Support Headquarters in the USA .....	97
Alternate Patton Support for Europe, Middle East, and Africa (EMEA) .....	97
Warranty Service and Returned Merchandise Authorizations (RMAs) .....	97
Warranty Coverage .....	97
Out-of-warranty service .....	98
Returns for credit .....	98
Return for credit policy .....	98
RMA Numbers .....	98
Shipping instructions .....	98



## Introduction

---

This chapter contains the following information:

- “Contact Information”—describes how to contact Patton technical support for assistance.
- “Warranty Service and Returned Merchandise Authorizations (RMAs)”—contains information about the warranty and obtaining a return merchandise authorization (RMA).

## Contact Information

---

Patton Electronics offers a wide array of free technical services. If you have questions about any of our other products we recommend you begin your search for answers by using our technical knowledge base. Here, we have gathered together many of the more commonly asked questions and compiled them into a searchable database to help you quickly solve your problems.

### **Patton Support Headquarters in the USA**

- Online support: available at [www.patton.com](http://www.patton.com)
- E-mail support: e-mail sent to [support@patton.com](mailto:support@patton.com) will be answered within 1 business day
- Telephone support: standard telephone support is available five days a week—from 8:00 am to 5:00 pm EST (1300 to 2200 UTC/GMT)—by calling +1 (301) 975-11000
- Fax: +1 (301) 869-9293

### **Alternate Patton Support for Europe, Middle East, and Africa (EMEA)**

- Online support: available at [www.patton.com](http://www.patton.com)
- E-mail support: e-mail sent to [support@patton.com](mailto:support@patton.com) will be answered within 1 business day
- Telephone support: standard telephone support is available five days a week—from 9:00 am to 5:30 pm CET (0800 to 1630 UTC/GMT)—by calling +41 (0)31 985 25 55
- Fax: +41 (0)31 985 25 26

## Warranty Service and Returned Merchandise Authorizations (RMAs)

---

Patton Electronics is an ISO-9001 certified manufacturer and our products are carefully tested before shipment. All of our products are backed by a comprehensive warranty program.

**Note** If you purchased your equipment from a Patton Electronics reseller, ask your reseller how you should proceed with warranty service. It is often more convenient for you to work with your local reseller to obtain a replacement. Patton services our products no matter how you acquired them.

### **Warranty Coverage**

Our products are under warranty to be free from defects, and we will, at our option, repair or replace the product should it fail within one year from the first date of shipment. Our warranty is limited to defects in workmanship or materials, and does not cover customer damage, lightning or power surge damage, abuse, or unauthorized modification.

### *Out-of-warranty service*

Patton services what we sell, no matter how you acquired it, including malfunctioning products that are no longer under warranty. Our products have a flat fee for repairs. Units damaged by lightning or other catastrophes may require replacement.

### *Returns for credit*

Customer satisfaction is important to us, therefore any product may be returned with authorization within 30 days from the shipment date for a full credit of the purchase price. If you have ordered the wrong equipment or you are dissatisfied in any way, please contact us to request an RMA number to accept your return. Patton is not responsible for equipment returned without a Return Authorization.

### *Return for credit policy*

- Less than 30 days: No Charge. Your credit will be issued upon receipt and inspection of the equipment.
- 30 to 60 days: We will add a 20% restocking charge (crediting your account with 80% of the purchase price).
- Over 60 days: Products will be accepted for repairs only.

### **RMA Numbers**

RMA numbers are required for all product returns. You can obtain an RMA by doing one of the following:

- Completing a request on the RMA Request page in the *Support* section at [www.patton.com](http://www.patton.com)
- By calling +1 (301) 975-11000 and speaking to a Technical Support Engineer
- By sending an e-mail to [returns@patton.com](mailto:returns@patton.com)

All returned units must have the RMA number clearly visible on the outside of the shipping container. Please use the original packing material that the device came in or pack the unit securely to avoid damage during shipping.

### *Shipping instructions*

The RMA number should be clearly visible on the address label. Our shipping address is as follows:

**Patton Electronics Company**

RMA#: xxxx

7622 Rickenbacker Dr.

Gaithersburg, MD 20879-4773 USA

Patton will ship the equipment back to you in the same manner you ship it to us. Patton will pay the return shipping costs.

## Appendix A **Compliance Information**

---

### **Chapter contents**

Compliance .....	100
EMC .....	100
Low-Voltage Directive (Safety) .....	100
Radio and TV Interference .....	100
CE Declaration of Conformity .....	100
Authorized European Representative .....	100

## Compliance

---

### **EMC**

- FCC Part 15, Class A
- EN55022, Class A
- EN55024

### **Low-Voltage Directive (Safety)**

- UL 60950-1/CSA C22.2 No. 60950-1
- IEC/EN60950-1, 2nd edition

## Radio and TV Interference

---

The ForeFront router generates and uses radio frequency energy, and if not installed and used properly—that is, in strict accordance with the manufacturer’s instructions—may cause interference to radio and television reception. The ForeFront router have been tested and found to comply with the limits for a Class A computing device in accordance with specifications in Subpart B of Part 15 of FCC rules, which are designed to provide reasonable protection from such interference in a commercial installation. However, there is no guarantee that interference will not occur in a particular installation. If the ForeFront router does cause interference to radio or television reception, which can be determined by disconnecting the unit, the user is encouraged to try to correct the interference by one or more of the following measures: moving the computing equipment away from the receiver, re-orienting the receiving antenna and/or plugging the receiving equipment into a different AC outlet (such that the computing equipment and receiver are on different branches).

## CE Declaration of Conformity

---

Patton Electronics, Inc declares that this device is in compliance with the essential requirements and other relevant provisions of Directive 2004/108/EC relating to electromagnetic compatibility, Directive 2006/95/EC relating to electrical equipment designed for use within certain voltage limits and Directive 2011/65/EC relating to RoHS compliance. The Declaration of Conformity may be obtained from Patton Electronics, Inc at [www.patton.com/certifications](http://www.patton.com/certifications).

The safety advice in the documentation accompanying this device shall be obeyed. The conformity to the above directive is indicated by CE mark on the device.

## Authorized European Representative

---

D R M Green

European Compliance Services Limited.

Greyfriars Court

Paradise Square

Oxford, OX1 1BE, UK

## Appendix B **Specifications**

---

### **Chapter contents**

Interfaces .....	102
LED Indicators .....	102
Standards Support .....	102
Protocol Support .....	102
Security .....	102
Device Management .....	103
Physical .....	103

## Interfaces

---

24 VDSL2 Ports

Two RJ-45 100/1000Mbps Ethernet Combo Ports

Management Ethernet

1 x RS-232 Serial Console

POTS Splitter

## LED Indicators

---

SYS, ALM, LINK, ACT

24 x VDSL LEDs

## Standards Support

---

VDSL2 ITU-T G.993.2

VDSL2 Profiles: 8a, 8b, 8c, 8d, 12a, 12b, 17a and 30a

802.1d L2 Bridging

DHCP Server/Client/Relay

IEEE 802.1q VLAN (Port-based VLAN and Protocol-Based VLAN)

VLAN Stacking (Q-in-Q)

IEEE 802.1p Spanning Tree Protocol (STP)

IEEE 802.3ad Link Aggregation

## Protocol Support

---

IGMP Snooping/Proxy v1, v2 and v3

Multicast Forwarding with IGMP Snooping v1 and v2 (RFC 1112 and RFC 2236)

Multicast MAC address mapping

Up to 512 Multicast Channels

Profile-based Multicast Access Control (up to 24 profiles)

Fast and Normal Leave Modes

## Security

---

L2 Frame Filtering by MAC Addresses

L3 Frame Filtering by IP Addresses, protocol ID, and TCP/UDP

DHCP and ARP Broadcasting Frames Filtering

Support Secured Forwarding

## Device Management

---

Web-based Graphical User Interface, Telnet, CLI and SSH

Support OAM&P Functions

Support VLAN Priority Queue (IEEE 802.1p)

Support CoS, ToS, DSCP, etc.

Support SNMP v1/v2/v3 and MIB I/II

## Physical

---

Case: 1.5U High Pizza-Box Type

**Dimensions:** 10.2W x 5.7H x 1.6D inch (260W x 143H x 39.5D mm)

**Weight:** 4 lbs

**Operating temperature:** -10°C to 50°C

**Storage Temperature:** -40°C to 70°C

**Relative Humidity:** Up to 95% (non-condensing)