

## **5224AV-2GBE/2SFP**

**IP Digital Subscriber Line Access Multiplexer**

## **Web Configuration Tool Guide**

Part Number A0-31-0130-2.3  
Issue 2.3, August 2011

# **DATA-CONNECT**

*The Right Connection!*

Contents

1

Using the Web Interface

1

1.1

Navigation .....

1

1.2

Title Bar Icons.....

2

1.3

Ending a Session.....

2

2

Using the Online Help

3

3

System Description

4

3.1

Features .....

4

4

Status 5

4.1

Status / Bridge .....

5

4.2

Status / Front Panel .....

6

4.3

Status / Interface / DSL Port Rates .....

8

4.4

Status / Interface / DSL Port Statistics.....

10

4.5

Status / Interface / DSL Performance.....

12

4.6

Status / Interface / Ethernet Statistics.....

16

4.7

Status / Interface / LLDP Statistics .....

31

4.8

Status / Interface / VLAN Counter .....

32

4.9

Status / Mgmt Radius Status.....

33

4.10

Status / Multicast.....

35

4.11

Status / Users .....

39

5

System

41

5.1

System / Alarms & Events.....

41

5.2

System / Boot Loader .....

46

5.3

System / Firmware.....

47

5.4

System / Options .....

50

5.5

System / Restart .....

51

5.6

System / Save & Restore.....

52

5.7

System / System Information .....

55

5.8

System / User Administration.....

58

6

Configuration

60

6.1

Configuration / Auth (802.1x - RADIUS) / DSL Port Authentication / Server Configuration.....

60

6.2

Configuration / Auth (802.1x - RADIUS) / DSL Port Authentication / Port Configuration .....

63

6.3

Configuration / Auth (802.1x - RADIUS) / Mgmt Port Authentication .....

67

6.4

Configuration / Bridge / Interface / Profiles / Alarm Threshold Profiles .....

72

6.5

Configuration / Bridge / Interface / Profiles / xDSL Configuration Profiles.....

74

6.6

Configuration / Bridge / Interface / Setup / ADSL Bridge Port.....

85

6.7

Configuration / Bridge / Interface / Setup / Uplink Bridge Port.....

89

6.8

Configuration / Bridge / Interface / Setup / VDSL Bridge Port.....

95

6.9

Configuration / Bridge / Interface / Setup / xDSL Interface .....

99

6.10

Configuration / LLDP / Link Layer Discovery Protocol (LLDP).....

101

6.11

Configuration / Bridge / Policer / Policer – Rate Limit Profile .....

107

# DATA-CONNECT

*The Right Connection!*

Contents

6.12 Configuration / Bridge / Policer / Policer – Broadcast Select .....	110
6.13 Configuration / Bridge / Policer / Policer – Port Select .....	111
6.14 Configuration / Bridge / Policer / Policer – VLAN Select.....	112
6.15 Configuration / Bridge / System-Wide Services.....	113
6.16 Configuration / Cluster Configuration .....	116
6.17 Configuration / Cluster Legacy.....	120
6.18 Configuration / DHCP / DHCP (PPPoE) Config.....	121
6.19 Configuration / DHCP / DHCP (PPPoE) Port .....	123
6.20 Configuration / DHCP / DHCP Clients List .....	124
6.21 Configuration / DHCP / DHCP Server Profile Config .....	125
6.22 Configuration / DHCP / DHCP Server Profile Select .....	126
6.23 Configuration / DHCP / DHCP Static IP Config .....	127
6.24 Configuration / Filtering / Access Control List (ACL).....	128
6.25 Configuration / Filtering / Anti Arp Spoofing (per Port) .....	129
6.26 Configuration / Filtering / Filter Rules .....	131
6.27 Configuration / Filtering / IP Filtering .....	133
6.28 Configuration / Forwarding / Bridge .....	134
6.29 Configuration / Forwarding / Bridge Table - Static .....	135
6.30 Configuration / Forwarding / Fdb Delete Control .....	136
6.31 Configuration / Forwarding / Secure Forwarding .....	137
6.32 Configuration / IGMP / Configure IGMP .....	139
6.33 Configuration / IGMP / IGMP ACL Profiles .....	143
6.34 Configuration / IGMP / IGMP ACL Profile Select .....	146
6.35 Configuration / Management / Mgmt Link Config .....	147
6.36 Configuration / Management / SNMP.....	150
6.37 Configuration / Management / SNTP .....	154
6.38 Configuration / Management / Syslog .....	155
6.39 Configuration / STP / STP Bridge.....	156
6.40 Configuration / STP / STP Port .....	158
6.41 Configuration / Traffic Prioritization / ADSL Traffic Desc Select .....	160
6.42 Configuration / Traffic Prioritization / Traffic Desc Profile .....	161
6.43 Configuration / Traffic Prioritization / Uplink VPMT Configure.....	163
6.44 Configuration / Traffic Prioritization / VDSL VPMT Profile.....	164
6.45 Configuration / Traffic Prioritization / VDSL VPMT Select.....	166
6.46 Configuration / VLAN / Static Multicast Pass Through.....	167
6.47 Configuration / VLAN Configuration / VLAN – Egress Rate Limit .....	169
6.48 Configuration / VLAN Configuration / VLAN – Members & State .....	170
6.49 Configuration / VLAN Configuration / VLAN – Priority Remark.....	173
6.50 Configuration / VLAN Configuration / VLAN – Protocol Based .....	176
6.51 Configuration / VLAN Configuration / VLAN – Rate Limit .....	178
6.52 Configuration / VLAN Configuration / VLAN – Translation.....	179
<b>7 Diagnostics .....</b>	<b>183</b>
7.1 Diagnostics / DELT .....	183
7.2 Diagnostics / Power Mode .....	187
7.3 Diagnostics / Power-On Self-Test (POST) .....	188
<b>Appendix .....</b>	<b>189</b>
A. Alarm Table .....	190
B. Event Table .....	192

## 1 Using the Web Interface

This online Help contains information about the Web interface. For tips about using the Help screens, click [here](#).

For an introduction to the 5224AV-2GBE/2SFP IP DSLAM, click [here](#).

### Web Browser Support

IE 7 with the following default settings is recommended:

Language script	Latin based
Web page font	Times New Roman
Plain text font	Courier New
Encoding	Western European (windows)
Text size	Medium

Firefox 3.6.3 with the following default settings is recommended:

Web page font	Times New Roman
Encoding	Western (ISO-8859-1)
Text size	16

Without the default setting, the browser may have problem with displaying the web pages.

*Note 1:* You can reset your IE 7 browser to its default settings by clicking Tool → Internet Options → Advanced → Reset → Reset.

*Note 2:* The other browser IE 6/8, other version of Firefox may have some problems!

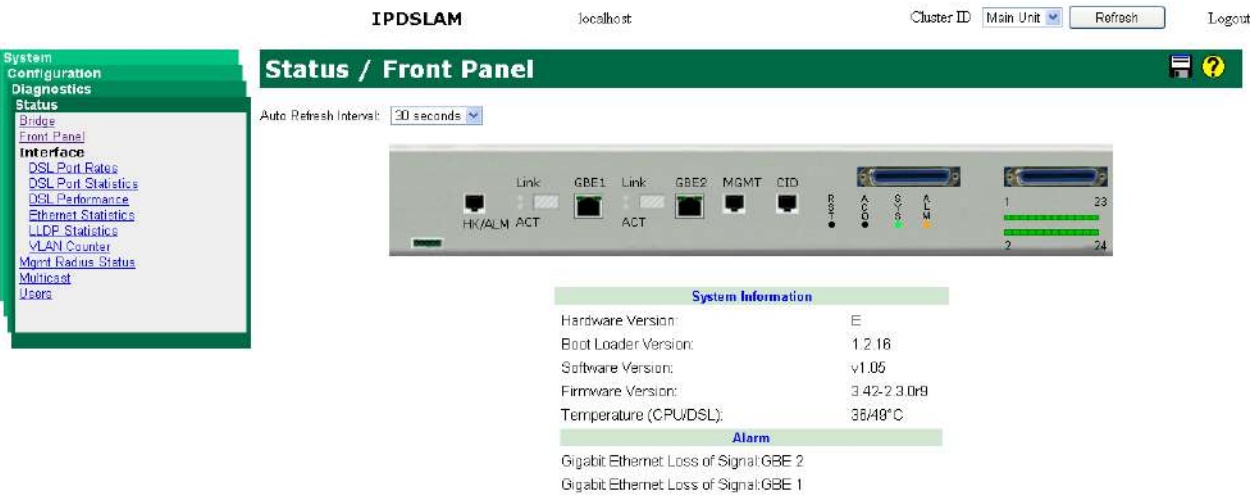
### 1.1 Navigation

All main screens of the web interface can be reached by clicking on hyperlinks in the four menu boxes on the left side of the screen:

- **Status** - Display statistics, status, and contents of memory
- **Diagnostics** - Start and stop tests
- **Configuration** - Configure the system, interfaces, and filters
- **System** - Display system information, download firmware, back up configurations, and modify users

# DATA-CONNECT

The Right Connection!



## 1.2 Title Bar Icons

### Help Button

For more information about any screen, click on the Help button on the screen. Help is displayed in a new window.

### Save Button

If any unsaved change has been made to the configuration (by you during this or a prior session, or by any other administrator using the web interface or the Command Line Interface), a Save icon appears in the title line. To save the running configuration to the startup configuration:


- 1 Click on the Save icon. The System/Save and Restore screen appears.
- 2 Click on Submit next to *Data Control Action* drop-down list on top of System/Save and Restore screen.

## 1.3 Ending a Session

To end a session, close your web browser. This prevents an unauthorized user from accessing the system using your user name and password.



## 2 Using the Online Help

Each screen has a  Help button that invokes a page of information relevant to the particular screen. The Help is displayed in a new window.

Each web page of Configuration/Status/System/Diagnostics functions has a corresponding help page.

## 3 System Description

The 5224AV-2GBE/2SFP is a rack-mountable pizza-box VDSL2 IP DSLAM. It supports two Gigabit Ethernet (GbE) trunk interfaces and 24 VDSL2 ports (ADSLx backward compatible) at line side. It's ideal for deployment in space-constrained indoor MDU or external cabinets.

The 5224AV-2GBE/2SFP takes advantage of VDSL2 technology with core IP switching functionality to participate in the competition of broadband last mile. This allows operators to easily offer services such as IPTV, VoIP, HDTV, VOD, videoconferencing, Internet access and advanced voice services at the same copper line.

### 3.1 Features

- Highly compact solution that provides 24 VDSL2 only by 1U space and stackable for higher port density
- Scalable solution that allow new revenue to be generated with minimum installation time and expense
- Equipped with fan and air filter, low power requirements plus full diagnostics and alarm reporting capability
- Standard-based with remote configuration and software upgrade that help service providers minimize daily operational costs
- Wide operating temperature range from -40°C ~ 65°C
- Provide two combo GBE trunk interfaces with both RJ-45 and SFP ports, and the priority for these two types of connectors (RJ-45 first or SFP first) is configurable
- Support Link Aggregation in IEEE 802.3ad that allows 2 GBE links to be aggregated together as a logical link. Support both LACP protocol (dynamic) for load sharing and failover in case of loss of Ethernet link
- Support SNTP to automatically calibrate the time and date of the system
- Support on board thermal sensor to detect temperature conditions with software configurable thresholds that generate SNMP traps and syslog alarm entries
- Provide SSH (Secure Shell) for more secure remote operation
- Meet CE requirement



## 4 Status

### 4.1 Status / Bridge

Use the Status/Bridge screen to display the status of the transparent forwarding database. The forwarding table will reveal the information of MAC addresses that are learned or statically configured on a specific bridge port.

Status / Bridge

Auto Refresh Interval: 30 seconds

Previous Command Result: Normal

Bridge Table(Forwarding Table)

No. From 1 To 128

Query

No.	Source MAC	Physical Port	Status	VID	Aging Bit	Process Mode
-----	------------	---------------	--------	-----	-----------	--------------

To view the information in forwarding database, in the field “No. From...To...” select the range of entry number in the forwarding database to be displayed. Click on Query button to get most recent status of MAC addresses forwarding.

### 4.2 Status / Front Panel

Use the Status/Front Panel screen to view the status of front panel status remotely. This screen also displays some system information including HW/FW/SW version, CPU/DSL temperature, current alarm, etc.

Status / Front Panel

Auto Refresh Interval: 30 seconds

HK/ALM

Link

GBE1

Link

GBE2

MGMT

CID

ROT

AOD

SYS

ALM

ACT

ACT

1

23

2

24

System Information

Hardware Version:

E

Boot Loader Version:

1.2.16

Software Version:

v1.06

Firmware Version:

3.42-2.3.0-r9

Temperature (CPU/DSL):

37/49°C

Alarm

Gigabit Ethernet Loss of Signal: GBE 2

Gigabit Ethernet Loss of Signal: GBE 1

You can click on the interfaces on the faceplate to jump to related screens:

Click on . . .	To jump to . . .
HK/ALM Port	System/Alarms & Events
MGMT Port	Configuration/Management/Mgmt Link Config
DSL Port 1~24 (Connector)	Configuration/Bridge/Interface/Setup/xDSL Interface
GBE1/GBE2 port	Status/Interface/Ethernet statistics
DSL1~DSL24 (DSL Ports)	Status/Interface/DSL Port Rates

Front Panel LEDs



LED	Color	Indication / Condition
SFP1 - LINK	Green - On	Valid network connection established
SFP2 - LINK	Off	Disconnection
SFP1- ACT	Off	Disconnection
SFP2- ACT	Off	Disconnection
SYS	Red	Self-test fail
	Green	Normal Operation
ALM	Red	Major alarm set
	Red – Blink	Major and Minor alarm set
	Amber	Minor alarm set
	Green	Normal operation

Front Panel Buttons

Button	Description
RST	A button for hardware resetting.
ACO	For Alarm Cut Off service.

### 4.3 Status / Interface / DSL Port Rates

Use the Status/Interface/DSL Port Rates screen to view the VDSL Status including upstream and downstream rate of each DSL port, and VDSL Inventory including serial number, vendor ID, etc.

Select a tab (DSL Status, DSL Inventory) on top of the screen first.

#### DSL Status

DSL StatusDSL Inventory

Auto Refresh Interval: 30 seconds

Port	OpState	Rate(DS/US)[kbps]	Config. Profile	Alarm Profile	Alarm
Port-1	Idle	0 / 0	DEFVAL	DEFVAL	Normal
Port-2	Idle	0 / 0	DEFVAL	DEFVAL	Normal
Port-3	Idle	0 / 0	DEFVAL	DEFVAL	Normal
Port-4	Idle	0 / 0	DEFVAL	DEFVAL	Normal
Port-5	Idle	0 / 0	DEFVAL	DEFVAL	Normal
Port-6	Idle	0 / 0	DEFVAL	DEFVAL	Normal
Port-7	Idle	0 / 0	DEFVAL	DEFVAL	Normal
Port-8	Idle	0 / 0	DEFVAL	DEFVAL	Normal
Port-9	Idle	0 / 0	DEFVAL	DEFVAL	Normal
Port-10	Idle	0 / 0	DEFVAL	DEFVAL	Normal
Port-11	Idle	0 / 0	DEFVAL	DEFVAL	Normal
Port-12	Idle	0 / 0	DEFVAL	DEFVAL	Normal
Port-13	Idle	0 / 0	DEFVAL	DEFVAL	Normal
Port-14	Idle	0 / 0	DEFVAL	DEFVAL	Normal
Port-15	Idle	0 / 0	DEFVAL	DEFVAL	Normal

Field	Description
Port	Shows the number of physical line port.
OpState	Shows current operational status of the line.
Rate (US/DS)	Shows the upstream/downstream data rate for the port in Kbps.
Config. Profile	Shows current configuration profile used for the port.
Alarm Profile	Shows current alarm profile used for the port.
Alarm	Shows the alarm status of the port. Normal: no XDSL alarm Alarm: there is XDSL-related alarm (alarm ID between 601 and 622)

DSL Inventory

DSL Status

DSL Inventory

Auto Refresh Interval: 30 seconds

Near End:

Serial Number	Vendor ID	Version Number
NA	NA	NA

Far End:

Port	Serial Number	Vendor ID	Version Number
Port-1	NA	NA	NA
Port-2	NA	NA	NA
Port-3	NA	NA	NA
Port-4	NA	NA	NA
Port-5	NA	NA	NA
Port-6	NA	NA	NA
Port-7	NA	NA	NA
Port-8	NA	NA	NA

Near End	
Serial Number	Displays the serial number of the near-end device, if available.
Vendor ID	Displays the vendor-specified identification for the near-end device, if available.
Version Number	Displays the version number of the near-end device, if available.
Far End	
Port	Shows the number of physical line port.
Serial Number	Displays the serial number of the far-end device, if available.
Vendor ID	Displays the vendor-specified identification for the far-end device, if available.
Version Number	Displays the version number of the far-end device, if available.

4.4 Status / Interface / DSL Port Statistics

Use the Status/Interface/DSL Port Statistics screen to obtain the statistics of DSL ports for the near-end and far-end with a selection of "Summary of PM", "Interval PM", which is able to accommodate ninety-six (96) entries with an interval of fifteen (15) seconds, or "Day PM", which has a capacity of seven (7) entries with an interval of twenty-four (24) hours.

Status / Interface / DSL Port Statistics

Auto Refresh Interval: 30 seconds

Select PM: Summary of PMPhysical Site: Far EndRefreshClear PM

Related: ConfigStatusEthernetAlarms

Physical Port	Status	LOFS	Los	Loss	LOPRS	ES	SES	UAS	Init	CellPkts	RxHec	Fixed Octets (Fast)	Bad blks (Fast)	Fixed Octets (Slow)	Bad blks (Slow)
Port-1	Idle	0	0	0	NA	0	0	0	0	0	0	0	0	0	0
Port-2	Idle	0	0	0	NA	0	0	0	0	0	0	0	0	0	0
Port-3	Idle	0	0	0	NA	0	0	0	0	0	0	0	0	0	0
Port-4	Idle	0	0	0	NA	0	0	0	0	0	0	0	0	0	0
Port-5	Idle	0	0	0	NA	0	0	0	0	0	0	0	0	0	0
Port-6	Idle	0	0	0	NA	0	0	0	0	0	0	0	0	0	0
Port-7	Idle	0	0	0	NA	0	0	0	0	0	0	0	0	0	0
Port-8	Idle	0	0	0	NA	0	0	0	0	0	0	0	0	0	0
Port-9	Idle	0	0	0	NA	0	0	0	0	0	0	0	0	0	0
Port-10	Idle	0	0	0	NA	0	0	0	0	0	0	0	0	0	0
Port-11	Idle	0	0	0	NA	0	0	0	0	0	0	0	0	0	0
Port-12	Idle	0	0	0	NA	0	0	0	0	0	0	0	0	0	0
Port-13	Idle	0	0	0	NA	0	0	0	0	0	0	0	0	0	0
Port-14	Idle	0	0	0	NA	0	0	0	0	0	0	0	0	0	0
Port-15	Idle	0	0	0	NA	0	0	0	0	0	0	0	0	0	0

To display performance, specify the type of PM (summary/interval/day) and select near end or far end, and then click on Query. Click on **Clear PM** to flush displayed statistics. The displayed statistics are reset to zero.

The following information is displayed:

Field	Description
Physical Port	Shows the physical port number (1 ~ 24).
Validity	Shows the validity of the PM data (Valid/Invalid).
LOF	Loss Of Frame Count
LOS	Loss Of Signal Failure Count
LOSS	Loss Of Signal seconds
LPRS	Loss Of Power seconds (for VTUR only)
ESS	Errored Seconds
SESS	Severely Errored Seconds
UAS	Unavailable Seconds
Init	Modem Failed Initialization events (for VTUC only)
CellPkts	Total Cell Count (for Summary of PM only)
RxHec	ATM HEC violation count (for Summary of PM only)
Fixed Octets(Fast)	Count of corrected octets for fast channel.



# DATA-CONNECT

*The Right Connection!*

Status

Bad blks(Fast)	Count of uncorrectable blocks for fast channel.
Fixed Octes(Slow)	Count of corrected octets for slow channel.
Bad blks(Slow)	Count of uncorrectable blocks for slow channel.

4.5 Status / Interface / DSL Performance

Use the Status/Interface/DSL Performance screen to obtain the actual performance of each DSL port such as "Line", which indicates the line rate, "Channel", which indicates the payload rate, "Failures", which indicates the failed behavior, and "Tones", which indicates the bit loading of each tone.

Line:

LineChannelFailuresTones

Auto Refresh Interval: 30 seconds

Physical Port: Port-01Refresh

DSL Layer Performance : Near End

Physical Port	Port-1
AdminState	Off
OpState	Idle
SnrMgn	0.00[dB]
Attenuation	0.00[dB]
Output power	0.00[dBm]
Attainable rate	0[kbps]
Line Rate	0[kbps]
OH Rate	0[kbps]
Actual OpMode	NA
Current Framing Mode	NA
OpCapability	NA

DSL Layer Performance : Far End

Physical	Port-1
AdminState	Off
OpState	Idle
SnrMgn	0.00[dB]
Attenuation	0.00[dB]
Output power	0.00[dBm]
Attainable rate	0[kbps]
Line Rate	0[kbps]
OH Rate	0[kbps]
Actual OpMode	NA
Current Framing Mode	NA
OpCapability	NA

To display performance, specify a physical port and click on Query.

The following information is displayed:

Field	Description
Adminstate	Administrative state (On/Off)
OpState	Operational state (Data/Idle)
SnrMgn	Signal-to-Noise Ratio margin (dB)
Attenuation	Loop Attenuation (dB)
Output power	Actual output power (dBm)
Attainable rate	Attainable data rate (kbps)
Line Rate	Actual line rate (kbps)
OH Rate	Overhead data rate (kbps)
Actual OpMode	Actual XDSL operation mode
Current Framing Mode	Current framing mode
OpCapability	Shows the operation modes this physical site supports.

Channel:

Line

Channel

Failures

Tones

Auto Refresh Interval: 30 seconds

Physical Port: Port-01Latency: InterleaveRefresh

Near End

Physical Port	Port-1
AdminState	Off
Op State	Idle
Interleave Delay	0.00[ms]
CRC Block Length	0[bytes]
Tx Rate(Data Rate)	0[kbps]
Tx Protection	0.0[DMT Symbols]

Far End

Physical Port	Port-1
AdminState	Off
Op State	Idle
Interleave Delay	0.00[ms]
CRC Block Length	0[bytes]
Tx Rate(Data Rate)	0[kbps]
Tx Protection	0.0[DMT Symbols]

To display performance, specify a physical port and channel ID and then click on Query.

The following information is displayed:

Field	Description
Adminstate	Administrative state (On/Off)
OpState	Operational state (Data/Idle)
Interleave Delay	Actual Interleaving Delay (ms)
CRC Block Length	CRC block length (bytes)
Tx Rate (Data Rate)	Actual transmit data rate (kbps)
TxProtection	Actual transmit impulse noise protection (DMT symbols)

Failures:

LineChannelFailuresTones

Related: ConfigStatistic

Auto Refresh Interval: 30 seconds

Refresh

Physical Port	Admin State	Op State	NE FE	LOS	LOF	LOPWR	LOL	LSQ	IF	NP	ESE	NCDSW	LCDSW	NCDFT	LCDFT	BLOW_SLA_US	BLOW_SLA_DS
Port-1	Off	Idle	NE														
			FE														
Port-2	Off	Idle	NE														
			FE														
Port-3	Off	Idle	NE														
			FE														
Port-4	Off	Idle	NE														
			FE														
Port-5	Off	Idle	NE														
			FE														

Click on Query to view if there has been a failure due to the following conditions:

Field	Description
LOS	Loss Of Signal
LOF	Loss Of Framing
LOPWR	Loss Of Power Failure
LOL	Loss Of Link
LSQ	Loss Of Signal Quality
IF	Line Initialization Failure
NP	Far End No Peer xTUR Present
ESE	Excessive Severely Errored Seconds
NCDSW	No Cell Delineation on the slow channel
LCDSW	Loss of Cell Delineation on the slow channel
NCDFT	No Cell Delineation on the fast channel
LCDFT	Loss of Cell Delineation on the fast channel
BLOW_SLA_US	Available data rate is less than the configured Service Level Agreement threshold for upstream direction
BLOW_SLA_DS	Available data rate is less than the configured Service Level Agreement threshold for downstream direction

Tones:

LineChannelFailuresTones

Related: ConfigStatist

Physical Port:Port-13Near EndRefresh

Query Table

Row #	1	2	3	4	5	6	7	8
0 ~ 7	0	0	0	0	0	0	0	0
8 ~ 15	0	0	0	0	0	0	0	0
16 ~ 23	0	0	0	0	0	0	0	0
24 ~ 31	0	0	0	0	0	0	0	0
32 ~ 39	0	0	0	0	0	0	0	0
40 ~ 47	0	0	0	0	0	0	0	0
48 ~ 55	0	0	0	0	0	0	0	0
56 ~ 63	0	0	0	0	0	0	0	0
64 ~ 71	0	0	0	0	0	0	3	3
72 ~ 79	3	4	4	4	5	5	4	4
80 ~ 87	4	5	7	7	7	7	8	7
88 ~ 95	8	9	7	7	7	9	9	9
96 ~ 103	9	9	9	9	9	7	7	7
104 ~ 111	9	10	9	10	10	10	10	10
112 ~ 119	9	9	10	10	11	10	11	10
120 ~ 127	11	11	11	11	9	9	9	11
128 ~ 135	11	12	11	12	11	12	11	10
136 ~ 143	9	10	12	12	11	12	12	12
144 ~ 151	12	12	12	11	12	12	12	12
152 ~ 159	12	12	12	13	12	13	11	11
160 ~ 167	11	12	13	12	13	12	13	12

To display the VDSL Tone Bit-Loading data, specify a physical port and site and then click on Query.

The following information is displayed:

There are total 4096 (0 ~ 4095, representing the sub-carriers index) cells in the table. Each cell has a value 0 ~ 15 to indicate the bits allocation (how many bits are used) for a sub-carrier channel.

4.6 Status / Interface / Ethernet Statistics

Use the Status/Interface/Ethernet Statistics screen to display the status, error counts, and throughput of Ethernet ports. Select a tab (Interface or RMON) on top of the screen first.

Interface:

Interface

RMON

Auto Refresh Interval: 30 seconds

Previous Command Result: Normal

Physical Port: GigaBit-1

Query

Reset Port

Items	Value
Data Valid	Valid
User Port	1
MTU Size	1536bytes
Description	Giga Ethernet

Counter	Value	Output Counter	Value
Input Bytes	202883599	Output Bytes	0
Unicast PKTs	17408	Unicast PKTs	0
Not Unicast PKTs	0	Not Unicast PKTs	0
Discard PKTs	50702	Discard PKTs	0
Error PKTs	14	Error PKTs	0
Multicast PKTs	0	Multicast PKTs	0
Broadcast PKTs	0	Broadcast PKTs	0

To display interface Ethernet statistics, specify a bridge interface (for line bridge interface, select Line and then specify physical port and PVC number or Packet mode) and click on Query.

The following information is displayed:

Field	Description
Input Counter	
Input Bytes	Counter of bytes were received.
Input Unicast PKTs	Counter of unicast valid packets were received.
Input Not Unicast PKTs	Counter of broadcast or multicast valid packets were received.
Input Discard PKTs	- Counter of frames that were discarded by VLAN acceptable filtering, ingress filtering or classifier (DFC deny).



	<ul style="list-style-type: none"><li>- Counter of frames that were discarded because their source MAC address was unknown or denied.</li><li>- Counter of frames that were discarded because their destination MAC address was denied.</li></ul>
Input Error PKTs	<ul style="list-style-type: none"><li>- Counter of frames received that have a integral 64 to 1518 byte length and contain a Frame Check Sequence error,</li><li>- Counter of received frames from 64 to 1518 (non VLAN) or 1522 (VLAN) bytes in length that contain an invalid FCS and are not an integral number of bytes.</li><li>- Counter of frames received in which the 802.3 length field did not match the number of data bytes actually received (46 - 1500 bytes). The counter is not incremented if the length field is not a valid 802.3 length, such as an EtherType value.</li><li>- Counter of number of instances where a valid carrier was present and at least one invalid data symbol was detected.</li><li>- Counter of frames received that are less than 64 bytes in length, contain a valid FCS, and were otherwise well formed.</li><li>- Counter of frames received that exceeded 1518 (non VLAN) or 1522 (VLAN) bytes in length, contain a valid FCS, and were otherwise well formed.</li><li>- Counter of frames received which are less than 64 bytes in length and contain an invalid FCS, including integral and non-integral lengths,</li><li>- Counter of frames received which exceed 1518 (non VLAN) or 1522 (VLAN) bytes in length and contain an invalid FCS, including alignment errors.</li><li>- Counter of frames received that are streamed to the system but are later dropped due to lack of system resources.</li><li>- Counter of number of received Ethernet frames which were closed (in a middle of a frame) or discarded due to a receive buffer overrun event (no available buffers).</li><li>- Counter of the number of Ethernet frames which were closed due to the maximum frame size has been exceeded.</li><li>- Counter of the number of received Ethernet frames whose MAC-DA is not valid. (Unrecognized by address recognition routine in DPS).</li><li>- Counter of the number of received Ethernet Interworking frames which were dropped due to free buffer pool (FBP) Overrun.</li><li>- Counter of the number of received Ethernet Interworking frames which were dropped due to the Maximum Receive Unit frame size being exceeded.</li></ul>

# DATA-CONNECT

The Right Connection!

Status

Input Multicast PKTs	Counter of multicast valid packets were received.
Input Broadcast PKTs	Counter of broadcast valid packets were received.
<b>Output Counter</b>	
Output Bytes	Counter of bytes were forwarded.
Output Unicast PKTs	Counter of unicast frames that were forwarded.
Output Not Unicast PKTs	Counter of broadcast or multicast frames that were forwarded.
Output Discard PKTs	<ul style="list-style-type: none"><li>- Counter of dropped packets due to congestion, MTU violation or congestion in transmit queue.</li><li>- Counter of packets denied.</li><li>- Counter of group filtered packets.</li></ul>
Output Error PKTs	<ul style="list-style-type: none"><li>- Counter of frames that were deferred upon first transmission attempt. Does not include frames involved in collisions.</li><li>- Counter of number of frames aborted that were deferred for an excessive period of time (3036 byte times).</li><li>- Counter of frames transmitted which experienced exactly one collision during transmission.</li><li>- Counter of frames transmitted which experienced 2-15 collisions (including any late collisions) during transmission as defined using the RETRY[3-0] field of the TX function control register.</li><li>- Counter of frames transmitted that experienced a late collision during a transmission attempt. Late collisions are defined using the LCOL[50] field of the TX Function control register.</li><li>- Counter of frames that experienced 16 collisions during transmission and were aborted.</li><li>- Counter of number of frames transmitted that had no collision.</li><li>- Counter of number of times a valid PAUSE MAC Control frame was transmitted and honored.</li><li>- Counter of number of times the input PFH is asserted.</li><li>- Counter of oversized transmitted frames with an incorrect FCS value.</li><li>- Counter of valid sized packets transmitted with an incorrect FCS value.</li><li>- Counter of valid size frames transmitted with a Type Field signifying a Control frame.</li><li>- Counter of oversized transmitted frames with a correct FCS value.</li><li>- Counter of transmitted frames less then 64 bytes, with a correct FCS value.</li><li>- Counter of transmitted frames less then 64 bytes, with an incorrect FCS value.</li></ul>

# DATA-CONNECT

*The Right Connection!*

Status

	- Counter of number of times Ethernet transmitter underun occurred.
Output Multicast PKTs	Counter of multicast frames that were forwarded.
Output Broadcast PKTs	Counter of broadcast frames that were forwarded.

RMON:

Interface

RMON

Auto Refresh Interval: 30 seconds

Previous Command Result: Normal

Select Type: [Select]

RMON Table

(1) RMON ETH Statistics

(2) RMON History Control

(3) RMON ETH History

(4) RMON Alarm

(5) RMON Event

(6) RMON LOG

This page allows you to configure and query the RMON Statistics. The 5224AV-2GBE/2SFP supports performance statistics defined in RMON MIB groups 1 (Ethernet statistics), 2 (history control), 3 (alarm), and 9 (event) per RFC 2819 for all network uplink ports.

Click on *Select type* drop-down list and select a type of RMON table to be displayed.

(1) ETH Statistics

Auto Refresh Interval: 30 seconds

Previous Command Result: Success

Select Type: ETH Statistics

Index	Data Source	Owner
2	GBE1	RMON2

Create

Modify

Delete

Query

Index	1
Data Source	GBE1
Owner	RMON1
DropEvents	00000000
Octets	0c17c20f
Pkts	00020a15
BroadcastPkts	00000000
MulticastPkts	00000000
CRCAAlignErrors	00000007
UndersizePkts	00000000
OversizePkts	00000000
Fragments	00000000
Jabbers	00000000
Collisions	00000000
Pkts64Octets	00000000
Pkts65to127Octets	00000000
Pkts128to255Octets	00000000
Pkts256to511Octets	00000000
Pkts512to1023Octets	00000002
Pkts1024to1518Octets	00020a13

This option is for displaying the Ethernet interface RMON data. Click on the Data Source drop-down list and select GBE1 or GBE2. Type in an owner name and then click on Create button to create a new ETH statistics entry. An owner is the entity that configured this entry and is therefore using the resources assigned to it.

The following parameters are monitored in this table:

Variable	Description
DropEvents	Monitoring Rx dropped packets
Octets	Monitoring Rx bytes packets
Pkts	Monitoring Rx packets

BroadcastPkts	Monitoring Rx broadcast packets
MulticastPkts	Monitoring Rx multicast packets
CRCAAlignErrors	Monitoring Rx error alignment packets
UndersizePkts	Monitoring Rx undersize packets
OversizePkts	Monitoring Rx oversize packets
Fragments	Monitoring Rx fragments packets
Jabbers	Monitoring Rx jabber packets
Collisions	Monitoring Tx single collision packets
Pkts64Octets	Monitoring Tx 64 octets
Pkts65to127Octets	Monitoring Tx 65 to 127 octets
Pkts128to255Octets	Monitoring Tx 128 to 255 octets
Pkts256to511Octets	Monitoring Tx 256 to 511 octets
Pkts512to1023Octets	Monitoring Tx 512 to 1023 octets
Pkts1024to1518Octets	Monitoring Tx 1024 to 1518 octets

To modify an entry in this table, click in the selection box next to the entry index you want to modify, type in new value, and then click on Modify. To delete an entry, select the entry and click on Delete.



(2) History Control

Auto Refresh Interval: 30 seconds

Previous Command Result: Success

Select Type: History Control

Index	Data Source	Owner	Requested	Interval
2	GBE1	RMON2	96	1800

Create

Modify

Delete

Query

Index

1

Data Source

GBE1

Owner

RMON1

Requested

96

Granted

96

Interval

1800

This table is for controlling the ETH History table (see next option). History Control 1 is for controlling ETH History table 1; History Control 2 is for controlling ETH History table 2; etc. Type in the Requested value and Interval (sec) and then click on Create button to create a History Control entry. Up to 10 History Control entries can be created.

Field	Description
Data Source	Data source identifies the source of the data for which historical data was collected and placed in a table on behalf of this HistoryControl entry. Here the source is GBE1 interface or GBE2 interface.
Owner	An owner is the entity that configured this entry and is therefore using the resources assigned to it.
Requested	Requested value is the requested number of intervals over which data is to be saved in the part of the media-specific table associated with this HistoryControl entry.
Interval	The interval in seconds over which the data is sampled for each bucket in the part of the media-specific table associated with this HistoryControl entry. The value range is 1 to 3600 (sec).

To modify an entry, click in the selection box next to the entry index you want to modify, type in new value, and then click on Modify. To delete an entry, select the entry and click on Delete.

(3) ETH History

Auto Refresh Interval: 30 seconds

Previous Command Result: Success

Select Type: ETH History

History Index: History1

Query

HistIndex	1	1	1	1	1	1	1
SampleIndex	31	32	33	37	38	39	30
IntervalStart	2345469	2345471	2345473	2345481	2345483	2345485	2345467
DropEvents	00000000	00000000	00000000	00000000	00000000	00000000	00000000
Octets	00168090	00168090	00168090	00168090	00168090	00168090	00168090
Pkts	000034e0	000034e0	000034e0	000034e0	000034e0	000034e0	000034e0
BroadcastPkts	00001a68	00001a68	00001a68	00001a68	00001a68	00001a68	00001a68
MulticastPkts	00001a78	00001a78	00001a78	00001a78	00001a78	00001a78	00001a78
CRCAAlignErrors	00000000	00000000	00000000	00000000	00000000	00000000	00000000
UndersizePkts	00000000	00000000	00000000	00000000	00000000	00000000	00000000
OversizePkts	00000000	00000000	00000000	00000000	00000000	00000000	00000000
Fragments	00000000	00000000	00000000	00000000	00000000	00000000	00000000
Jabbers	00000000	00000000	00000000	00000000	00000000	00000000	00000000
Collisions	00000000	00000000	00000000	00000000	00000000	00000000	00000000
TxBytes	00000000	00000000	00000000	00000000	00000000	00000000	00000000
TxPackets	00000000	00000000	00000000	00000000	00000000	00000000	00000000
TxMulticast	00000000	00000000	00000000	00000000	00000000	00000000	00000000
TxBroadcast	00000000	00000000	00000000	00000000	00000000	00000000	00000000
Utilization	00000000	00000000	00000000	00000000	00000000	00000000	00000000

This option is for displaying Ethernet interface RMON history data. Before a history table is available, you have to create a History Control entry in advance (see previous option). To query the History table, click on the History Index drop-down list and select a history table and then click on Query.

Field	Description
HistIndex	Shows the History Table index. The history identified by this index is the same history as identified by the same value of History Control index.
SampleIndex	Shows the Sample index that uniquely identifies the particular Sample among all samples associated with the same History Control entry.

IntervalStart	Shows the value of System Up Time* at the start of the interval over which this sample was measured. <small>*System Up Time is the time since the network management portion of the system was last re-initialized.</small>
---------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

The following parameters are monitored in this table:

Variable	Description
DropEvents	Monitoring Rx dropped packets
Octets	Monitoring Rx bytes packets
Pkts	Monitoring Rx packets
BroadcastPkts	Monitoring Rx broadcast packets
MulticastPkts	Monitoring Rx multicast packets
CRCAAlignErrors	Monitoring Rx error alignment packets
UndersizePkts	Monitoring Rx undersize packets
OversizePkts	Monitoring Rx oversize packets
Fragments	Monitoring Rx fragments packets
Jabbers	Monitoring Rx jabber packets
Collisions	Monitoring Tx single collision packets
TxBytes	Monitoring Tx bytes
TxPackets	Monitoring Tx packets
TxMulticast	Monitoring Tx multicast
TxBroadcast	Monitoring Tx broadcast
Utilization	Monitoring Tx Utilization

(4) Alarm

Select Type: 

Alarm

Index	3
Interval	1800
Owner	RMON3
OID	DropEvents <div></div> .1 <div></div>
SampleType	ABSOLUTE <div></div>
StartupAlarm	RISING <div></div>
Rising Threshold	0
Rising Event Index	1
Falling Threshold	0
Falling Event Index	1

CreateModifyDeleteQuery

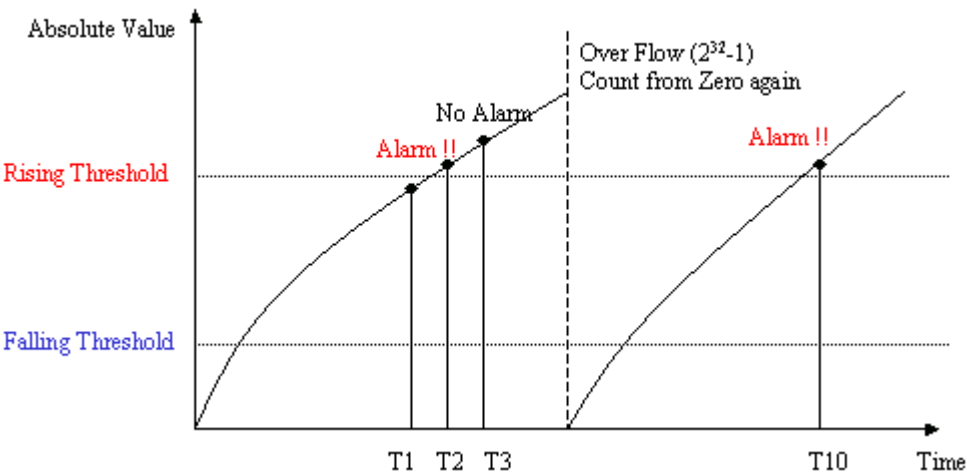
Index	1 <div></div>	2 <div></div>
Interval	1800	1800
Owner	RMON1	RMON2
OID Variable	DropEvents <div></div> 1 <div></div>	MulticastPkts <div></div> 1 <div></div>
SampleType	Sampling ABSOLUTE <div></div>	Sampling DELTA <div></div>
StartupAlarm	Startup By RISING <div></div>	Startup By FALLING <div></div>
Value	0	0
Rising Threshold	0	0
Falling Threshold	0	0
Rising Event Index	1	1
Falling Event Index	1	1

This option allows you to configure the RMON alarm setting. This table controls the conditions on which alarms occur. To create an entry, enter or select the following fields and then click on Create. To modify an entry, click in the selection box next to the entry index you want to modify, type in new value, and then click on Modify. To delete an entry, select the entry and click on Delete.

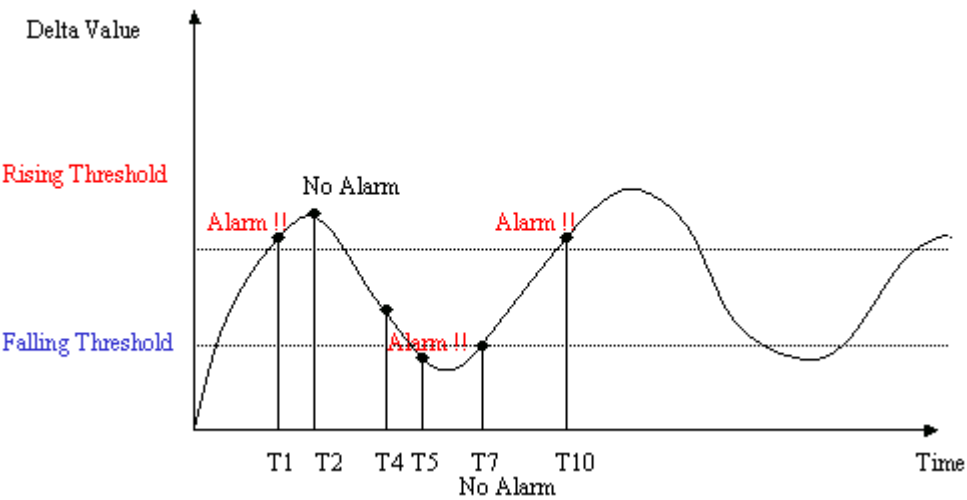
Field	Description
Interval	The interval in seconds over which the data is sampled and compared with the rising and falling thresholds. Value range: 0~2147483647 (0: disable).
Owner	RMON alarm owner (max 31 characters).

OID	Click on the drop-down list to select ETH statistics variable and index of ETH Statistics table entries.
Sample Type	RMON alarm sample type includes: ABSOLUTE: the value of the selected variable will be compared directly with the thresholds at the end of the sampling interval. DELTA: the value of the selected variable at the last sample will be subtracted from the current value, and the difference compared with the thresholds.
Startup Alarm	Set the alarm type that may be sent. Options are <b>Startup by Rising</b> , <b>Startup by Falling</b> , and <b>Start up by Both</b> . Rising or Both: If the first sample after this entry becomes valid is greater than or equal to the Rising Threshold, then a single rising alarm will be generated. Falling or Both: If the first sample after this entry becomes valid is less than or equal to the Falling Threshold, then a single falling alarm will be generated.
Value	This field shows the value of the monitored data.
Rise Threshold	RMON alarm rising threshold (0~4294967295).
Rise Event Index	This index is used when a rising threshold is crossed. You must refer to the index of RMON Event table. If there is no corresponding entry in the Event table, then no association exists.
Fall Threshold	RMON alarm falling threshold (0~4294967295).
Fall Event Index	This index is used when a falling threshold is crossed. You must refer to the index of RMON Event table. If there is no corresponding entry in the Event table, then no association exists.

Following figure shows an example of RMON alarm for ABSOLUTE sample type. As shown in the figure, the counting value keeps increasing. But when the value overflows, the system will count from zero again. The sample in T2 is the first one crossing the Rising Threshold, so an alarm occurs. While no alarms will be generated afterwards unless the counting value overflows and count from zero again (the sample in T10 causes an alarm again).



Another figure shows the example of RMON alarm for DELTA sample type. As shown in the following figure, the delta value varies high and low. The sample in T1 is the first one crossing the Rising Threshold, so an alarm occurs. While no alarms will be generated afterwards until T5 sample which is crossing the Falling Threshold (note that the value of the previous sample, T4 sample, is greater than the Falling Threshold and the value of T5 sample). Alarm is not generated for T7 sample since an alarm is already generated for T5 sample and the curve is not in a downward trend around T7. A Rising Threshold crossing alarm is generated again for T10 sample, because a Falling Threshold crossing alarm (T5) has occurred after the previous Rising Threshold crossing alarm (T1).





(5) Event

Interface

RMON

Auto Refresh Interval: 30 seconds

Previous Command Result: Normal

Select Type: Event

Index

3

Description

Description3

Community

Community3

Owner

RMON3

Event Type

NONE

Create

Modify

Delete

Query

Index

1

Description

Description1

EventType

NONE

Community

Community1

LastTimeSent

0

Owner

RMON1

Index

2

Description

Description2

EventType

NONE

Community

Community2

LastTimeSent

0

Owner

RMON2

This option allows you to configure the RMON event setting. To create an entry, enter or select the following fields and then click on Create.

To modify an entry, click in the selection box next to the entry index you want to modify, type in new value, and then click on Modify. To delete an entry, select the entry and click on Delete.

Field	Description
Description	Type in comment describing the event.
Event Type	Click on the drop-down list and select event type. Options are NONE, LOG (an entry is made in the log table for each event), SNMPTRAP (an SNMP trap is sent to one or more management stations), LOGANDTRAP (log and send trap).
Community	If an SNMP trap is to be sent, it will be sent to the SNMP community specified in this column.
LastTimeSent	(read-only) Shows the value of System Up Time at the time this event entry last generated an event.
Owner	Type in the RMON event owner.

(6) LOG

Previous Command Result: Normal

Select Type: LOG

Query

Index	EventIndex	Time Tick	Description
252	3	1220592	Description3
253	3	1220603	Description3
254	3	1220603	Description3
255	3	1220614	Description3
256	3	1220614	Description3
257	3	1220625	Description3
258	3	1220625	Description3

This option allows you to query the RMON LOG. Click on Query button to display latest log. Only the event indices with LOG or LOGANDTRAP event type (see previous option) will appear in the log.

4.7 Status / Interface / LLDP Statistics

Use the Status/Interface/LLDP Statistics screen to obtain LLDP (Link Layer Discovery Protocol) statistics for ports.

Status / Interface / LLDP Statistics

Auto Refresh Interval: 30 seconds

Previous Command Result: Normal

Select Port: GigaBit-1

Query

Clear Stats

LLDP neighborhood counter	0
Total numbers of LLDPDU frames are sent	0
The number of age-outs that occurred	0
The number of LLDP frames discarded	0
The number of invalid LLDP frames received	0
The number of valid LLDP frames received	0
The number of LLDP TLVs discarded	0
The number of LLDP TLVs received but not recognized	0

To display LLDP statistics, specify a port and click on Query. To flush displayed statistics, click on Clear Stats.

Field	Description
LLDP neighbour hood counter	The valid neighbor numbers are on the indicated port.
Total number of LLDPDU frames are sent	The total numbers of LLDPDU frames are sent from the port.
The number of age-out that occurred	The counter that represents the number of age-outs that occurred on a given port.
The number of LLDP frames discarded	The number of LLDP frames discarded for any reason by this LLDP agent on the indicated Port.
The number of invalid LLDP frames received	The number of invalid LLDP frames received by this LLDP agent on the indicated port, while this LLDP agent is enabled.
The number of valid LLDP frames received	The number of valid LLDP frames received by this LLDP agent on the indicated port, while this LLDP agent is enabled.
The number of LLDP TLVs discarded	The number of LLDP TLVs discarded for any reason by this LLDP agent on the indicated port.
The number of LLDP TLVs received but not recognized	The number of LLDP TLVs received on the given port that are not recognized by this LLDP agent on the indicated port.

4.8 Status / Interface / VLAN Counter

Use the Status/Interface/VLAN Counter screen to display VLAN statistics of each bridge port within a VLAN.

Status / Interface / VLAN Counter

Auto Refresh Interval: 30 seconds

Select page: page-1

VLAN : 1

Query

Physical Port	VLAN	ForwardPkts	DeniedPkts	FbpdDropPkts	Group Filtered Pkts	MtuDropPkts	TxQueueDropPkts
GigaBit-1	1	0	0	0	0	0	0
GigaBit-2	1	0	0	0	17408	0	0

To display VLAN counter, specify a VLAN and page to be displayed and click on Query.  
The following information is displayed:

Field	Description
ForwardPkts	Counter of packets forwarded.
DeniedPkts	Counter of packets denied.
FbpdropPkts	Counter of dropped packets due to congestion.
Group FilteredPkts	Counter of group filtered packets. (Isolation)
MtuDropPkts	Counter of dropped packets due to MTU violation.
TxQueueDropPkts	Counter of dropped packets due to congestion in transmit queue.

4.9 Status / Mgmt Radius Status

Use the Status/Mgmt Radius Status screen to display the status of the RADIUS server.

Status / Mgmt Radius Status

Auto Refresh Interval: 30 seconds

Server Index

Server IP Address

Stats

The following fields are displayed:

Field	Description
Server Index	Shows the number uniquely identifying each RADIUS Authentication server with which this client communicates.
Server IP Address	Shows the IP address of the RADIUS authentication server referred to in this table entry.
Client Round Trip Time (sec)	The time interval between the most recent Access-Reply/Access-Challenge and the Access-Request that matched it from this RADIUS authentication server.
Number of Access-Request/Challenge-Response packets sent to this server	Shows the number of RADIUS Access-Request packets sent to this server. This does not include retransmissions.
Number of Access-Request/Challenge-Response retransmitted sent to this server	Show the number of RADIUS Access-Request packets retransmitted to this RADIUS authentication server.
Number of Access-Accept packets received from the server	The number of RADIUS Access-Accept packets (valid or invalid) received from this server.
Number of Access-Reject packets received from the server	The number of RADIUS Access-Reject packets (valid or invalid) received from this server.
Number of Access-Challenge packets received from the server	The number of RADIUS Access-Challenge packets (valid or invalid) received from this server.
Number of Access Response packets containing invalid authenticators from the server	The number of RADIUS Access-Response packets containing invalid authenticators or Signature attributes received from this server.
Number of Authentication Timeouts	The number of authentication timeouts to this server. After a timeout the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a

# DATA-CONNECT

*The Right Connection!*

Status

	retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout.
Number of radius packets which were received from the server were dropped	The number of RADIUS packets of which were received from this server on the authentication port and dropped for some other reason.



4.10 Status / Multicast

Use the Status/Multicast screen to obtain IGMP multicast status and statistics for the system. Select a tab (Groups or Stats) on top of the screen first.

Groups:

Groups

Stats

Auto Refresh Interval: 30 seconds

Select page: page-1

Query

Index	Group IP	VID	Member Add Actions	Number Of Sources	IGMP Mode	Bridge Port List
1	224.001.001.005	1	46	0	INCLUDE	Port-1--PacketMode
2	224.001.001.004	1	46	0	INCLUDE	Port-1--PacketMode
3	224.001.001.003	1	47	0	INCLUDE	Port-1--PacketMode
4	224.001.001.002	1	47	0	INCLUDE	Port-1--PacketMode
5	224.001.001.001	1	47	0	INCLUDE	Port-1--PacketMode

The 5224AV-2GBE/2SFP supports up to 512 concurrent IGMP groups (multicast channels) per system.

To display IGMP multicast status, specify a page of entries to be displayed and click on Query.

The following information is displayed:

Field	Description
Index	Shows the index of the entry in the IGMP Group List.
Group IP	Shows the IGMP group IP address.
VID	Shows the IGMP group VLAN ID.
Member Add Actions	Shows how many times the IGMP group is joined by the group members.
Number Of Sources	Shows how many Source IPs are joining the IGMP group (for IGMP V3 only).
IGMP Mode	Shows current IGMP mode: INCLUDE or EXCLUDE (for IGMP V3 only, refer to RFC 3376 for filter-mode).
Bridge Port List	Shows the bridge ports that are joining the multicast group.

Stats:

Groups

Stats

Auto Refresh Interval: 30 seconds

Previous Command Result: Normal

Select: By Bridge Port

Bridge Port : GigaBit-1

Query

Clear

Clear All

Physical Port	Gigabit-1
Receive	
General Queries	0
Specific Queries	0
V12 Reports	0
V3 Reports	0
Leave	0
V12 Reports Fail	0
V3 Reports Fail	0
Leaves Fail	0
Total Invalid Messages	0
Transmit	
General Queries	0
Specific Queries	0
V12 Reports	0
V3 Reports	0
Leaves	0

To display IGMP statistics, select to display By Bridge Port or By VLAN, specify a bridge port or VLAN, and then click on Query.

Click on Clear to flush displayed statistics for the specified bridge port, or click on Clear All to flush displayed statistics for all ports at a time.

The following information is displayed:

#By Bridge Port

Field	Description
Receive	
General Queries	This statistic represents the frame count of IGMP General Query messages received from this bridge port.

Specific Queries	This statistic represents the frame count of IGMP Specific Query messages received from this bridge port.
V12 Reports	This statistic represents the frame count of IGMP V1/V2 Report messages received from this bridge port.
V3 Reports	This statistic represents the frame count of IGMP V3 Report messages received from this bridge port.
Leave	This statistic represents the frame count of IGMP Leave messages which are received and accepted (not discarded) by the system from this bridge port.
V12 Reports Fail	This statistic represents the frame count of IGMP V1/V2 Report messages which are received but not accepted (discarded) by the system from this bridge port.
V3 Reports Fail	This statistic represents the frame count of IGMP V3 Report messages which are received but not accepted (discarded) by the system from this bridge port.
Leaves Fail	This statistic represents the frame count of received IGMP Leave messages which are received but not accepted (discarded) by the system from this bridge port.
Total Invalid Messages	This statistic represents the frame count of received IGMP messages which are discarded by the IGMP filtering mechanisms of the system from this bridge port.
<b>Transmit</b>	
General Queries	This statistic represents the frame count of IGMP General Query messages transmitted from this bridge port.
Specific Queries	This statistic represents the frame count of IGMP Specific Query messages transmitted from this bridge port.
V12 Reports	This statistic represents the frame count of IGMP V1/V2 Report messages transmitted from this bridge port.
V3 Reports	This statistic represents the frame count of IGMP V3 Report messages transmitted from this bridge port.
Leaves	This statistic represents the frame count of IGMP Leave messages transmitted from this bridge port.

#By VLAN

Field	Description
<b>Network Side</b>	
General Queries	This statistic represents the frame count of IGMP General Query messages which are received from network side.
Specific Queries	This statistic represents the frame count of IGMP Specific Query messages which are received from network side.
V12 Reports	This statistic represents the frame count of IGMP V1/V2 Report messages which are transmitted to network

	side.
V3 Reports	This statistic represents the frame count of IGMP V3 Report messages which are transmitted to network side.
Leave Tx	This statistic represents the frame count of IGMP Leave messages which are transmitted to network side.
Total Invalid Messages Tx	This statistic represents the frame count of failed or invalid IGMP messages transmitted to network side.
Total Invalid Messages Rx	This statistic represents the frame count of IGMP messages received from network side, which are discarded by the IGMP filtering mechanisms of the system.
<b>User Side</b>	
General Queries	This statistic represents the frame count of IGMP General Query messages which are transmitted to multicast clients of user link bridge ports.
Specific Queries	This statistic represents the frame count of IGMP Specific Query messages which are transmitted to multicast clients of user link bridge ports.
V12 Reports	This statistic represents the frame count of IGMP V1/V2 Report messages which are received from multicast clients in user link bridge ports.
V3 Reports	This statistic represents the frame count of IGMP V3 Report messages which are received from multicast clients in user link bridge ports.
Leaves Rx	This statistic represents the frame count of IGMP Leave messages which are received from multicast clients of user link bridge ports.
Invalid V12 Reports Rx	This statistic represents the frame count of received IGMP V1/V2 Report messages which are received but not accepted (discarded) by the system.
Invalid V3 Reports Rx	This statistic represents the frame count of received IGMP V3 Report messages which are received but not accepted (discarded) by the system.
Invalid Leaves Rx	This statistic represents the frame count of IGMP Leave messages which are received but not accepted (discarded) by the system.
Total Invalid Messages Tx	This statistic represents the frame count of failed or invalid transmitted IGMP messages.
Total Invalid Messages Rx	This statistic represents the frame count of IGMP messages received from multicast clients of user link bridge ports, which are discarded by the IGMP filtering mechanisms of the system.

4.11 Status / Users

Use the Status/Users screen to show users currently logged on the system.

Status / Users

Auto Refresh Interval: 30 seconds

The user marked with "\*" means yourself.

Index	Interface Type	Account Name	User Access Level	Information
1	WEB	*admin	Super User	192.168.7.29 via http

The list displayed contains the following information:

Field	Description
Index	Shows the index of login user list.
Interface Type	Shows the mode of access. Possible values are: Console, Telnet, SSH, Cluster, Web.
Account Name	Shows the account name of the user
User Access Level	Shows the access level of the user
Information	Shows more information about the user including IP address of the management host, etc.

# DATA-CONNECT

*The Right Connection!*

Status

---



## 5 System

### 5.1 System / Alarms & Events

Use the System/Alarms & Events screen to check alarms and event on the hardware and DSL ports, and to configure alarm profile as well as temperature profile.

Select a tab (Alarms, Events, Alarm Config, or Temp Config) on top of the screen first.

#### Alarms:

Alarms

Events

Alarm Config

Event Config

Temp. Config

Auto Refresh Interval: 30 seconds

Alarm Select

Current Alarm

Row from 1To 10

Query

ACO

Row	ID	Description	Level	State	Sequential Number	Date Time
1	201	Gigabit Ethernet Loss of Signal:GBE 2	MN	Set	2	07/27/2011 02:54:18
2	201	Gigabit Ethernet Loss of Signal:GBE 1	MN	Set	1	07/27/2011 02:54:18

To query alarm, click on the *Alarm Select* drop-down list to specify Current Alarm or History Alarm and specify the range of rows (1~65536) to be displayed. Then click on Query.

Click on ACO to cut off alarms. Click on Clear History to clear history alarm table.

The list displayed contains the following information:

Field	Description
Row	Shows the row number (1~65536).
ID	Shows the alarm ID.
Description	Shows the description for the alarm.
Level	Shows the alarm level. Valid values are: MJ: major alarm. MN: minor alarm.
State	Shows the alarm state: Set or Clear.
Sequential Number	Shows the order number of the current alarm occurred.
Date Time	Shows alarm occurring date and time.

# DATA-CONNECT

The Right Connection!

## Events:

Alarms

Events

Alarm Config

Event Config

Temp. Config

Auto Refresh Interval: 30 seconds

Previous Command Result: Normal

Row from 1 To 10

Query

ACO

Clear Event

☐ Check All ☐ Uncheck All

Delete

	Row	Event Description	Sequential Number	Date Time	Rate(kbps) downstream/upstream
<input type="checkbox"/>	1	User Login Failure:System	5	07/28/2011 02:35:38	---
Event Binding : method: telnet, username: zhong, ip: 192.168.9.30					
<input type="checkbox"/>	2	User Logout:System	4	07/28/2011 02:35:27	---
Event Binding : method: telnet, username: admin, ip: 192.168.9.30					
<input type="checkbox"/>	3	User Login Success:System	3	07/28/2011 02:35:14	---
Event Binding : method: telnet, username: admin, ip: 192.168.9.30					
<input type="checkbox"/>	4	User Logout:System	2	07/28/2011 02:11:26	---
Event Binding : method: telnet, username: admin, ip: 192.168.9.30					
<input type="checkbox"/>	5	User Login Success:System	1	07/28/2011 02:10:59	---
Event Binding : method: telnet, username: admin, ip: 192.168.9.30					

To display events, specify the range of rows (1 ~ 256) to be displayed. Then click on Query.

Click on ACO to cut off alarms. Click on Clear Event to clear event log.

To delete an event, select the checkbox of that event and click on Delete. Select the checkbox Check All to select all events. Select the checkbox Uncheck All to deselect all selected events.

The list displayed contains the following information:

Field	Description
Row	This field shows the row number (1~256).
Event Description	This field shows the description for the event.
Sequential Number	The order number of the event occurred.
Date Time	Event occurring date and time.
Rate(kbps) downstream/upstream	This field reports the line rate when XDSL_PORT_LINKUP event occurs.

Alarm Config:

Alarms

Events

Alarm Config

Event Config

Temp. Config

Related: [Syslog Config](#)

Previous Command Result: Normal

☐ Check All ☐ Uncheck All

Level: 

MN

 Mask: 

Mask

 Notify type: 

Both

Modify to selected

 (Modify selected entry with Left Selections.)

Modify

 (Modify selected entry with Selections inside the table.)

ID	Type	Level	Mask	Notify Type	ID	Type	Level	Mask	Notify Type
<input type="checkbox"/> 101	Housekeep 1	<div>MN</div>	<div>UnMask</div>	<div>Both</div>	<input type="checkbox"/> 102	Housekeep 2	<div>MN</div>	<div>UnMask</div>	<div>Both</div>
<input type="checkbox"/> 103	Housekeep 3	<div>MN</div>	<div>Mask</div>	<div>Both</div>	<input type="checkbox"/> 104	Housekeep 4	<div>MN</div>	<div>UnMask</div>	<div>Both</div>

To modify the alarm profile, click in the selection box nearby the alarm ID, select the Level (Major/Minor), Mask/Unmask, Notify Type and then click on **Modify** button. If you want to set the same options for multiple alarm IDs, you can select alarm ID from table first and then click button on top of page, button name is **Modify to selected**.

You can click the Check All box to select all Alarm IDs at a time (Click Uncheck All box to cancel the selected items).

- Each Alarm Type is allowed to set its own notification method, the options as below:
- Trap Only      Send SNMP Trap to targeted host when alarm occurs. Need to configure SNMP target table also.
  - Syslog Only      Send Alarm message to Syslog Server when alarm occurs. Also need to configure Syslog.
  - Both      Send Alarm with SNMP Trap and also send to Syslog Server when alarm occurs.
  - None      No notification.

Event Config:

Alarms

Events

Alarm Config

Events Config

Temp. Config

Related: [Syslog Config](#)

Previous Command Result: Normal

☐ Check All ☐ Uncheck All

Level: 

MN

 Mask: 

Mask

 Notify: 

Both

Modify to selected

 (Modify selected entry with Left Selections.)

Modify

 (Modify selected entry with Selections inside the table.)

	ID	Type	Level	Mask	Notify type		ID	Type	Level	Mask	Notify type
<input type="checkbox"/>	1	System Restart	<div>MN</div>	<div>Mask</div>	<div>Both</div>	<input type="checkbox"/>	2	Download Begin	<div>MN</div>	<div>Mask</div>	<div>Both</div>
<input type="checkbox"/>	3	Download Success	<div>MN</div>	<div>Mask</div>	<div>Both</div>	<input type="checkbox"/>	4	Download Fail	<div>MN</div>	<div>UnMask</div>	<div>Both</div>

To modify the event profile, click the selection box nearby the event ID, select the Level (Major/Minor), Mask/Unmask, Notify Type and then click on **Modify** button. If you want to set the same options for multiple event IDs, you can select these event IDs from table first and then click the button on top of page, button name is **Modify to selected**.

You can click the Check All box to select all Event IDs at a time (Click Uncheck All box to cancel the selected items).

- Each Event Type is allowed to set its own notification method, the options as below:
- Trap Only      Send SNMP Trap to targeted host when event occurs. Need to configure SNMP target table also.
  - Syslog Only      Send Event message to Syslog Server when event occurs. Also need to configure Syslog.
  - Both      Send Event with SNMP Trap and also send to Syslog Server when event occurs.
  - None      No notification.

Temp Config:

Alarms

Events

Alarm Config

Event Config

Temp. Config

Auto Refresh Interval: 30 seconds

Previous Command Result: Normal

Current CPU °C	Current DSL °C	Up Shift TH °C	Up Shift Time(Sec)	Down Shift TH °C	Down Shift Time(Sec)	Fan ON TH °C
28	33	65	10	-40	10	-40

Modify

Query

Default

If current temperature exceeds/descends Up/Down Shift Threshold, Alarm Manager will declare that there is a high/lower temperature alarm after Up/Down ShiftTime seconds.  
(If exceeded the Alarm Manager also turn Fan module on after "Fan shift Time")

To modify the temperature profile, enter values for the parameters and then click on Modify to apply.

Click on Query to retrieve the latest data.

Click on Default to set the parameters to their default values.

The table displayed contains the following information:

Field	Description
Current CPU °C	Shows the current CPU temperature.
Current DSL °C	Shows the current DSL temperature.
Up Shift TH °C	The system will produce notification (alarm) when the monitored system temperature is higher than Up Shift TH (-55~85 °C) for over Up Shift Time (1~255 sec).
Up Shift Time (Sec)	Refer to the description for Up Shift TH.
Down Shift TH °C	The system will produce notification (alarm) when the monitored system temperature is lower than Down Shift TH (-55~85 °C) for over Down Shift Time (1~255 sec).
Down Shift Time (Sec)	Refer to the description for Down Shift TH.
Fan ON TH °C	FAN Enable temperature threshold (-40~15 °C). When the system temperature is higher than the threshold, the fan will be turned on automatically.

5.2 System / Boot Loader

Use the System/Boot Loader screen to upgrade boot loader in the system.

Downloading Boot Loader:

System / Boot Loader

Previous Command Result: Normal

Remote Server IP

:

21

Server User Name

Server Password

File Name

FTP Get and Write Flash

☐ Reboot After RemoteDownload

Warning:Upgrading boot loader may cause system crash

To download new boot loader from an FTP server to the system:

Enter or select the appropriate parameters in the Boot Loader Download box as shown in the following table.

Field	Description
Remote Server IP	Type in the IP address of the FTP server where the boot loader is stored.
Server User Name	Type in a user name accepted by the FTP server.
Server Password	Type in a password accepted by the FTP server.
File Name	Type in the name of the boot loader file (string length 1 ~ 64).
FTP Get and Write Flash	After you have entered the FTP server, user name & password, and boot loader file name, click on this button to start the boot loader update process.
Reboot After RemoteDownload	Select the checkbox if you want the system reboot automatically once the boot loader update is finished.



5.3 System / Firmware

Use the System/Firmware screen to upgrade firmware or switch versions of firmware in the system.

Upgrading Firmware:

To download new firmware from an FTP server to the system:

- 1. Enter or select the following parameters:

FTP Information	
Remote Server IP	Type in the IP address of the FTP server where the firmware is stored.
Server User Name	Type in a user name accepted by the FTP server.
Server Password	Type in a password accepted by the FTP server.
File Name	Type in the name of the firmware file (string length 1 ~ 64).
Reboot After Remote Download	Select the checkbox if you want the system reboot automatically once the firmware update is finished.

System / Firmware

Previous Command Result: Normal

FTP Information

Remote Server IP

Server User Name

Server Password

File Name

FTP Write Flash

:

21

FTP Get and Write Flash

☐ Reboot After RemoteDownload

Partition Information

Partition Location	Current Boot	Next Boot	Description
Partition:0	YES	YES	v1.01
Partition:1	---	---	v1.01

Change Partition

Partition 0

Submit

Note:Upgrading firmware may disconnect this page.  
Please refresh the page if it is disconnected.  
Warning:Upgrading firmware may take a few minutes.  
Please don't turn off or reset the BOX

- 2. Click on FTP Get and Write Flash. A confirmation dialog appears. Click on Yes to

continue. The firmware download starts and the following message is displayed on screen:

Remote download starts.....

and in a short time, the **Previous Command Result** shows "Getting firmware image file...(in progress)!".

After FTP get firmware file successfully, the system start to write firmware to flash (to the alternate partition, not current boot partition). The **Previous Command Result** shows

Writing flash image...(in progress)!

**WARNING:** The Flash Write process may take a few minutes. **Do not turn off or reset the system during the process.**

Once the Flash Write process completes successfully, the system will restart automatically (if you selected the **Reboot After Remote Download** checkbox). Wait for the system to restart.

After the system restart, login the Web GUI again. Go to the *System/Firmware* screen and verify that the firmware update was successful. Now the alternate partition before the firmware update becomes Current Boot partition. Check whether the displayed firmware version of Current Boot partition is correct.

Previous Command Result: Normal

FTP Information

Remote Server IP

Server User Name

Server Password

File Name

FTP Write Flash

FTP Get and Write Flash

☐ Reboot After RemoteDownload

Partition Information

Partition Location	Current Boot	Next Boot	Description
Partition:0	YES	YES	v1.01
Partition:1	---	---	v1.01

Change Partition

Partition 0

Submit

Note:Upgrading firmware may disconnect this page.  
Please refresh the page if it is disconnected.  
Warning:Upgrading firmware may take a few minutes.  
Please don't turn off or reset the BOX

## Switching Firmware:

To switch between the firmware currently running and alternate firmware stored in the system:

1. Verify that the firmware in Partition 0 and Partition 1 displayed in the Partition Information are different versions.
2. Click on Change Partition drop-down list and select the other partition (not Current Boot) and then click on Submit to apply. The system is reset and:
  - Current Boot partition becomes the alternate partition
  - The alternate partition becomes Current Boot partition

**WARNING:** It may take up to a minute or more for the system to finish switching the firmware and reset. **Do not reset the system or turn off the power while the system is switching firmware.**

5.4 System / Options

Use the System/Options screen to define characteristics of the operational interface.

System / Options

Previous Command Result: Normal

Modify

Idle Timeout

0seconds

Max session count

4

To set system options:

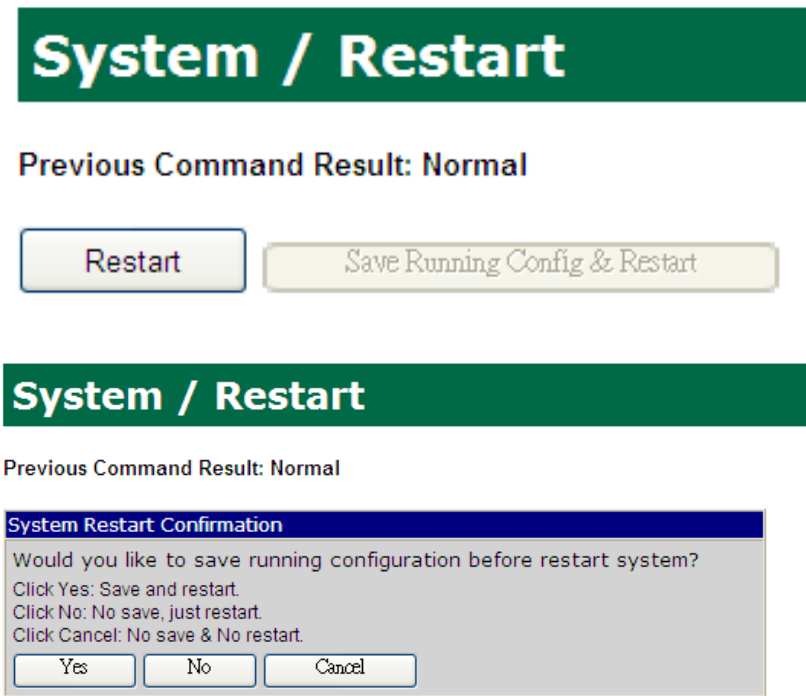
- 1. Specify appropriate values for parameters as shown in the following table.
- 2. Click on Modify.

Field	Description
Idle Timeout	Specify the timeout seconds for the operational interface (CLI or Web GUI session). The session will be closed once the idle time exceeds this timeout value. Value range is 60 ~ 65535. 0 means disable timeout setting.
Max session count	Specify the maximum allowed sessions for the operational interface (1 ~ 10).

## 5.5 System / Restart

### Restart

Use the System/Restart screen to restart the system.



This is a software reset that does not power down the system.

Click on Restart to restart the system without saving current running configuration. Or click on Save Running Config & Restart to save current running configuration and then restart the system.

### Save Running Config

This button will redirect to "System/ Restore >> (P) Save running config to flash replacing the specified backup".

5.6 System / Save & Restore

Use the System/Save & Restore screen to:

- Replace the running configuration with factory default configuration or another restoration configuration in flash memory
- Save the running configuration in flash memory
- Save (export) the running configuration to an external file using FTP
- Restore (import) the configuration from an external file using FTP
- Save (export) the alarm (history) log to an external file using FTP
- Save (export) the event log to an external file using FTP

System / Save & Restore

?

Database Control Action: [Select] 

Submit

FTP Server IP	
FTP Account	
FTP Password	
Filename	
Inband DB	
General DB	
Boot inband DB	16 01/04/2010 01:01:40
Boot general DB	16 01/04/2010 01:01:14
Set active inband DB	16 01/04/2010 01:01:40
Set active general DB	16 01/04/2010 01:01:14
Current Database Status	MEMORY WRITE SUCCESS

The running configuration is the set of configuration options currently in use. The active restoration configuration is the set of configurations loaded when the system is reset or first powered up.

On top of the screen, click on Database Control Action drop-down list and select an action you want to perform.



**(A) Save runtime config. and set to new active DB:**

This option allows you to save inband configuration and runtime configuration as the active restoration database for next power-on restoration. You can specify the configuration database name for saving or not. And you can specify the same or different name for inband DB and general DB.

After you click on Submit, the system starts to write runtime configuration to flash. The Current Database Status shows "Memory write in progress". While configuration is saved successfully, Current Database Status will show "Memory write success", and you will see the filename you save (if you have specified) appear in the *Set active inband DB/Set active general DB*.

**(B) Choose another DB/**

**(C) Choose another DB and restart**

These two options allow you to restore inband configuration and control plane configuration (other general configuration) by setting another restoration database active. Click on Set active inband DB and Set active general DB drop-down list to select the database you want to restore. There are up to 16 inband and general databases respectively for you to select. Click on Submit button. For action (C), a confirming dialog box will appear on screen; click Yes to continue. Current Database Status will show "Memory write in progress". For action (C), the system will restart once the memory write has finished.

**(D) Clear active DB including inband/**

**(E) Clear active DB including inband and restart**

These two options allow you to clear inband configuration and control plane configuration (general configuration) in the active restoration database (Warn: runtime configuration is also cleared and inband configuration is lost). Click on Submit button. For action (E), confirming dialog box will appear on screen; click Yes to continue. For action (E), the system will restart and restore to factory default once the database has been cleared.

**(F) Clear active DB excluding inband/**

**(G) Clear active DB excluding inband and restart**

These two options allow you to clear control plane configuration (general configuration) in the active restoration database (Warn: runtime configuration is also changed.). Click on Submit button. For action (G), a confirming dialog box will appear on screen; click Yes to continue. For action (G), the system will restart and restore to factory default once the database has been cleared.

**(H) Export CLI Command**

This option allows you to export runtime configuration in CLI command format to ftp server. Type in the FTP server's IP address, FTP user name & password and specify the CLI command file name, then click on Submit button.

Click on Database on the menu tree to refresh Current Database Status. While the CLI command file is exported successfully, the Current Database Status will show

"FTP Put Success" (actually there will be two files config11 and config12 saved).

## **(I) Export binary DB**

This option allows you to export runtime configuration in binary format to ftp server. Type in the FTP server's IP address, FTP user name & password and specify the binary DB file name, then click on Submit button.

Click on Database on the menu tree to refresh Current Database Status. While the binary file is exported successfully, the Current Database Status will show "FTP Put Success" (actually there will be two files config21 and config22 saved).

## **(J) Import CLI Command/**

## **(K) Import CLI Command and restart**

These two options allow you to import database in CLI command format from ftp server and set it to the active restoration database (Warning: system will restart for action (K)). Type in FTP server IP address, FTP user name & password, CLI command file name, and then click on Submit button. For action (K), you must wait several minutes for the system to restart after the DB has been imported successfully.

## **(L) Import binary DB/**

## **(M) Import binary DB and restart**

These two options allow you to import database in binary format from ftp server and set it to the active restoration database (Warning: system will restart for action (M)). Type in FTP server IP address, FTP user name & password, binary DB file name, and then click on Submit button. For action (M), you must wait several minutes for the system to restart after the DB has been imported successfully.

## **(N) Export Alarm (History) Log**

This option allows you to export alarm history log to ftp server. Type in the FTP server's IP address, FTP user name & password, specify the file name for alarm log, and then click on Submit button.

## **(O) Export Event Log**

This option allows you to export event log to ftp server. Type in the FTP server's IP address, FTP user name & password, specify the file name for event log, and then click on Submit button.

## **(P) Save running config to flash replacing the specified backup**

This option allows you to save running configuration in a specified DB backup index. This option supports both inband and general configuration respectively and independently. If an existing backup owns the specified DB backup index, the existing backup will be replaced with the new backup after this action command is submitted.

5.7 System / System Information

Use the System/System Information screen to view information about the system, and to specify a system name, location, and contact.

Select a tab (System ID, Hardware, or Software) on top of the screen first.

System ID:

System IDHardwareSoftware

Previous Command Result: Normal

Apply System Info Changes

System

System Name	localhost
System Location	Location
System Contact	Contact
System Description	VDSL2 IP-DSLAM-DC VDSL2 24-port

To set the system name and location:

- 1. Enter the name and location as shown in the System table below.

Field	Description
System Name	Enter 1 to 255 characters (ASCII CODE: 0x01 - 0x7F).
System Location	Enter 0 to 255 characters (ASCII CODE: 0x01 - 0x7F).
System Contact	Enter 0 to 255 characters (ASCII CODE: 0x01 - 0x7F).
System Description	Description of the system (this field is for display only)

- 2. Click on Apply System Info Changes.

Hardware:

System ID	Hardware	Software
System Information		
Power Type	[DC]	
Port Count	[24]	
Temperature Hardened	[Industrial]	
VLR Support	[Supported]	
Filter Type	[POTS]	
VDSL Band	[6 Bands(Maximum)]	
Hardware Version	[C]	
Model Info	[]	
Part Number	[]	
System Revision	[]	
Serial Number	[]	

This page displays various information related to the system’s hardware.

Software:

System ID

Hardware

Software

System Information

Software Version	[v1.05]
CPLD Version	[B3]
Boot Loader Version	[1.2.16]
Firmware Version	[3.42-2.3.0r9]

Module version

FWAPI Module Version	[1.0.5.2]
SNMP Module Version	[6.9_a]
SNTP Module Version	[1.0]
OAMP Module Version	[4.1.0.149]
VDSLMGR Module Version	[3.42]
VDSLMGR_EMU Module Version	[2.2.0.19]
WEB Module Version	[4.1-L]
WDDI Module Version	[2.4.3.11]
WLS Module Version	[3.2.4.4]

This page displays information about the system’s respective software module version.

5.8 System / User Administration

Use the System/User Administration screen to display, create, modify, and delete user definitions.

System / User Administration

Previous Command Result: Success

Select page: Page 1 of 4(No. 1 to 8)

Create

Delete

Modify

	No.	User Name	Access Level	Comment
<input type="radio"/>	1	admin	Super User	
<input type="radio"/>	2	Sang	Guest	[Comments]

Users already configured are displayed in the user table:

Field	Description
User Name	Shows the user name (up to 31 characters).
Access Level	Show the access level of the user: <b>SUPER USER</b> - The user has access to all functions <b>ENGINEER</b> - The user has access to all functions except user account management <b>GUEST</b> - The user has access to basic display functions
Comment	Description of the user account (up to 31 characters).

Creating a User:

Click on Create to create a user definition. The following box is displayed:

Access Level: GUEST

User Name	sang
Password	....
Confirm Password	....
Comment	[Comments]

Apply

Back

1. Enter the fields in the Create User box as shown in the table below.

Field	Description
User Name	Enter a user name of 1–31 characters.
Password	Enter a login password of 1–31 characters.
Confirm Password	Enter the login password of previous field again.



Comment	Enter description of the user account (0-31 characters).
---------	----------------------------------------------------------

2. Click on Apply. The new user appears in the configured users table.

Modifying a User:

To modify an existing user definition, click on the button next to a user name in the configured users table and then click on Modify. The Modify User screen appears. Make modification from that screen.

Access Level: Guest

User Name	Sang
Old Password	....
New Password	.....
Retry Password	.....
Comment	[Comments]

Apply

Back

1. Verify that the user name to be modified is displayed in the User Name field.

2. To change the login password, type the old password in the Old Password field.  
Type a new password in the New Password field and type the new password again in the Retry Password field.

3. Click on Apply.

Deleting a User:

To delete an existing user definition, click on the button next to a user name in the configured users table and then click on Delete. A confirmation dialogue appears. Click on Yes. Note that the default **admin** user cannot be deleted.

## 6 Configuration

### 6.1 Configuration / Auth (802.1x - RADIUS) / DSL Port Authentication / Server Configuration

Use the Configuration/Auth (802.1x –RADIUS)/~/Server Configuration screen to configure the system for supporting 802.1x.

Select a tab (System, Local, or RADIUS) on top of the screen first.

**System:**

SystemLocalRadius

Previous Command Result: Normal

Modify

802.1x System Control

Disable

802.1x Authentication Type

Both

To do 802.1x system configuration:

Field	Description
802.1x System Control	Select Disable/Enable 802.1x function of the system.
802.1x Authentication Type	Select authentication type: Both, RADIUS, or Local. When "Both" is selected, the system will try Radius Server Authentication first. If authentication fails, the system will then try Local Server Authentication.
Modify	Once you have specified the 802.1x system control and authentication type, click on this button to apply the modification.

Local:

SystemLocalRadius

Related: DSL Port Auth. Mgmt Auth.

Previous Command Result: Normal

Create New

Delete Selected

Delete All

	Profile Index	User Name	Password
<input type="checkbox"/>	1	user1	12345

- To **create** a profile for local server authentication:
1. Click on Create New. The Local Server Authentication–Create screen appears.
  2. Enter user name and password needed for authentication.
  3. Click on Create
- To **delete** a profile from local server authentication table:
1. Select the checkbox next to the profile index you want to delete.
  2. Click on Delete Selected.
  3. You can click on Delete All to delete all profiles at a time.

Field	Description
Profile Index	Shows profile index of local server authentication.
User Name	Shows the username used for local server authentication.
Password	Shows the password used for local server authentication.

RADIUS:

SystemLocalRadius

Related: DSL Port Auth. Mgmt Au

Previous Command Result: Success

Create New

Modify Selected

Delete Selected

Delete All

	Index	Radius Server IP	Auth Port	Accounting Port	Max Fail	Vlan ID	Secret
<input checked="" type="checkbox"/>	1	172.16.10.10	1812	1813	3	1	abcxx

- To **create** a RADIUS server for authentication:
1. Click on Create New. The Radius Server Authentication–Create screen appears.
  2. Enter values as required.
  3. Click on Create
- To **modify** an existing RADIUS server:
1. Select the checkbox next to the RADIUS server index you want to modify.
  2. Modify the settings as required.
  3. Click on Modify to apply.
- To **delete** a server from RADIUS server authentication table:
1. Select the checkbox next to the RADIUS server index you want to delete.
  2. Click on Delete Selected.
  3. You can click on Delete All to delete all servers at a time.

Field	Description
Index	Shows the RADIUS server index
Radius Server IP	Shows the IP address of the remote RADIUS server.
Auth Port	Shows the port number for RADIUS Authentication in the Layer-4 header. Default is 1812.
Accounting Port	Shows the port number for RADIUS Accounting in the Layer-4 header. Default is 1813.
Max Fail	Shows the maximum allowable times of continuously failed authentication attempts.
Vlan ID	Shows the VID of the VLAN where the RADIUS server belongs.
Secret	Shows the authentication key in text format.

## 6.2 Configuration / Auth (802.1x - RADIUS) / DSL Port Authentication / Port Configuration

Use the Configuration/Auth (802.1x –RADIUS)/~/Port Configuration screen to setup the 802.1x authentication mechanism for each DSL bridge port.

Select a tab (Port or Timer) on top of the screen first.

Port:

Port

Timer

Related: DSL Server Auth. Mgmt Au

Previous Command Result: Normal

Select page: page-1

☐ Check All

☐ Uncheck All

Modify

	Physical Port	Per Port control	Port control	ReAuth	Accounting	Max ReAuthReq	Max Req	Auth PAE State	Backend Auth State
<input type="checkbox"/>	Port-3--PVC-1	OFF	Auto	ON	Stop	2	2	NONE	NONE
<input type="checkbox"/>	Port-1--PacketMode	OFF	Auto	ON	Stop	2	2	NONE	NONE
<input type="checkbox"/>	Port-2--PacketMode	OFF	Auto	ON	Stop	2	2	NONE	NONE

To modify the authentication configuration for a port:

1. Click in the selection box next to the port you want to modify. You can click in the Check All selection box to select all ports at a time (To cancel the selection, click in UnCheck All selection box).
2. Enter or select the following fields:

Field	Description
Physical Port	Shows the bridge port interface/number.
Per Port-control	OFF/ON: disable/enable 802.1x authentication function for the bridge port. When 802.1x is disabled, the system allows bidirectional normal traffic in this port in spite of its authentication state. Default is OFF.
Port-control	<b>Force-unauthorized:</b> cause the port to stay in the unauthorized state, ignoring all attempts by the client to authenticate. <b>Force-authorized:</b> disable 802.1X authentication and cause the port to transition to the authorized state without any authentication exchange required. <b>Auto</b> (default): enable 802.1x authentication and cause the port to begin the authentication process from unauthorized state.
ReAuth	Click on this checkbox to cancel the selection of all profiles.

Accounting	OFF: notify RADIUS server to stop accounting for this port. ON: notify RADIUS server to start accounting for this port. Default is OFF.
Max ReAuthReq	Type in the number of times our system will send authentication requests to the authentication server (RADIUS) if no response from the server is received. Value range: 1 ~ 10. Default value is 2.
Max Req	Type in the number of times our system will send authentication requests to Supplicant if no response from the Supplicant is received. Value range: 1 ~ 10. Default value is 2.
Auth PAE State	This field displays the current value of the Authenticator (our system's role) PAE state machine. Possible states are: none, initialize, disconnected, connecting, authenticating, authenticated, aborting, held, forceAuth, forceUnauth
Backend Auth State	This field displays the current value of the Backend Authentication state machine (current authentication state to the backend authentication server). Possible states are: none, initialize, request, response, success, fail, timeout, idle

3. Click on Modify.



Timer:

Port

Timer

Related: DSL Server Auth. Mgmt Au

Previous Command Result: Normal

Select page: 

page-1

☒ Check All ☐ Uncheck All

Modify

	Physical Port	Reauth Period (Sec)	Server Timeout (Sec)	Supplicant Timeout (Sec)	Tx Period (Sec)	Quiet Period (Sec)	Interim Interval (Sec)
<input checked="" type="checkbox"/>	Port-3--PVC-1	<div>3600</div>	<div>30</div>	<div>30</div>	<div>30</div>	<div>60</div>	<div>300</div>
<input checked="" type="checkbox"/>	Port-1--PacketMode	<div>3600</div>	<div>30</div>	<div>30</div>	<div>30</div>	<div>60</div>	<div>300</div>
<input checked="" type="checkbox"/>	Port-2--PacketMode	<div>3600</div>	<div>30</div>	<div>30</div>	<div>30</div>	<div>60</div>	<div>300</div>

To modify the timer configuration for a port:

1. Click in the selection box next to the port you want to modify. You can click in the Check All selection box to select all ports at a time (To cancel the selection, click in UnCheck All selection box).
2. Enter the following fields:

Field	Description
Reauth Period (Sec)	Type in the number of seconds between re-authentication requests. Value range: 1 ~ 65535. Default is 3600 (sec).
Server Timeout (Sec)	Type in the number of seconds our system waits for a reply before resending the EAP response to the RADIUS server. Value range: 1 ~ 65535. Default is 30 (sec).
Supplicant Timeout (Sec)	Type in the number of seconds our system waits for a response when relaying a request from the authentication server to the supplicant before resending the request. Value range: 1 ~ 65535. Default is 30 (sec).
Tx-period (Sec)	Type in the number of seconds our system waits for a response to an EAP-request/identity packet from the supplicant before resending the request. Value range: 1 ~ 65535. Default is 30 (sec).
Quiet period (Sec)	Type in the number of seconds that our system remains in the quiet state following a failed authentication exchange with the supplicant. Value range: 0 ~ 65535 (sec). Default is 60 (sec).
Interim Interval (Sec)	Type in the interval between accounting information updates. Value range: 60 ~ 600 (sec). Default is 300 (sec).

3. Click on Modify.

### 6.3 Configuration / Auth (802.1x - RADIUS) / Mgmt Port Authentication

5224AV-2GBE/2SFP supports RADIUS Client for management authentication. With this feature, operators’ Management Accesses will be controlled centrally by remote RADIUS server. While DSLAM receives a management access request, DSLAM, which acts as a RADIUS Client, will encapsulate the request with RADIUS protocol and then send it to network for finding RADIUS Server’s authentication.

Note:

- 1. This feature is available on all in-band and out-band management interfaces.
- 2. Telnet, SSH (command line) and Web GUI are supported by this feature, but SNMP are not.
- 3. This feature is a system-wide basis. Once it is enabled, all interfaces will use this rule.

Use the Configuration/Auth (802.1x –RADIUS)/Mgmt Port Authentication screen to setup the authentication mechanism for Management Accesses.

Select a tab (System or Radius) on top of the screen first.

System:

SystemRadius

Previous Command Result: Normal

Modify

Management RADIUS Authentication

Local

Authentication Session Cache Aging Time (Sec)

30

To modify system configuration of management port authentication:

- 1. Enter or select the following fields:

Field	Description
Authentication Method for management login	Select an authentication method. <b>Local:</b> Disable management authentication through Radius server. <b>Both:</b> Enable management authentication through RADIUS server. 'Both' means RADIUS Authentication first priority. The precedence sequence is Server 1 → Server2 → Server3 → Server 4 →Local. First Server timeout then go to next (follow above sequence) and so on. If all the RADIUS Server response timeout, then the system will turn to run local authentication. Once Radius Server response access reject, it should reject

	the login request. Once Radius Server response access, the system should accept the login request and do not need to check other Radius server and Local authentication.
Authentication Session Cache Aging Time (sec)	<p>5224AV-2GBE/2SFP maintains a non-blocking authentication method, which stores an Access Request status in internal DB cache.</p> <p>The possible Access Request statuses are InProgress, Pass, Fail, NoResponse. When the status is InProgress, the cache does not count down aging. Once the status is updated as Pass/Fail/NoResponse, it will start to count down follow the configuration as cache aging. Before the aging time is expired, any new Access Request that has the same username/password will be directly referred to Access Request Status of this session cache.</p> <p>The range of session cache aging time is 10 ~ 600 (sec). Default value is 30 sec.</p>

2. Click on Modify.

RADIUS:

System

Radius

Related: [Uplink](#) [Mgmt Auth.](#) [DSL Server Au](#)

Previous Command Result: Success

Create

Server Index	Server IP Address	Radius Server Authentication UDP Port Number	Retry Count for Access Request Timeout	VLAN ID for Radius Authentication Communication	Access Request Timeout (Sec)	Encryption Secret
2	0.0.0.0	1812	3	1	10	

Delete

	Server Index	Server IP Address	Radius Server Authentication UDP Port Number	Retry Count for Access Request Timeout	VLAN ID for Radius Authentication Communication	Access Request Timeout (Sec)	Encryption Secret	Stats
<input type="checkbox"/>	1	10.10.10.10	1812	3	1	10	geaaxx12	<a href="#">Stats</a>

To create a RADIUS server for management port authentication:

1. Enter or select the following fields:

Field	Description
Server Index	This field shows the entry index. Value range: 1~4.
Server IP Address	Specify the RADIUS server IP address.
RADIUS Server Authentication UDP Port Number	Enter RADIUS server authentication UDP socket port number. Value range: 1 ~ 65535. Default value is 1812.
Retry Count for Access Request Timeout	Enter RADIUS retry count after Access Request does not response timeout. Value range: 1 ~ 10. Default value is 3.
VLAN ID for RADIUS authentication communication	Enter the VLAN ID for RADIUS authentication communication. This value indicates the VLAN of RADIUS server. Value range: 1 ~ 4094.
Access Request Timeout (sec)	Enter the time frame that DSLAM will wait every time it sends an Access Request to RADIUS server. If DSLAM does not receive the response of an Access Request after the configured time frame, this Access Request will be treated as no response. Value range: 1 ~ 30 (sec). Default value is 10.
Encryption Secret	Enter the secret key for encrypting the transmission of the User-Password in a request accomplished by a shared secret. Max size is 16 characters. The last space is for '\0'.

2. Click on Create.

To view an existing RADIUS server stats:

1. Click on **Stats** in the RADIUS server table. The Mgmt RADIUS Status screen appears.

Previous Command Result: Normal

stats clear

back

Server Index	1
Server IP Address	10.10.10.10
Client Round Trip Time (Sec)	0.00
Number of Access-Request/Challenge-Response packets sent to this server	0
Number of Access-Request/Challenge-Response retransmitted sent to this server	0
Number of Access-Accept packets received from the server	0
Number of Access-Reject packets received from the server	0
Number of Access-Challenge packets received from the server	0
Number of Access Response packets containing invalid authenticators from the server	0
Number of Authentication timeouts	0
Number of radius packets which were received from the server were dropped	0

Following information is displayed:

Field	Description
Server Index	A number uniquely identifying each Radius sever with which the client communicates. The range is from 1 to 4.
Server IP Address	The IP address of the RADIUS sever referred to in this table entry. (IP address)
Client Round Trip Time (Sec)	The time interval (10 ms as a unit, in hundredths of a second) between the most recent Access-Reply/Access-Challenge and the Access-Request that matched it from this Radius authentication server. (10ms as a unit) From Access-Request to Access-Challenge should update Round trip time. From Challenge-Response (new Access-Request) to Access-Reject/Access-Accept should update Round trip time.
Number of Access-Request/Challenge-Response packets sent to this server	The number of Radius Access-Request/Challenge-Response packet sent to this server. This does not include retransmissions.
Number of Access-Request/Challenge-Response retransmitted	The number of Radius Access-Request/Challenge-Response packets retransmitted to this Radius server.



sent to this server	
Number of Access-Accept packets received from the server	The number of Radius Access-Accept packets received from this server.
Number of Access-Reject packets received from the server	The number of Radius Access-Reject packets received from this server.
Number of Access-Challenge packets received from the server	The number of Radius Access-Challenge packets received from this server.
Number of Access Response packets containing invalid authenticators from the server	The number of Radius Access Response packets containing invalid authenticators received from this server.
Number of Authentication timeouts	The number of Authentication timeouts to this server. A retry to the same server is counted as a retransmit as well as a time out. A send to a different server is counted as a Request as well as a timeout. It means any of mgmtRadiusSrvTimeout timeout happens this count should increase 1.
Number of radius packets which were received from the server were dropped	The number of Radius packets which were received from this sever were dropped (Silent drop internally).

2. You can click on stats clear to clear statistic counters.

3. Click on Back to return to RADIUS server table.

To delete a RADIUS server for management port authentication:

1. Click in the selection box next to the server index you want to delete.

2. Click on Delete.

## 6.4 Configuration / Bridge / Interface / Profiles / Alarm Threshold Profiles

Use the Configuration/Bridge/~ / Alarm Threshold Profiles screen to create, modify, and delete sets of alarm thresholds that you can apply to line ports.

Previous Command Result: Normal

Related: Alarms

Create New

Modify Selected

Delete Selected

Delete All

	Profile Name	Init Failures	Internal Row Status	DS ESs second (s)	DS SESs second (s)	DS UASs second (s)	US ESs second (s)	US SESs second (s)	US UASs second (s)	DS Day ESs second (s)	DS Day SESs second (s)	DS Day UASs second (s)	US Day ESs second (s)	US Day SESs second (s)	US Day UASs second (s)
<input type="checkbox"/>	DEFVAL	Disable	Active	0	0	0	0	0	0	0	0	0	0	0	0
<input type="checkbox"/>	ADSL_A_DEFVAL	Disable	Active	0	0	0	0	0	0	0	0	0	0	0	0
<input type="checkbox"/>	ADSL_B_DEFVAL	Disable	Active	0	0	0	0	0	0	0	0	0	0	0	0

### Creating alarm threshold profiles:

To create an alarm threshold profile:

- Click on Create New. The Alarm Threshold Profile Create screen appears.
- Enter or select the following fields:

Field	Description
Profile Name	Specify a name for this alarm profile.
Internal Row Status	Set the profile to be Active or Not In Service. You cannot bind a line port to the alarm profile of which the row status is NotInService. Before a profile can be deleted or taken out of service, (by setting this status to NotInService) it must be first unreferenced from all associated lines.
Init Failures	Select the checkbox to enable initialization failure to generate InitFailureTrap messages as specified in RFC 2662.
Downstream (Near End) / Upstream (Far End) Interval Alarm Profile	
ESs	An SNMP trap is sent if the number of Errored Seconds events in a 15-minute interval meets or exceeds the selected value (0-900 seconds, where 0 disables the messages).
SESs	An SNMP trap is sent if the number of Severely Errored Seconds events in a 15-minute interval meets or exceeds the selected value (0-900 seconds, where 0 disables the messages).
UASs	An SNMP trap is sent if the number of Unavailable Seconds events in a 15-minute interval meets or exceeds the selected value (0-900 seconds, where 0 disables the messages).

Downstream (Near End) / Upstream (Far End) Day Alarm Profile	
ESs	An SNMP trap is sent if the number of Errored Seconds events in a 24-hour interval meets or exceeds the selected value (0-86400 seconds, where 0 disables the messages).
SESSs	An SNMP trap is sent if the number of Severely Errored Seconds events in a 24-hour interval meets or exceeds the selected value (0-86400 seconds, where 0 disables the messages).
UASs	An SNMP trap is sent if the number of Unavailable Seconds events in a 24-hour interval meets or exceeds the selected value (0-86400 seconds, where 0 disables the messages).

3. Click on Apply

Modifying an alarm threshold profile:

To modify an alarm threshold profile:

1. Click in the selection box next to the profile you want to modify.
2. Click on Modify Selected. The Alarm Threshold Profile Modify screen appears.
3. Modify the fields as required.
4. Click on Modify.

Deleting an alarm threshold profile:

To delete an alarm threshold profile:

1. Click in the selection box next to the profile you want to delete.
2. Click on Delete Selected.
3. You can click on Delete All to delete all profiles at a time.

## 6.5 Configuration / Bridge / Interface / Profiles / xDSL Configuration Profiles

Use the Configuration/Bridge/~xDSL Configuration Profiles screen to create, modify, and delete xDSL configuration profiles to be assigned to ports.

Configuration / Bridge / Interface / Profiles / xDSL Configuration Profiles

Previous Command Result: Success

Create New

Modify Selected

Delete Selected

Delete All

	Profile Name	Latency	DS Max Rate(kbps)	DS Min Rate(kbps)	US Max Rate(kbps)	US Min Rate(kbps)
<input type="checkbox"/>	DEFVAL	InterleavedOnly	200000	32	200000	32
<input type="checkbox"/>	ADSL_A_DEFVAL	InterleavedOnly	200000	32	200000	32
<input type="checkbox"/>	ADSL_B_DEFVAL	InterleavedOnly	200000	32	200000	32
<input checked="" type="checkbox"/>	profile_A	InterleavedOnly	150000	32	150000	32

Note that operators can create up to 24 profiles that can be modified and deleted. There are three system default profiles, which cannot be modified and deleted. They are:

- DEFVAL:** default VDSL profile
- ADSL\_DEFVAL\_A:** default ADSLx Annex A profile
- ADSL\_DEFVAL\_B:** default ADSLx Annex B profile

To create a xDSL configuration profile:

- Click on Create New. The xDSL Configuration Profiles Create screen appears.
- Specify a name for this line configuration profile. The allowed characters include: 0-9, A-Z, a-z, “\_” and “-”.
- Select a tab (Line Config, Advanced, PSD Shaping, UPBO, or DPBO) on top of the screen first.

Line Config:

Profile Name:

DEFVAL

Create

Line Config

Advanced

PSD Shaping

UPBO

DPBO

Internal RowStatus:

Active

Attribute	Value	Description
Rate Mode	AdaptAtStart	Manual, AdaptAtStart. Manual: rate is determined by "Maximum" data rate.
LineOpMode	<div><div><div><input type="checkbox"/> ADSL1_ANNEX_A</div><div><input type="checkbox"/> ADSL1_ANNEX_B</div></div><div><div><input type="checkbox"/> ADSL2_ANNEX_A</div><div><input type="checkbox"/> ADSL2_ANNEX_B</div></div><div><div><input type="checkbox"/> ADSL2_PLUS_ANNEX_A</div><div><input type="checkbox"/> ADSL2_PLUS_ANNEX_B</div></div><div><div><input type="checkbox"/> ADSL2_PLUS_ANNEX_M</div><div><input checked="" type="checkbox"/> ITU_G993_2_8A</div></div><div><div><input checked="" type="checkbox"/> ITU_G993_2_8B</div><div><input checked="" type="checkbox"/> ITU_G993_2_8C</div></div><div><div><input checked="" type="checkbox"/> ITU_G993_2_8D</div><div><input checked="" type="checkbox"/> ITU_G993_2_12A</div></div><div><div><input checked="" type="checkbox"/> ITU_G993_2_12B</div><div><input checked="" type="checkbox"/> ITU_G993_2_17A</div></div><div><div><input checked="" type="checkbox"/> ITU_G993_2_30A</div><div></div></div></div>	

Multiple selected BITS

Enter or select the following fields:

Field	Description
Internal Row Status	Click on the drop-down list and select the service status of the profile (Active/NotInService). You cannot bind a line port to the configuration profile of which the row status is Not In Service.
Rate Mode	Click on the drop-down list and select the Rate Adaptive Mode. Valid options are: Manual – Rate changed manually AdpatAtStart – Rate automatically selected at start up only and does not change after that
LineOpMode	Click on the checkboxes to select the allowed xDSL



# DATA-CONNECT

The Right Connection!

Configuration

	operation modes. Options are: ADSL1_ANNEX_A, ADSL1_ANNEX_B, ADSL2_ANNEX_A, ADSL2_ANNEX_B, ADSL2_PLUS_ANNEX_A, ADSL2_PLUS_ANNEX_B, ADSL2_PLUS_ANNEX_M, ITU_G993_2_8A, ITU_G993_2_8B, ITU_G993_2_8C, ITU_G993_2_8D, ITU_G993_2_12A, ITU_G993_2_12B, ITU_G993_2_17A, ITU_G993_2_30A. (Note: if the system supports maximum 5 VDSL bands not 6 bands, 30A will not be available. You can check in System -> System Inventory -> VDSL band for how many bands the system supports)
Line Type	Click on the drop-down list and select the Line Type (latency). Options are: NoChannel: No channels exist. FastOnly: Only fast channel exists. InterleavedOnly: Only interleaved (slow) channel exists.
DS1StartTone	Type in the DS1 Start tone (0~1023 in 4.3125 KHz Tone Spacing).
Max. Data Rate - Downstream	Type in the Maximum downstream data rate for fast channel.
Max. Data Rate - Upstream	Type in the Maximum upstream data rate for fast channel.
Min. Data Rate - Downstream	Type in Minimum downstream data rate for fast channel.
Min. Data Rate - Upstream	Type in Minimum upstream data rate for fast channel.
Slow Max. Data Rate - Downstream	Type in the Maximum downstream data rate for slow channel.
Slow Max. Data Rate - Upstream	Type in the Maximum upstream data rate for slow channel.
Slow Min. Data Rate - Downstream	Type in Minimum downstream data rate for slow channel.
Slow Min. Data Rate - Upstream	Type in Minimum upstream data rate for slow channel.
MaxSnrMgn – Downstream	Type in the downstream maximum SNR margin.
MaxSnrMgn - Upstream	Type in the upstream maximum SNR margin.
TargetSnrMgn – Downstream	Type in the downstream target SNR margin.
TargetSnrMgn - Upstream	Type in the upstream target SNR margin.
MinSnrMgn – Downstream	Type in the downstream minimum SNR margin.
MinSnrMgn – Upstream	Type in the upstream minimum SNR margin.
MaxInterDelay – Downstream	Type in the downstream maximum interleaver delay.



# DATA-CONNECT

*The Right Connection!*

Configuration

MaxInterDelay - Upstream	Type in the upstream maximum interleaver delay.
MinProtection - Downstream	Type in the downstream minimum protection against impulse noise.
MinProtection - Upstream	Type in the upstream minimum protection against impulse noise.
MaxPwr - Downstream	Type in the downstream maximum power.
MaxPwr - Upstream	Type in the upstream maximum power.
MaximumPSD - Downstream	Type in the downstream maximum PSD.
MaximumPSD - Upstream	Type in the upstream maximum PSD.
Overhead Data Rate - Downstream	Type in the downstream overhead data rate.
Overhead Data Rate - Upstream	Type in upstream overhead data rate.
Service Level Agreement - Downstream	Type in the downstream Service Level Agreement data rate threshold. Note that 0 means to disable threshold crossing alarm.
Service Level Agreement - Upstream	Type in the upstream Service Level Agreement data rate threshold. Note that 0 means to disable threshold crossing alarm.

Advanced:

Line Config

Advanced

PSD Shaping

UPBO

DPBO

Attribute	Value	Description
Band Plan	998_138_30000_4K_Tones_30A	Plan997, Plan998, ...
VDSL2 Frequency Plan.	VDSL2 Annex C TTC (Default)(Japan)	Select VDSL2 Frequency Plan. Notes: Only available in VDSL2
PSD Mask	ANSI_M2_EX	Select the PSD Mask
Tx Band Config.	DISABLE_2200K_BELOW	Select Tx Config.
Rx Band Config.	ALL_TONES_ON	Select Rx Band Config.
Opt. Band Config.	DISABLE	Select OptBand Config.
		To configure G.Hs

Enter or select the following fields:

Field	Description
Band Plan	<div>Click on the drop-down list and select the VDSL band plan to be used. Options are:</div> <div>998_138_8500 -- Plan 998-138KHz-8500KHz_Long_Reach</div> <div>998_138_12000 -- Plan 998-138KHz-12000KHz High Data Rate</div> <div>998_640_30000 -- Plan 998-640KHz-30000KHz 100/100</div> <div>997_138_8500 -- Plan 997-138KHz-8500KHz Flex_138_4400 -- Plan Flex-138KHz-4400KHz</div> <div>998_138_4400 -- Plan 998-138KHz-4400KHz 997_138_4400 -- Plan 997-138KHz-4400KHz</div> <div>998_138_4400_optBand -- Plan 998-138KHz-4400KHz-optBand</div> <div>997_138_4400_optBand -- Plan 997-138KHz-4400KHz-optBand</div> <div>998_138_12000_4K_Tones -- Plan 998-138KHz-12000KHz 4K Tones</div> <div>997_138_12000_4K_Tones -- Plan 997-138KHz-12000KHz 4K Tones</div> <div>998_138_17000_4K_Tones -- Plan 998-138KHz-17000KHz 4K Tones</div> <div>998_138_30000_4K_Tones_30A -- Plan 998-138KHz-30000KHz 4K Tones (30A) (Note: if the system supports maximum 5 VDSL bands not 6 bands, 30a will not be available. You can check in System -&gt; System Inventory -&gt; VDSL band for how many bands the system supports)</div>
VDSL2 Frequency Plan	Click on the drop-down list and select the frequency plan for VDSL2.
PSD Mask	Click on the drop-down list and select the PSD Mask.

# DATA-CONNECT

*The Right Connection!*

Configuration

	Options are: VENDER_DEFAULT_PSD, ANSI_M1_CAB, ANSI_M2_CAB, ETSI_M1_CAB, ETSI_M2_CAB, ANNEX_F, ANSI_M1_EX, ANSI_M2_EX, ETSI_M1_EX_P2, ETSI_M2_EX_P2, PSD_K, PSD_CHINA, ETSI_M1_EX_P1, ETSI_M2_EX_P1
Tx Band Config.	Click on the drop-down list and select the configuration for transmit band. Options are: ALL_TONES_ON, DISABLE_640K_BELOW, DISABLE_1100K_BELOW, DISABLE_2200K_BELOW.
Rx Band Config.	Click on the drop-down list and select the configuration for receive band. Options are: ALL_TONES_ON, DISABLE_640K_BELOW, DISABLE_1100K_BELOW, DISABLE_2200K_BELOW.
Opt Band Config.	Click on the drop-down list and select the configuration for optional band. Options are: DISABLE, ANNEX_A_26K_TO_138K, ANNEX_B_138K_TO_276K, ANNEX_B_26K_TO_276K.
G.HS Carrier Set	Click on the checkbox to select the carrier set for G.Handshake (ITU-T G.994.1) feature. For VDSL modem, select V43; for ADSL/2/2+ Annex A or Annex M modem, select A43; for ADSL/2/2+ Annex B, suggest selecting B43; for Ikanos VDSL1 100/100 Mbps, select I43. Note that A43 and B43 cannot be set at the same time.
ADSL2 Annex M US0 Mask	Click on the checkboxes to select the US0 mask of Annex M. Options are: eu36, eu40, eu44, eu48, eu52, eu56, eu60, eu64.
VDSL2 Annex A US0 Mask	Click on the checkboxes to select the US0 mask of Annex A. Options are: eu32, eu36, eu40, eu44, eu48, eu52, eu56, eu60, eu64, ds1, ds9.
VDSL2 Annex B US0 Mask	Click on the checkboxes to select the US0 mask of Annex B. Options are: US_A, US_M, US_B.
Standard RFI Notch	Click on the checkboxes to select the RFI transmit bands to be notched. Options are:

	RFI_1810_1825 -- 1.810 - 1.825 MHz: ANNEX F RFI_1810_2000 -- 1.810 - 2.000 MHz: ETSI, T1E1 RFI_19075_19125 -- 1.9075 - 1.9125 MHz: ANNEX F RFI_3500_3575 -- 3.500 - 3.575 MHz: ANNEX F RFI_3500_3800 -- 3.500 - 3.800 MHz: ETSI RFI_3500_4000 -- 3.500 - 4.000 MHz: T1E1 RFI_3747_3754 -- 3.747 - 3.754 MHz: ANNEX F RFI_3791_3805 -- 3.791 - 3.805 MHz: ANNEX F RFI_7000_7100 -- 7.000 - 7.100 MHz: ANNEX F, ETSI RFI_7000_7300 -- 7.000 - 7.300 MHz: T1E1 RFI_10100_10150 -- 10.100 - 10.150 MHz: ANNEX F, ETSI, T1E1 RFI_14000_14350 -- 14.000 - 14.350 MHz: ANNEX F, ETSI, T1E1 RFI_18068_18168 -- 18.068 - 18.168 MHz: ANNEX F, ETSI, T1E1 RFI_1800_1825 -- 1.800 - 1.825 MHz: HAM Band 1 RFI_3500_3550 -- 3.500 - 3.550 MHz: HAM Band 2 RFI_3790_3800 -- 3.790 - 3.800 MHz: HAM Band 3 RFI_1800_1810 -- 1.800 - 1.810 MHz: RFI Notch RFI_21000_21450 -- 21.000 - 21.450 MHz: ANNEX F, ETSI, T1E1 RFI_24890_24990 -- 24.890 - 24.990 MHz: ANNEX F, ETSI, T1E1 RFI_28000_29100 -- 28.000 - 29.100 MHz: ANNEX F, ETSI, T1E1 RFI_28000_29700 -- 28.000 - 29.700 MHz: ANNEX F, ETSI, T1E1
MaxUsableTone	Type in the maximum usable tone.
Framing Mode	Click on this drop-down list and select framing mode. Options are: PTM, EFM, ATM, and AUTO (PTM/EFM/ATM auto selection).
DeploymentScenario	Click on the drop-down list and select the deployment scenario: Options are FTTCAB (Fibre-to-the-cabinet), FTTEX (Fibre-to-the-exchange), OTHER.

PSD Shaping:

Line Config

Advanced

PSD Shaping

UPBO

DPBO

DownStream PSD Shaping Type: 

MAX\_PSD (VDSL)

Field	Description
Downstream PSD Shaping Type	Click on this drop-down list and select downstream PSD shaping type. Options are: MAX_PSD (VDSL), LOG_TSSI (ADSL)

UPBO:

Line Config

Advanced

PSD Shaping

UPBO

DPBO

Attribute	Value	Description
UpboKL	<div>0.0</div> [dB]	0 ~ 127.5 dB, Steps: 0.1 dB
UpboKLF	<div>Disable UPBO</div>	Select

	UPBO K1	UPBO K2	Description
OPT	<div>0</div> [0.001 dBm/Hz]	<div>0</div> [0.001 dBm/Hz]	-1000000~100000; unit: 0.001 dBm/Hz; step: 0.001 dBm/Hz
US1	<div>-60000</div> [0.001 dBm/Hz]	<div>-15780</div> [0.001 dBm/Hz]	
US2	<div>-60000</div> [0.001 dBm/Hz]	<div>-10710</div> [0.001 dBm/Hz]	
US3	<div>-60000</div> [0.001 dBm/Hz]	<div>-5400</div> [0.001 dBm/Hz]	Change of K1 and K2 values use more flexibility using UPBO.
US4	<div>0</div> [0.001 dBm/Hz]	<div>0</div> [0.001 dBm/Hz]	K1 values for lower US bands K2 values for higher US bands
US5	<div>0</div> [0.001 dBm/Hz]	<div>0</div> [0.001 dBm/Hz]	

Field	Description
UpboKL	Type in the UPBO electrical length kl0. Value range: 0 ~ 127.5 (dB).
UpboKLF	Click on this drop-down list and select: Auto: The VTUs will autonomously determine the electrical length. Override: Forces the VTU-R to use the electrical length of its line, kl0, of the CO-MIB (UPBOKL) to compute the UPBO. DisableUpbo: Disables UPBO so that UPBO is not

# DATA-CONNECT

*The Right Connection!*

Configuration

	utilized.
UPBO K1	K1 and K2 parameters allow the user more flexibility in using Upstream Power Back-Off (UPBO) on CPE modem. Changing K1 and K2 values will affect the CPE Tx PSD. Please refer to VDSL standards for exact relation between K1, K2 parameters and Tx PSD. There is a set of K1/K2 parameters associated with each upstream band in the PSD: Upstream Band 0 or Optional band, Upstream band 1, Upstream band 2, Upstream band 3, Upstream band4, and Upstream Band 5. Setting all K2 parameters to 0 and all K1 to a high power level (ie low number) will essentially disable UPBO.
UPBO K2	



DPBO:

Line Config	Advanced	PSD Shaping	UPBO	DPBO
Attribute	Value	Description		
ADSL Mode	Disable	Select ADSL Mode.		
ESEL(E-Side Electrical Length)	0.0 [dB]	Range: 0 ~ 255.5 dB; Unit: dB; Step: 0.1 dB Note : Value 0 has special meaning , it disables DPBO feature		
MUFCTRL(Shaping)	0.0 [dB]	0 ~ 255; Unit: dB ; Step: 0.1 dB		
Offset	0.0 [dB]	-25.6 ~ 255.9; Unit: dB ; Step: 0.1 dB		
ESCMA	-1.000000 [dB]	-1 ~ 1.5; Units: dB , Step : 1/256 dB (i.e. 0.00390625 dB)		
ESCMB	-1.000000 [dB]	-1 ~ 1.5; Units: dB , Step : 1/256 dB (i.e. 0.00390625 dB)		
ESCMC	-1.000000 [dB]	-1 ~ 1.5; Units: dB , Step : 1/256 dB (i.e. 0.00390625 dB)		
FMAX(DPBO Max Frequency)	138.0000	138 ~ 29997.75; Unit: KHz ; Step: 4.3125 KHz		
FMIN(DPBO Min Frequency)	0.0000 [KHz]	0 ~ 8832; Unit: KHz ; Step: 4.3125 KHz		
FMUS(Min Usable Signal)	-127.5 [dBm/Hz]	-127.5 ~ 0; Unit: dBm/Hz ; Step: 0.5 dBm/Hz		
RSEL(Remote side Electrical Length)	0.00 [dB]	0 ~ 255.99; Unit: dB ; Step: 0.01 dB		

Field	Description
ADSL Mode	Click on the drop-down list and select disable or enable ADSL mode (whether DBPO applies to ADSL mode).
ESEL (E-Side Electrical Length)	Type in E-side electrical length for Downstream Power Back-Off (DPBO). (refer to ITU-T G.997.1)
MUFCTRL (Shaping)	Type in the set of extra DPBO parameters (xDPBO) extends the flexibility of the DPBO shaping algorithm.
Offset	Type in the Extra DPBO offset by modifying the standard DPBO algorithm.
ESCMA	Type in values of parameters DPBOESCMA, DPBOESCMB, DPBOESCMC. Note: $ESCM(f) = (DPBOESCMA + DPBOESCMB * SQRT(f) + DPBOESCMC * f) * DPBOESEL$ ESCM: E-Side Cable Model
ESCMB	
ESCMC	
FMAX (DPBO Max Frequency)	Type in the DPBO upper frequency bound.
FMIN (DPBO Min Frequency)	Type in the DPBO lower frequency bound.
MUS (Min Usable Signal)	Type in the assumed minimum usable receive PSD mask.
RSEL (Remote Side Electrical	Type in the Remote side electrical length.

Length)	
---------	--

4. Click on Create.

**To modify a xDSL configuration profile:**

1. Click in the selection box next to the profile you want to modify.
2. Click on Modify Selected. The xDSL Configuration Profile Modify screen appears.
3. Modify the fields as required.
4. Click on Modify.

**To delete a xDSL configuration profile:**

1. Click in the selection box next to the profile you want to delete.
2. Click on Delete Selected.
3. You can click on Delete All to delete all configuration profiles at a time.

## 6.6 Configuration / Bridge / Interface / Setup / ADSL Bridge Port

Use the Configuration/Bridge/~ /ADSL Bridge Port screen to create, modify, and delete ADSL bridge port.

Select a tab (PVC, Bridge, or Security) on top of the screen first.

**PVC:**

PVCBridgeSecurity

Related: Bridge (Learned) Status Filters Anti-ARP Secure Forward

Previous Command Result: Normal

Create

Physical Port	VPI	VCI	Traffic Descriptor	Encapsulation	VLANTrans	
Port-1	PVC-1	0	35	1	LLC	Disable

Select page: page-1

☐ Check All☐ Uncheck All

ModifyDelete

	Physical Port	VPI	VCI	Traffic Descriptor	Encapsulation	VLANTrans
<input type="checkbox"/>	Port-3-PVC-1	0	35	1	LLC	Disable

**To create a PVC:**

1. Enter or select the following fields:

Field	Description
Physical Port	Click on the drop-down list and select the port number (1~24, or All).
VPI	Type in the VPI value: 0 ~ 255. Default value is 0.
VCI	Type in the VCI value: 21, 32 ~ 65535. Default value is 35.
Traffic Descriptor	Click on the drop-down list and select the traffic descriptor.
Encapsulation	Select AAL5 Encapsulation Type: VCMUX/LLC
VLANTrans	Enable/disable bridging according to VLAN translation / protocol based VLAN function

2. Click on Create.

**To modify a PVC:**

1. Click in the selection box next to the PVC you want to modify.
2. Modify the fields as required.
3. Click on Modify.

To delete a PVC:

- 1. Click in the selection box next to the profile you want to delete.
- 2. Click on Delete.

Bridge:

PVC

Bridge

Security

Related: Bridge (Learned) Status Filters Anti-ARP Secure Forwarding

Previous Command Result: Normal

Select page: 

page-1

☐ Check All ☐ Uncheck All

Modify

<input type="checkbox"/>	Physical Port	VLAN Mode	Ingress Filter	Acceptable Frame	Force Priority Mode
<input type="checkbox"/>	Port-3 -- PVC-1	<div>Non-TLS</div>	<div>On</div>	<div>All</div>	<div>Disabled</div>

To modify an ADSL bridge port:

- 1. Click in the selection box next to the bridge port (PVC) you want to modify. You can click in the Check All selection box to select all bridge ports at a time (To cancel the selection, click in UnCheck All selection box).
- 2. Enter or select the following fields:

Field	Description
VLAN Mode	<b>non-TLS:</b> normal VLAN mode <b>QinQ:</b> enable N:1 VLAN stacking feature (our system adds the default VLAN tag to all the incoming frames through this port) <b>TLS:</b> enable TLS (Transparent LAN Service) so that this bridge port becomes VLAN transparent (refer to DSL Forum, TR-101). A pre-configured S-Tag is used to encapsulate TLS traffic going through this port. That is, an S-Tag (PVID here) will be added to all the upstream frames received on this port, and the C-Tags will be the original tags of these frames (no C-Tag for untagged incoming frames). On the other hand, the S-Tag will be removed from all the downstream (outgoing) frames.
Ingress Filter	Click on the drop-down list and select Ingress filter On/Off. Ingress filter ON: check if the VID of the incoming frame is in the member set. If not in the member set, block the frame. Ingress filter OFF: Ingress filter disabled.
Acceptable Frame	Click on the drop-down list and select to accept ALL Frame or only VLAN tagged frame.
Force Priority Mode	Click on the drop-down list and select the priority-forcing mode. Options are: <b>Disabled:</b> Reserve the original priority of all packets.

**Force-ingress:** All packets, **no matter what VLAN ID they are**, if **they come into** this line bridge port, their VLAN priority will be changed to this line bport's default VLAN priority. No dependency on configured 'VLAN Mode'.

**Force-egress:**

For **single tagged** packet - when the line bridge port is ready to **output** the packet, if the packet's VLAN ID is equal to the line bport's default VLAN ID, the packet's VLAN priority will be changed to this line bport's default VLAN priority.

Ex. If the line bport's default VLAN ID and priority is (5,5)

Original (VID, V-Pri)	Result (VID, V-Pri)
(5,1)	(5,5)
(1,1)	(1,1)

For **double tagged** packet - if the packet's S-VID is equal to the line bport's default VLAN ID, the packet's S-Tag priority is replaced with this line bport's default priority value (but when VLAN Mode = TLS, the packet's C-Tag priority is replaced instead and the S-Tag will be removed from the packet before it is sent out).

Ex. If the line bport's default VLAN ID and priority is (5,5), VLAN Tagging mode is tagged:

When VLAN Mode = TLS,

Original S(VID, V-Pri) and C(VID, V-Pri)	Result (VID, V-Pri)
(5,1) (2,2)	(2,5)

When VLAN Mode = QinQ,

Original S(VID, V-Pri) and C(VID, V-Pri)	Result S(VID, V-Pri) and C(VID, V-Pri)
(5,1) (2,2)	(5,5) (2,2)

**Force-both:** Combine the rules of Ingress and Egress.

3. Click on Modify.



Security:

PVC

Bridge

Security

Related: Bridge (Learned) Status Filters Anti-ARP Secure Forwarding

Previous Command Result: Normal

Select page: 

page-1

☐ Check All ☐ Uncheck All

Modify

	Physical Port	Aging Time	Max Mac	Manage VLAN	Mac Learning
<input type="checkbox"/>	Port-3 -- PVC-1	300	16	Disabled	Enabled

To modify the security setting for an existing ADSL bridge port:

1. Click in the selection box next to the bridge port (PVC) you want to modify. You can click in the Check All selection box to select all bridge ports at a time (To cancel the selection, click in UnCheck All selection box).

2. Enter or select the following fields:

Field	Description
Aging Time	The aging time for MAC address table (10 ~ 600 sec). If a MAC does not transmit a new frame within the aging time, this MAC entry will be deleted from the MAC address table.
Max Mac	Type in the maximum number of MAC addresses that can be learned by the bridge port (0 ~ 512, default is 16).
Manage VLAN	Enable: this bridge port can use the management VLAN. Disable: this bridge port cannot use the management VLAN.
Mac Learning	Enable/disable MAC learning ability. Sometimes you can disable MAC learning on specified bridge port. This function is for 1:1 VLAN translation scenario.



## 6.7 Configuration / Bridge / Interface / Setup / Uplink Bridge Port

Use the Configuration/Bridge/~ /Uplink Bridge Port screen to configure the uplink bridge ports.

Previous Command Result: Normal

Related: [Status](#)

Modify

Refresh

LACP Enable

LACP Disable

	Physical Port	Max Mac	Aging Time	Ingress Filter	Acceptable Frame	Mode
<input checked="" type="checkbox"/>	GigaBit-1	1024	300	On	All	Up-Link
<input type="checkbox"/>	GigaBit-2	1024	300	On	All	Up-Link

To modify an uplink bridge port:

- Click in the selection box next to the bridge port you want to modify.
- Enter or select the following fields:

Field	Description
Max Mac	Type in the maximum number of MAC addresses that can be learned by the trunk bridge port (1 ~ 4095, default is 1024).
Aging Time	The aging time for MAC address table. If a MAC does not transmit a new frame within the aging time, this MAC entry will be deleted from the MAC address table. Value range: 10 ~ 1M (sec), default is 300 (sec).
Ingress Filter	Click on the drop-down list and select Ingress filter On/Off. Ingress filter ON: check if the VID of the incoming frame is in the member set. If not in the member set, block the frame. Ingress filter OFF: Ingress filter disabled.
Acceptable Frame	Click on the drop-down list and select to accept ALL Frame or only VLAN tagged frame.
Mode	Click on the drop-down list and specify the trunk link to be an Up-Link or User-Link.

- Click on Modify.
- Click on Refresh to retrieve current settings saved in the system.

To enable LACP mode:

Click on LACP Enable button. The following screen appears.

Previous Command Result: Success

Related: Status

Modify

Refresh

LACP Enable

LACP Disable

	Physical Port	Max Mac	Aging Time	Ingress Filter	Acceptable Frame	Mode
<input type="checkbox"/>	LACP-3	1024	300	On	All	Up-Link

LACP System

Modify

Refresh

Config. Items	Values
Actor Priority	21845

State Items	Values
Bridge ifIndex mapping	3
MAC Address	00-00-00-00-00-00
Aggregate or Individual	Aggregate
ActorOperKey	0
PartnerSystemID	00-00-00-00-00-00
PartnerSystemPriority	0
PartnerOperKey	0
Actor Admin Key	1

LACP Port

State Items	GBE1	GBE2	State Items	GBE1	GBE2
	<input checked="" type="checkbox"/> Activity <input type="checkbox"/> Timeout <input checked="" type="checkbox"/> aggregation	<input checked="" type="checkbox"/> Activity <input type="checkbox"/> Timeout <input checked="" type="checkbox"/> aggregation		<input type="checkbox"/> Activity <input type="checkbox"/> Timeout <input type="checkbox"/> aggregation	<input type="checkbox"/> Activity <input type="checkbox"/> Timeout <input type="checkbox"/> aggregation

To disable LACP mode:

Click on LACP Disable button.

LACP System

LACP System

Modify

Refresh

Config. Items	Values
Actor Priority	<input type="text" value="21845"/>

State Items	Values
Bridge ifIndex mapping	3
MAC Address	00-00-00-00-00-00
Aggregate or Individual	Aggregate
ActorOperKey	0
PartnerSystemID	00-00-00-00-00-00
PartnerSystemPriority	0
PartnerOperKey	0
Actor Admin Key	1

When LACP mode is enabled, following information is displayed:

Field	Description
Bridge ifindex mapping	Shows the bridge interface index of the LACP interface. The value is 3.
MAC Address	Shows a 6-octet value carrying the individual MAC address assigned to the Aggregator.
Aggregate or Individual	Indicating whether the Aggregation Port is able to Aggregate or is only able to operate as an Individual link.
Actor Oper Key	Shows the current operational value of the Key for the Aggregator. The administrative Key value may differ from the operational Key value. The meaning of particular Key values is of local significance.
Partner System ID	This is a 6-octet MAC address that is a unique identifier for the System that contains this Aggregator.
Partner System Priority	A value that indicates the priority value associated with the Partner's System ID. Value range is 0 ~ 65535.
Partner Oper Key	Shows the current operational value of the Key for the Aggregator. The administrative Key value may differ from the operational Key value. The meaning of particular Key values is of local significance.
Actor Admin Key	Admin Key of the Actor (read-only). The Admin Key is the current administrative value of the Key for the Aggregator. The administrative Key value may differ from the operational Key value. The meaning of particular Key values is of local significance. Valid value: 0x0000 ~ 0xFFFF (Hex). Note: Actor is the local entity in a Link Aggregation

	Control Protocol exchange; Partner is the remote entity in a Link Aggregation Control Protocol exchange.
--	----------------------------------------------------------------------------------------------------------

To modify LACP system configuration (only in LACP mode):

1. Enter the following field:

Field	Description
Actor Priority	Type in the System Priority of the Actor. System Priority is a value indicating the priority value associated with the Actor's System ID. Valid value: 0 ~ 65535.

2. Click on Modify.
3. Click on Refresh to confirm the modification succeeds.

LACP Port

LACP Port					
State Items	GBE1	GBE2	State Items	GBE1	GBE2
Actor Admin State(Fixed)	<div><div><input checked="" type="checkbox"/> Activity</div><div><input type="checkbox"/> Timeout</div><div><input checked="" type="checkbox"/> aggregation</div><div><input type="checkbox"/> synchronisation</div><div><input type="checkbox"/> collecting</div><div><input type="checkbox"/> distributing</div><div><input type="checkbox"/> defaulted</div><div><input type="checkbox"/> expired</div></div>	<div><div><input checked="" type="checkbox"/> Activity</div><div><input type="checkbox"/> Timeout</div><div><input checked="" type="checkbox"/> aggregation</div><div><input type="checkbox"/> synchronisation</div><div><input type="checkbox"/> collecting</div><div><input type="checkbox"/> distributing</div><div><input type="checkbox"/> defaulted</div><div><input type="checkbox"/> expired</div></div>	Partner Admin State	<div><div><input type="checkbox"/> Activity</div><div><input type="checkbox"/> Timeout</div><div><input type="checkbox"/> aggregation</div><div><input type="checkbox"/> synchronisation</div><div><input type="checkbox"/> collecting</div><div><input type="checkbox"/> distributing</div><div><input type="checkbox"/> defaulted</div><div><input type="checkbox"/> expired</div></div>	<div><div><input type="checkbox"/> Activity</div><div><input type="checkbox"/> Timeout</div><div><input type="checkbox"/> aggregation</div><div><input type="checkbox"/> synchronisation</div><div><input type="checkbox"/> collecting</div><div><input type="checkbox"/> distributing</div><div><input type="checkbox"/> defaulted</div><div><input type="checkbox"/> expired</div></div>
Actor Port	0	0	Partner Oper Port	0	0
Actor ID	00-00-00-00-00-00	00-00-00-00-00-00	Partner Oper ID	00-00-00-00-00-00	00-00-00-00-00-00
Actor Oper Key	0	0	Partner Oper Key	0	0
Partner Oper Priority	0	0	Partner Oper Port Priority	0	0
Actor Oper State	<div><div><input type="checkbox"/></div></div>	<div><div><input type="checkbox"/></div></div>	Partner Oper State	<div><div><input type="checkbox"/></div></div>	<div><div><input type="checkbox"/></div></div>
Aggregate Or Individual	[Aggregate]	[Aggregate]			

When LACP mode is enabled, following information is displayed:

Field	Description
Actor Admin State (Fixed) / Partner Admin State	<p>Shows the administrative state of Actor / Partner. Currently the state is fixed.</p> <p>Parameters include:</p> <p><b>Activity</b> - If the operational state shows Activity ON, this indicates the Activity control is Active LACP; otherwise, the Activity control is Passive LACP.</p> <p><b>Timeout</b> - Timeout means the Timeout control value with regard to this link. If the operational state shows Timeout ON, this indicates Short Timeout, otherwise, Long Timeout.</p> <p><b>Aggregation</b> - If the operational state shows aggregation ON, this indicates that the System considers this link to be Aggregatable; i.e., a potential candidate for aggregation. If not, the link is considered to be Individual; i.e., this link can be operated only as an individual link.</p> <p><b>Synchronization</b> - If the operational state shows Sync ON, the system considers this link to be IN_SYNC; i.e., it has been allocated to the correct Link Aggregation Group, the group has been associated with a compatible Aggregator, and the identity of the Link Aggregation Group is consistent with the System ID and operational Key information transmitted. If Sync OFF, then this link is currently OUT_OF_SYNC; i.e., it is not in the right Aggregation.</p> <p><b>Collecting</b> - If the operational state shows collecting ON, this means collection of incoming frames on this link is definitely enabled; i.e., collection is currently enabled and is</p>



# DATA-CONNECT

The Right Connection!

Configuration

	<p>not expected to be disabled in the absence of administrative changes or changes in received protocol information.</p> <p><b>Distributing</b> - If the operational state shows distributing OFF, this means distribution of outgoing frames on this link is definitely disabled; i.e., distribution is currently disabled and is not expected to be enabled in the absence of administrative changes or changes in received protocol information.</p> <p><b>Defaulted</b> - If the operational state shows defaulted ON, this indicates that the Actor's Receive machine is using defaulted operational Partner information, administratively configured for the Partner. If defaulted OFF, the operational Partner information in use has been received in a LACPDU.</p> <p><b>Expired</b> - If the operational state shows expired ON, this indicates that the Actor's Receive machine is in the EXPIRED state; if expired OFF, this indicates that</p>
Actor Port / Partner Oper Port	Shows the port number associated with this link assigned to the port by the Actor/Partner. Port number range is 0 ~ 65535.
Actor ID / Partner Oper ID	A 6-octet MAC address value that defines the value of the System ID for the System that contains this Aggregation Port.
Actor Oper Key / Partner Oper Key	Shows the current operational value of the Key for the Aggregation Port. This is a value between 0000 ~ FFFF. The meaning of particular Key values is of local significance.
Actor Oper Port Priority / Partner Oper Port Priority	Shows the current value of the port priority for the protocol Actor / Partner. Value range is 0 ~ 65535.
Actor Oper State / Partner Oper State	Shows the operational state of Actor / Partner. For more information, refer to the description for Actor Admin State / Partner Admin State.
Aggregate Or Individual	Shows current state is aggregate link or individual.



## 6.8 Configuration / Bridge / Interface / Setup / VDSL Bridge Port

Use the Configuration/Bridge/~ /VDSL Bridge Port screen to create, modify, and delete VDSL bridge port.

Select a tab (Bridge or Security) on top of the screen first.

### Bridge:

Bridge

Security

Related: Bridge (Learned) Status Filters Anti-ARP Secure Forwarding

Previous Command Result: Normal

Create

Physical Port	VPMT Profile	Ingress Filter	Acceptable Frame	VLAN Mode	VLANTrans	Force Priority Mode
Port-1	1	On	All	Non-TLS	Disable	Disable

Select page: page-1 ☐ Check All ☐ Uncheck All

ModifyDelete

	Physical Port	VPMT Profile	VLAN Mode	Ingress Filter	Acceptable Frame	VLANTrans	Force Priority Mode
<input type="checkbox"/>	Port-1	1	Non-TLS	On	All	Disable	Disable
<input type="checkbox"/>	Port-2	1	Non-TLS	On	All	Disable	Disable

### To create a VDSL bridge port:

1. Enter or select the following fields:

Field	Description
Physical Port	Click on the drop-down list and select the port number (1~24, or All).
VPMT Profile	Click on the drop-down list and select a VPMT (VLAN priority mapping table) profile to bind.
Ingress Filter	Click on the drop-down list and select Ingress filter On/Off. Ingress filter ON: check if the VID of the incoming frame is in the member set. If not in the member set, block the frame. Ingress filter OFF: Ingress filter disabled.
Acceptable Frame	Click on the drop-down list and select to accept ALL Frame or only VLAN tagged frame.
VLAN Mode	<b>non-TLS</b> : normal VLAN mode <b>QinQ</b> : enable N:1 VLAN stacking feature (our system adds the default VLAN tag to all the incoming frames through this port) <b>TLS</b> : enable TLS (Transparent LAN Service) so that this bridge port becomes VLAN transparent (refer to DSL Forum, TR-101). A pre-configured S-Tag is used to encapsulate TLS traffic going through this port. That is, an S-Tag (PVID here) will be added

	to all the upstream frames received on this port, and the C-Tags will be the original tags of these frames (no C-Tag for untagged incoming frames). On the other hand, the S-Tag will be removed from all the downstream (outgoing) frames.														
VLANTrans	Enable/disable bridging according to VLAN translation / protocol based VLAN function														
Force Priority Mode	<p>Click on the drop-down list and select the priority-forcing mode. Options are:</p> <p><b>Disabled:</b> Reserve the original priority of all packets.</p> <p><b>Force-ingress:</b> All packets, <b>no matter what VLAN ID they are</b>, if <b>they come into</b> this line bridge port, their VLAN priority will be changed to this line bport's default VLAN priority. No dependency on configured 'VLAN Mode'.</p> <p><b>Force-egress:</b></p> <p>For <b>single tagged</b> packet - when the line bridge port is ready to <b>output</b> the packet, if the packet's VLAN ID is equal to the line bport's default VLAN ID, the packet's VLAN priority will be changed to this line bport's default VLAN priority.</p> <p>Ex. If the line bport's default VLAN ID and priority is (5,5)</p> <table><tr><th>Original (VID, V-Pri)</th><th>Result (VID, V-Pri)</th></tr><tr><td>(5,1)</td><td>(5,5)</td></tr><tr><td>(1,1)</td><td>(1,1)</td></tr></table> <p>For <b>double tagged</b> packet - if the packet's S-VID is equal to the line bport's default VLAN ID, the packet's S-Tag priority is replaced with this line bport's default priority value (but when VLAN Mode = TLS, the packet's C-Tag priority is replaced instead and the S-Tag will be removed from the packet before it is sent out).</p> <p>Ex. If the line bport's default VLAN ID and priority is (5,5), VLAN Tagging mode is tagged:</p> <p>When VLAN Mode = TLS,</p> <table><tr><th>Original S(VID, V-Pri) and C(VID, V-Pri)</th><th>Result (VID, V-Pri)</th></tr><tr><td>(5,1) (2,2)</td><td>(2,5)</td></tr></table> <p>When VLAN Mode = QinQ,</p> <table><tr><th>Original S(VID, V-Pri) and C(VID, V-Pri)</th><th>Result S(VID, V-Pri) and C(VID, V-Pri)</th></tr><tr><td>(5,1) (2,2)</td><td>(5,5) (2,2)</td></tr></table> <p><b>Force-both:</b> Combine the rules of Ingress and Egress.</p>	Original (VID, V-Pri)	Result (VID, V-Pri)	(5,1)	(5,5)	(1,1)	(1,1)	Original S(VID, V-Pri) and C(VID, V-Pri)	Result (VID, V-Pri)	(5,1) (2,2)	(2,5)	Original S(VID, V-Pri) and C(VID, V-Pri)	Result S(VID, V-Pri) and C(VID, V-Pri)	(5,1) (2,2)	(5,5) (2,2)
Original (VID, V-Pri)	Result (VID, V-Pri)														
(5,1)	(5,5)														
(1,1)	(1,1)														
Original S(VID, V-Pri) and C(VID, V-Pri)	Result (VID, V-Pri)														
(5,1) (2,2)	(2,5)														
Original S(VID, V-Pri) and C(VID, V-Pri)	Result S(VID, V-Pri) and C(VID, V-Pri)														
(5,1) (2,2)	(5,5) (2,2)														

2. Click on Create.

**To modify a VDSL bridge port:**

1. Click in the selection box next to the bridge port you want to modify.
2. Modify the fields as required.
3. Click on Modify.

**To delete a VDSL bridge port:**

1. Click in the selection box next to the profile you want to delete.
2. Click on Delete.

Security:

Bridge

Security

Related: Bridge (Learned) Status Filters Anti-ARP Secure Forwarding

Previous Command Result: Normal

☐ Check All

☐ Uncheck All

Modify

	Physical Port	Aging Time	Max Mac	Manage VLAN	Mac Learning
<input type="checkbox"/>	Port-1	300	16	Disabled	Enabled
<input type="checkbox"/>	Port-2	300	16	Disabled	Enabled

To modify the security setting for an existing VDSL bridge port:

1. Click in the selection box next to the bridge port you want to modify. You can click in the Check All selection box to select all bridge ports at a time (To cancel the selection, click in UnCheck All selection box).

2. Enter or select the following fields:

Field	Description
Aging Time	The aging time for MAC address table (10 ~ 600 sec). If a MAC does not transmit a new frame within the aging time, this MAC entry will be deleted from the MAC address table.
Max Mac	Type in the maximum number of MAC addresses that can be learned by the bridge port (0 ~ 512, default is 16).
Manage VLAN	Enable: this bridge port can use the management VLAN. Disable: this bridge port cannot use the management VLAN.
Mac Learning	Enable/disable MAC learning ability. Sometimes you can disable MAC learning on specified bridge port. This function is for 1:1 VLAN translation scenario.

3. Click on Modify.

6.9 Configuration / Bridge / Interface / Setup / xDSL Interface

Use the Configuration/Bridge/~xDSL Interface screen to configure xDSL interfaces.

Configuration / Bridge / Interface / Setup / xDSL Interface

Previous Command Result: Normal

Related: Bridge (Learned) Status Filters Anti-ARP Secure Forward

☐ Check All ☐ Uncheck All ☐ Check All to Enable ☐ Check All to Disable

Refresh

Modify

	Physical Port	Admin Status	Op Status	Config. Profile	Alarm Profile	PortID	PhoneNumber	Description
<input type="checkbox"/>	Port-1	Off	Idle	DEFVAL	DEFVAL			
<input type="checkbox"/>	Port-2	Off	Idle	DEFVAL	DEFVAL			
<input type="checkbox"/>	Port-3	Off	Idle	DEFVAL	DEFVAL			
<input type="checkbox"/>	Port-4	Off	Idle	DEFVAL	DEFVAL			
<input type="checkbox"/>	Port-5	Off	Idle	DEFVAL	DEFVAL			
<input type="checkbox"/>	Port-6	Off	Idle	DEFVAL	DEFVAL			
<input type="checkbox"/>	Port-7	Off	Idle	DEFVAL	DEFVAL			
<input type="checkbox"/>	Port-8	Off	Idle	DEFVAL	DEFVAL			
<input type="checkbox"/>	Port-9	Off	Idle	DEFVAL	DEFVAL			
<input type="checkbox"/>	Port-10	Off	Idle	DEFVAL	DEFVAL			

To modify a xDSL interface:

1. Click in the selection box next to the bridge port you want to modify. You can click in the Check All selection box to select all bridge ports at a time (To cancel the selection, click in UnCheck All selection box).
2. Enter or select the following fields:

Field	Description
Check All to Modify	Clicking on this checkbox is equal to select the <i>Modify</i> checkboxes of all circuits.
Check All to Enable	Click on this checkbox to service-on all the circuits.
Check All to Disable	Click on this checkbox to service-off all the circuits.
Modify	Once you have changed the parameter value, click on this button to apply the modification.
Refresh	Click on this button to get most recent setup and status of the circuits.
Physical Port	Lists the physical port numbers.
Admin Status	Click on the drop-down list and select the Administrative status: ON (port enabled) or OFF (port disabled). You can click on Check All to Enable to enable all ports or click on Check All to Disable to disable all ports.
Op Status	Shows current operational status of the port.
Config. Profile	Click on the drop-down list and select the xDSL configuration profile to bind with the port.
Alarm Profile	Click on the drop-down list and select the xDSL alarm profile to bind with the port.
PortID	Type in the line identifier.

# DATA-CONNECT

*The Right Connection!*

Configuration

PhoneNumber	Type in the phone number of this line.
Description	Type in any comment of this line.

- 3. Click on Modify.
- 4. Click on Refresh to display the latest status.



### 6.10 Configuration / LLDP / Link Layer Discovery Protocol (LLDP)

Link Layer Discovery Protocol (LLDP) operates on data link layer. It stores and maintains the information about the local device and the devices directly connected to it for network administrators to manage networks through network management systems. In LLDP, device information is encapsulated in LLDPDUs in the form of TLV (meaning type, length, and value) triplets and is exchanged between directly connected devices. Information in LLDPDUs received is restored in standard MIB (management information base).

Use the Configuration/LLDP/Link Layer Discovery Protocol (LLDP) screen to configure LLDP function for the system.

Select a tab (System Config, Local Port, or Remote Port) on top of the screen first.

System Config:

System Config

Local Port

Remote Port

Previous Command Result: Normal

Modify

LLDP system admin status

Disable

The holdtime to be sent (Sec)

4

LLDP SysTime Message TxInterval (Sec)

30

Re-init delay (Sec)

2

LLDP SysTime TxDelay (Sec)

2

Chass ID subtype

MAC Address

Chass ID

00:FF:63:8E:26:C2

System Name

localhost

System Description

VDSL2 IP-DSLAM-DC VDSL2 24-port

System Capability Supported

0x00000004(Bridge)

System Capability Enabled

0x00000004(Bridge)

Management Address type

IPV4

Management Address

192.168.005.003

Interface numbering method

lIndex

Management Interface Number

--

The OID of management address

1.3.6.1.4.1.5833.18

The following information is displayed:

# DATA-CONNECT

The Right Connection!

Configuration

Field	Description
Chassis ID subtype	Shows the chassis subtype of chassis ID TLV. Valid values are: Chassis Component, Interface Alias, Port Component, MAC Address, Network Address, Interface Name, Locally Assigned
Chassis ID	Shows the value of chassis ID.
System Name	Shows the string value used to identify the system name.
System Description	Shows the string value used to identify the system description.
System Capability Supported	Shows system capabilities supported on the local system. Valid values are: BITS{ station(0), docsis(1), telephone(2), router(3), wap(4), bridge(5), repeater(6), other(7) }
System Capability Enabled	Shows system capabilities enabled on the local system. Valid values are: BITS{ station(0), docsis(1), telephone(2), router(3), wap(4), bridge(5), repeater(6), other(7) }
Management Address Type	Show the type of management address. Valid values are: IPV4, all802
Management Address	Shows the string value used to identify the management address component associated with the local system.
Interface numbering method	Shows the enumeration value that identifies the interface numbering method used for defining the interface number, associated with the local system. Valid values are: unknown, ifindex, and systemportnumber
Management Interface Number	Shows the integer value used to identify the interface number regarding the management address component associated with the local system.

The OID of management address	Shows the OID value used to identify the type of hardware component or protocol entity associated with the management address advertised by the local system agent.
-------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------

To modify the system’s LLDP configuration:

1. Enter or select the following fields:

Field	Description
LLDP system admin status	Select the LLDP administrative status of the system (Disable/Enable).
The hold time to be sent (sec)	Enter this parameter value, which is a multiplier on the next parameter (see the Field 'The rate at which LLDP packets are sent (sec)') that determines the actual TTL value used in an LLDPDU. Value range: 2 ~ 10. Default value is 4.
The rate at which LLDP packets are sent (sec)	Enter the interval at which LLDP frames are transmitted on behalf of this LLDP agent. Value range: 5 ~ 32768. Default value is 30.
Re-init delay (sec)	Enter the amount of delay from when admin status becomes 'disabled' until re-initialization will be attempted. Value range: 1 ~ 10. Default value is 2.
Delay between successive LLDP frame transmissions (Sec)	Enter the delay between successive LLDP frame transmissions initiated by value or status changes in the LLDP local systems MIB. The value for this parameter is set by the following range formula: 1 <= this parameter value <= (0.25 * the interval at which LLDP frames are transmitted). Value range: 1~8192. Default value is 2.

2. Click on Modify.

Local Port:

System Config

Local Port

Remote Port

Previous Command Result: Success

Select Port: GigaBit-1

Query

Modify

Tx/Rx Config

TX only

LLDP option tlvs

☒ port-desc-tlv

☒ sys-name-tlv

☒ sys-desc-tlv

☒ sys-cap-tlv

☒ man-addr-tlv

☒ port-vlan-tlv

☒ port-protocol-vlan-tlv

☒ protocol-id-tlv

☒ mac-phy-cfg-tlv

☒ link-aggr-tlv

☒ max-frame-size-tlv

number limitation of LLDP received

no limitation

Port Id Subtype

Interface Name

Port Id

GbE-1

Port Description

GigabitEthernet-1

VLAN ID

1

Protocol VLAN Supported

No

Protocol VLAN Enabled

No

Protocol VLAN ID

--

The following information is displayed:

Field	Description
Port ID Subtype	Shows the port ID subtype of Port ID TLV. Valid values are: Chassis Component, Interface Alias, Port Component, MAC Address, Network Address, Interface Name, Locally Assigned
Port ID	Shows the value of Port ID TLV.

Other displayed information depends on the supported TLVs (LLDP Option TLVs) you select:

Field	Description
Port Description	(When port-desc-tlv is selected) Shows the string value used to identify the IEEE 802 LAN station's port description associated with the local system.
VLAN ID	This field is shown when port-vlan-tlv is selected.
Protocol VLAN Supported	These fields are shown when port-protocol-vlan-tlv is selected.
Protocol VLAN Enabled	
Protocol VLAN ID	
Protocol ID	This field is shown when protocol-id-tlv is selected.
Auto Negotiation Supported	These fields are shown when mac-phy-cfg-tlv is selected. Note that MAU is an acronym for Medium Attachment Unit.
Auto Negotiation Enabled	
Auto Negotiation Capability Advertised	
Operational MAU Type	
Link Aggregation Status	These fields are shown when link-agg-tlv is selected.
Link Aggregation Port ID	
Maximum Frame Size	This field is shown when max-frame-size-tlv is selected.

To modify the LLDP configuration per port:

1. Click on *Select Port* drop-down list and select a port you want to modify the configuration for.
2. Enter or select the following fields:

Field	Description
Tx/Rx Config	Select LLDP Transmit and Receive mode for advertisement. Options are: Disable, Tx only, Rx only, Tx and Rx. Default is 'Disable'.
LLDP Option TLVs	Click in the selection box to select the supported TLVs. Available options are: port-desc-tlv (Port description TLV), sys-name-tlv (System name TLV), sys-desc-tlv (System description TLV), sys-cap-tlv (System capability TLV), man-addr-tlv (Management address TLV), port-vlan-tlv (Port VLAN ID TLV), port-protocol-vlan-tlv (Port and protocol VLAN ID TLV), protocol-id-tlv (Protocol identity TLV), mac-phy-cfg-tlv (MAC/PHY configuration/Status TLV), link-agg-tlv (Link aggregation TLV), max-frame-size-tlv (Maximum frame size TLV).
Number limitation of LLDP received	Select the LLDP number of bridge port, which can receive LLDP frame with different MSAP. The value may be 1~20, or no limitation

3. Click on Modify.

Remote Port:

System Config

Local Port

Remote Port

Previous Command Result: Normal

Select Port: 

GigaBit-1

Query

Clear Remote DB

The 5224AV-2GBE/2SFP maintains a table containing adjacent devices’ information by collecting LLDP packets transmitted by neighboring devices. The system supports aging out mechanism for entries in LLDP neighboring device information table according to the TTL value carried in received LLDP packets (when time is up, the entry is cleared). The system also refresh entries in LLDP neighboring device information table on receiving new LLDP packets with the same ‘Chassis ID’ and ‘Port ID’ TLVs.

To view the adjacent device’s information received from a port:

1. Click on *Select Port* drop-down list and select a port through which the LLDP packets are received.
2. Click on Query to get the latest data.
3. To clear neighboring device information table, click on clear remote DB.



6.11 Configuration / Bridge / Policer / Policer – Rate Limit Profile

Use the Configuration/Bridge/Policer/Policer – Rate Limit Profile screen to configure rate limit policer profiles.

Configuration / Bridge / Policer / Policer - Rate Limit Profile

Previous Command Result: SuccessRelated: Broadcast Port VLAN

Create NewDelete SelectedDelete All

	Profile Index	Profile Mode	CIR	CBS	Color Aware	Non Conf	Color Field	EIR	EBS	Green Val	Yellow Val	Red Val
<input type="checkbox"/>	1	Single Leaky Bucket	1000000000 [bps]	80 [ms]	Color Blind	To Discard	Vlan Priority	1000000000 [bps]	80[ms]	7	3	1
<input checked="" type="checkbox"/>	2	Single Leaky Bucket	1000000000 [bps]	80 [ms]	Color Blind	To Discard	DSCP	1000000000 [bps]	80[ms]	7	3	1

The 5224AV-2GBE/2SFP supports TCM Policer in accordance with the Metro Ethernet Forum (MEF) Bandwidth Profile and RFCs 2697 & 2698. Our TCM Policer supports both Color Aware and Color Blind modes. The “color” is used for determining whether a packet will proceed to the policer when TCM Policer works in Color Aware mode; also in the policer the packet may be remarked with new color according to the packet’s conformance to the policer rules. A packet is considered green when it enters the TCM Policer only if its input color field, VLAN priority bits or DSCP field, has the same value with the green value configured in this page (see also the following parameter description). Likewise, a packet is considered yellow only if its input color field has the same value with the yellow value configured in this page. All other values are considered red. Once a packet has passed through the TCM Policer, it will be directed to the class queues for scheduling.

The 5224AV-2GBE/2SFP supports two kinds of TCM Policer: two-rate TCM (with dual leaky buckets) and single-rate TCM (with single leaky bucket).

The single-rate TCM meters a traffic stream and marks its packets according to Committed Information Rate (CIR) and Committed Burst Size (CBS) to be either green, or red. The single-rate TCM operates with a single leaky bucket that is updated according to only one rate, the committed information rate - CIR. A packet is marked green if the leaky bucket is not full and red otherwise.

The two-rate TCM meters a traffic stream and marks its packets based on two rates, Committed Information Rate (CIR) and Excess Information Rate (EIR), and their associated burst sizes, Committed Burst Size (CBS) and Excess Burst Size (EBS), to be either green, yellow, or red. The two-rate TCM operates with dual leaky bucket, where each bucket is updated according to a different rate. The first bucket is updated according to the CIR, the second bucket is updated according to the EIR. A packet is marked red if it exceeds the PIR. Otherwise it is marked either yellow or green depending on whether it exceeds or doesn’t exceed the EIR.

To create a rate limit profile:

- 1. Click on Create New button. The following screen appears:

Create

Profile Index: 3

Attribute	Value
Profile Mode	Single Leaky Bucket
CIR	1000000000 [bps]
CBS	80 [ms]
Color Aware	Color Blind
Non Conf	To Discard
Color Field	Vlan Priority
EIR	1000000000 [bps]
EBS	80 [ms]
Green Val	7
Yellow Val	3
Red Val	1

2. Enter or select the following fields:

Field	Description
Profile Mode	For Single Leaky Bucket mode, there is one controlling parameter: CIR. For Dual Leaky Bucket mode, there are two controlling parameters: CIR and EIR.
CIR	Committed Information Rate (bit per second). The threshold rate to turn on the rate-limit mechanism. Value range is 1536 ~ 10000000000.
CBS	Committed Burst Size. The unit is millisecond. This parameter ranges from 1 to 1024. The first bucket depth is the product of CIR and this parameter.
Color Aware	<b>Color aware</b> mode: the packets are classified before they're sent through the policer. <b>Color blind</b> mode: the packets are directed through the entire policer regardless of their color.
Non Conf	This parameter defines the action for non-conforming packets. You can choose Tag or Discard. If Tag is chosen, then all the packets will be marked as red in the Color field rather than be discarded.
Color Field	There are two fields you can select for determining the packet's input color: the VLAN priority bits within the Ethernet header or the DSCP field within the IP header.
EIR	Excess Information Rate (1536 ~ 1G bits per second) controls the number of tokens in the second bucket (EBS)

	bucket).
EBS	Excess Burst Size. The unit is millisecond. This parameter ranges from 1 to 1024. The second bucket depth is the product of EIR and this parameter.
Green Val	Type in the green color value that is used when determining a packet's input color (for Color Aware mode) or remarking a packet's output color as green. Valid value is 0 ~ 7 for VLAN Priority color field or 0 ~ 63 for DSCP color field.
Yellow Val	Type in the yellow color value that is used when determining a packet's input color (for Color Aware mode) or remarking a packet's output color as yellow. Valid value is 0 ~ 7 for VLAN Priority color field or 0 ~ 63 for DSCP color field.
Red Val	Type in the red color value that is used when remarking a packet's output color as red. Valid value is 0 ~ 7 for VLAN Priority color field or 0 ~ 63 for DSCP color field.

3. Click on Create.

**To modify a rate limit profile:**

1. Click in the selection box next to the Profile Index of the profile you want to modify. Note that the system default profile (profile index 1) cannot be modified.
2. Click on Modify Selected. Then modify the fields as required.
3. Click on Modify.

**To delete a rate limit profile:**

1. Click in the selection boxes next to the Profile Index of the profiles you want to delete. Note that the system default profile (profile index 1) cannot be deleted.
2. Click on Delete Selected.

### 6.12 Configuration / Bridge / Policer / Policer – Broadcast Select

Use the Configuration/Bridge/Policer/Policer – Broadcast Select screen to modify the policer profile for broadcast traffic per bridge port.

Previous Command Result: Normal

Related: Policer Port VLAN

Select page: page-1

☐ Check All ☐ Uncheck All

Modify

	Physical Port	Ingress
<input type="checkbox"/>	Gigabit-1	1
<input type="checkbox"/>	Gigabit-2	1
<input type="checkbox"/>	Port-3--PVC-1	1
<input type="checkbox"/>	Port-1--VDSLMode	1
<input type="checkbox"/>	Port-2--VDSLMode	1

**To modify the broadcast policer profile for a port:**

1. Click in the selection box next to the bridge port you want to modify. You can click in the Check All selection box to select all bridge ports at a time (To cancel the selection, click in UnCheck All selection box).
2. Select the desired profile for the 'Modify Ingress' field.
3. Click on Modify.

### 6.13 Configuration / Bridge / Policer / Policer – Port Select

Use the Configuration/Bridge/Policer/Policer – Port Select screen to select policer profiles (rate limit profiles) to limit ingress/egress data rate for a line bridge port.

Configuration / Bridge / Policer / Policer - Port Select

Previous Command Result: Normal

Related: Policer Broadcast VLAN

Select page: page-1

☐ Check All ☐ Uncheck All

Modify

	Physical Port	Egress CIR	Egress Leaky Bucket	Ingress CIR	Ingress Leaky Bucket	Egress Policer	Ingress Policer
<input checked="" type="checkbox"/>	Port-2--PVC-1	Unlimited	80	Unlimited	80	1	1
<input type="checkbox"/>	Port-1--VDSLMode	Unlimited	80	Unlimited	80	1	1

To modify the rate limit profile for a port:

1. Click in the selection box next to the bridge port you want to modify. You can click in the Check All selection box to select all bridge ports at a time (To cancel the selection, click in UnCheck All selection box).

Field	Description
Physical Port	Shows the physical port number and its mode (ATM PVC or Packet)
Egress Policer Index	Shows current policer profile index for Egress direction.
Ingress Policer Index	Shows current policer profile index for Ingress direction.
Egress CIR	Shows current CIR for Egress direction.
Egress Leaky Bucket	Shows current Leaky Bucket size for Egress direction.
Ingress CIR	Shows current CIR for Ingress direction.
Ingress Leaky Bucket	Shows current Leaky Bucket size for Ingress direction.

2. Select the following fields:

Field	Description
Egress	Select the desired policer profile index for Egress direction.
Ingress	Select the desired policer profile index for Ingress direction.

3. Click on Modify.



### 6.14 Configuration / Bridge / Policer / Policer – VLAN Select

Use the Configuration/Bridge/Policer/Policer – VLAN Select screen to select policer profile to limit data rate per VLAN plus per bridge port.

Configuration / Bridge / Policer / Policer - VLAN Select

Previous Command Result: SuccessRelated: Policer Broadcast Port

Create NewModify SelectedDelete SelectedDelete All

	Index	Physical Port	VID	Egress	Ingress
<input checked="" type="checkbox"/>	1	Port-1--VDSLMode	1	1	1

To create a per-VLAN-plus-per-bridge-port rule:

- 1. Click on Create New. The Policer – VLAN Select – Create screen appears.
- 2. Enter or select the following fields:

Field	Description
Index	Shows the rule index.
Physical Port	Select the bridge port.
VID	Type in the VLAN ID (1 ~ 4094).
Egress	Select the desired policer profile index for Egress direction.
Ingress	Select the desired policer profile index for Ingress direction.

- 3. Click on Create.

To modify a per-VLAN-plus-per-bridge-port rule:

- 1. Click in the selection box next to the entry index you want to modify.
- 2. Click on Modify Selected. The Policer – VLAN Select – Modify screen appears.
- 3. Modify the fields as required.
- 4. Click on Modify.

To delete a per-VLAN-plus-per-bridge-port rule:

- 1. Click in the selection box next to the entry index you want to delete.
- 2. Click on Delete Selected.
- 3. You can click on Delete All to delete all entries at a time.



6.15 Configuration / Bridge / System-Wide Services

Use the Configuration/Bridge/System-Wide Services screen to enable/disable system-wide services.

Configuration / Bridge / System-Wide Services

Previous Command Result: Normal

Modify

Ext-TPID	0x 8100
Allow Downstream Broadcast	Enable
AgingTime PerPort	Disable
Mac Learning Rule	Normal
CDP	none of all
Ring Topology	Enable
Only Allow PPPoE	Disable
ACL Service	Disable
PPPoE Service	Disable
Filter And Priority Remark Service	Disable
RateLimit Service	Disable
VLAN Translation Service	Disable
NetBIOS Denial Service	Disable
Allow IP Service	Disable
Anti ARP Spoofing	Disable
Anti Mac Spoofing	Enable
Add AllowIpBySnoopDHCP	Disable

To enable or disable system-wide services:

1. Select the following fields:

Field	Description
Ext-TPID	Select the EtherType for the 802.1ad tagging, i.e. S-Tags. Options are: 0x88a8 (802.1ad) or 0x8100 (802.1q, Q-in-Q).
Allow Downstream Broadcast	The 5224AV-2GBE/2SFP protects the aggregation network and BNGs from broadcast storms at user and network port levels. It supports filtering out broadcast frames (destination MAC address

	0xFFFFFFFFFFFF) in the downstream direction. When Allow Downstream Broadcast is disabled, only protocol- specific broadcasts (DHCP, ARP) frames are allowed to be forwarded to downstream users. Default is enable.
Aging Time per Port	Enable/disable aging timer for the MAC address table per bridge port. Default is disable.
Mac Learning Rule	<b>Normal:</b> stop learning new MAC address when the bridge port has learned maximum supported MACs. <b>Delete Oldest Entry:</b> delete the oldest MAC address if the bridge port has learned maximum supported MACs while coming a new MAC. Default is Delete Oldest Entry.
CDP	Select the value to configure the system to allow Cisco’s proprietary CDP (Cisco Discovery Protocol) messages to be forwarded between trunk ports and/or between DSL ports and trunk ports. <b>Uplink-only:</b> Enable CDP messages to be forwarded between trunk ports, disable DSL CDP. <b>DSL-only:</b> Enable CDP messages to be forwarded between DSL line port and uplink port. <b>Both:</b> Enable Uplink & DSL CDP. <b>None of all:</b> Disable Uplink & DSL CDP.
Ring Topology	Enable/disable ring topology. Default is enable.
Only Allow PPPoE	The 5224AV-2GBE/2SFP supports an option to block all upstream traffic except PPPoE in all subscriber ports on a per system basis. When Only Allow PPPoE is enabled, only PPPoE frames are allowed to be forwarded to system. Default is Disable.
ACL Service	Select Enable to enable the following functions: Bridge port broadcast policer, downstream broadcast, Secure Forwarding, Anti ARP Spoofing, DHCP Relay, DHCP Server, and DHCP Snooping.
PPPoE Service	Enable/disable PPPoE Service.
Filter And Priority Remark Service	Enable/disable Filter and Priority Remark function.
Rate Limit Service	Enable/disable rate limit function for line bridge ports.
VLAN Translation Service	Enable/disable VLAN translation function.
NetBios Denial Service	Enable/disable denial Access Control List function in Configuration/Filtering.
Allow IP Service	Enable/disable Allow IP Filtering function.
Anti ARP Spoofing	Enable/disable ARP anti-spoofing service.

Anti Mac Spoofing	Enable/disable MAC address anti-spoofing service.
Add AllowIpBySnoopDHCP	Enable/disable allowed IP to be created via snooping DHCP sequences. When Allow IP Service is enabled, the packets received from a user port will be forwarded only if their source IP addresses are in the allowed IP list. The allowed IP list is either created via snooping DHCP sequences or manually configured by users.

2. Click on Modify.

6.16 Configuration / Cluster Configuration

Use the Configuration/Cluster Configuration screen to setup Cluster function, which can make a group of NEs (network elements) work together as a single NE from the management point of view.

Configuration / Cluster Configuration

Previous Command Result: Normal

Cluster Configuration:

Modify

\*Operators can only modify the local configuration.

Management IP address	0 . 0 . 0 . 0
Management Netmask	0 . 0 . 0 . 0
Management Gateway	0 . 0 . 0 . 0
Cluster Interface Selection	GBE (In Band)
Priority	0x0
Name	localhost
Domain	localdomain
Cluster Version	3.0.1.9
Cluster Protocol	Disable
Configured Roles	Slave Only

Cluster Status:

Cluster ID	0
Cluster State	CLUSTER_STATE_IDLE(0)
Cluster Failure State	CLUSTER_FAILURE_STATUS_NONE(0)
Member Count	0

Member Information:

ID	IP	Name
----	----	------

By default, the IPDSLAM is not in a cluster. The field Cluster Protocol shows “Disabled”. Before you group a Master and a Slave IPDSLAM, some parameters need to be well configured:

- 1. Cluster domain name: The group name for a cluster. Must be the same on Master and Slaves within a cluster group.
- 2. Cluster IP address: IP address to be used for remote management when Master and Slave are grouped together. Only one IP address is required for Master/slaves management within a cluster group.
- 3. NE cluster name: A unique name to identify the NE (Master or Slave) in a cluster group.

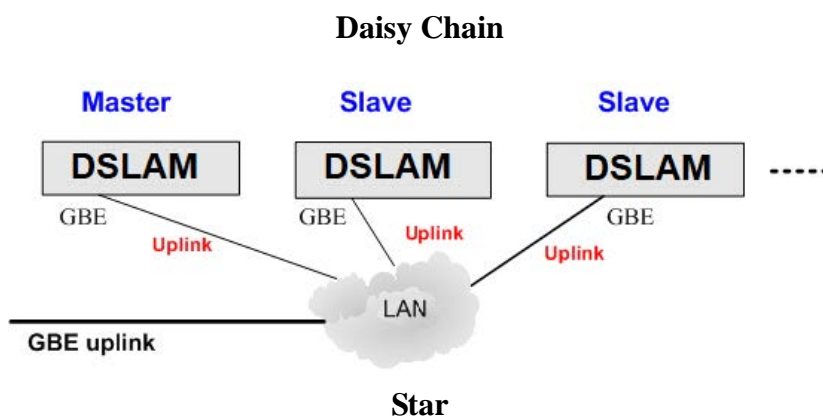
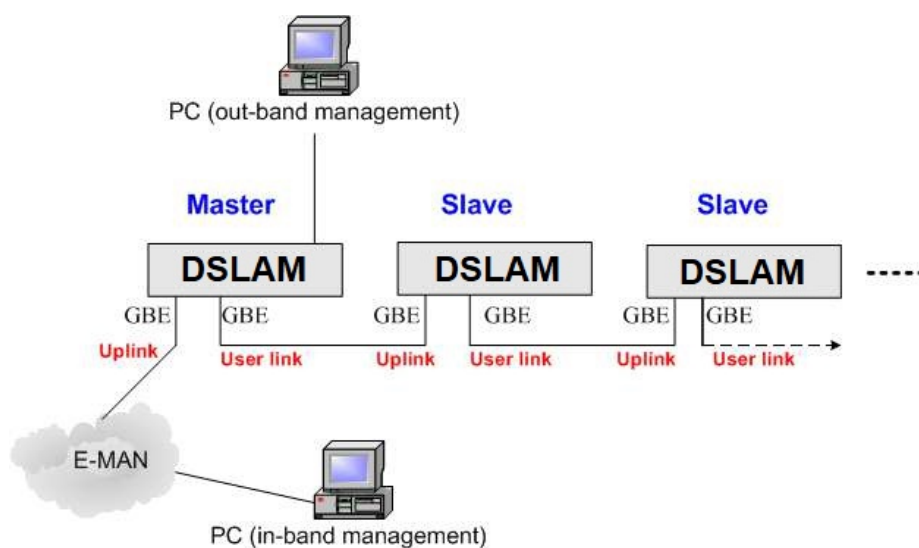
# DATA-CONNECT

## *The Right Connection!*

Configuration

4. Set private IP address on in-band port for both Master and Slave IPDSLAM. The private IP is used for communication between Master and Slave. The management center actually uses Cluster IP address for remote management.
5. Master and Slave need to be configured with same management VLAN.
6. The default gateway should be configured to the router that is aware how to route management traffic to Management Center of the management network. The setting of Cluster default gateway should be the same between Master and Slave.

Currently a 5224AV-2GBE/2SFP cluster can support up to 16 cluster members (NEs). The NEs in a cluster must all be in-band connected through the GBE port or out-band connected through the MGMT port. There are two possible network topologies for conducting a Clustering Management group: Daisy chain and Star.



For a cluster in Daisy Chain topology, each IPDSLAM must have one GBE port configured as Uplink and the other one configured as User link.

You can control all the IPDSLAMs in a cluster by connecting to the Cluster IP address, or by directly connecting to the Master IPDSLAM via its configured in-band or out-band IP address.

**To modify the cluster configuration:**



1. Enter or select the following fields:

Field	Description
Management IP address	Type in the cluster IP address. Users can connect to and manage the cluster via the cluster IP address through in-band connection.
Management Netmask	Type in the cluster's subnet mask.
Management Gateway	Type in the cluster's gateway IP address.
Cluster Interface Selection	Click on the drop-down list and select the connecting interface through which the DSLAMs are connected with each other in a cluster. Two kinds of interfaces are provided: GBE (in-band connection) and MGMT (out-band connection). This selection is available only when in Cluster Idle state (the DSLAM is not in a cluster).
Priority	Type in 0 or a positive integer as the priority to be Master. 0 means to let system decides Master and Slaves. If positive integer is typed in, the smaller the number is, the higher priority for the DSLAM to be a master in a cluster. But if there's already a Master in a cluster, a new added DSLAM cannot try to be the Master by entering a smaller voting key number; the Master cannot be changed in this way.
Name	Type in the NE name in the cluster (1 ~ 255 characters). Note that the name here is identical to the System Name set in the System Information page. If you modify the Name here, the System Name will also be changed accordingly.
Domain	Type in the name of the cluster domain.
Cluster Version	This field shows the Cluster protocol version. DSLAMs with different Cluster Version may fail to group as a cluster.
Cluster Protocol	Select to enable or disable cluster protocol.
Configured Roles	Valid options are: Master or Slave (Master or Slave is decided by the system), Slave Only (role for the DLSAM is always Slave).

2. Click on Modify.

3. The following information is displayed in Cluster Status:

Field	Description
Cluster ID	Shows the ID of the NE in the Cluster
Cluster State	Shows current state of the cluster. Possible states include: IDLE, REINIT, DISCOVERING, REQUESTING, VOTING, UNMANAGED, SLAVE, and MASTER.
Cluster Failure State	Shows the failure condition when a failure occurs in the cluster. Possible failure states include: NONE, Name Duplicated (cluster has hosts that have the same name), Out of Capacity



# DATA-CONNECT

*The Right Connection!*

Configuration

	(cluster is out of capacity), and Master Duplication (cluster has two masters).
Member Count	Shows the count of cluster members.

### 6.17 Configuration / Cluster Legacy

Use the Configuration/Cluster Legacy screen to configure legacy cluster group settings.

Configuration / Cluster Legacy

Previous Command Result: Normal.

Legacy Cluster Group Info:

Modify

Management IP Address of the cluster master	0.0.0.0
Web Port of the cluster master	80
Legacy Cluster Group Status	Not Active

To modify legacy cluster group settings:

1. Enter the following fields:

Field	Description
Management IP Address of the cluster master	Enter the management IP address of the cluster master.
Web Port of the cluster master	Enter the web port number of the cluster master. Value range is 1 ~ 65535.

2. Click on Modify.

6.18 Configuration / DHCP / DHCP (PPPoE) Config

Use the Configuration/DHCP/DHCP (PPPoE) Config screen to configure the DHCP option 82 and PPPoE relay function.

Configuration / DHCP / DHCP (PPPoE) Config

Previous Command Result: Normal

Modify

DHCP Mode	Transparent
Option	Agent Circuit ID
Circuit ID Type	Default
DSL Name	IPDSLAM
DHCP Forwarding Method	Secured Forwarding Mode
System-Wide	DEFVAL

To modify the system’s DHCP (PPPoE) configuration:

1. Enter or select the following fields:

Field	Description
DHCP Mode	Select the DHCP mode you want the DSLAM to act. Options are DHCP Transparent, DHCP Relay, and DHCP Server. Default mode is Transparent.
Option	Select the Relay Agent Information that is inserted to the forwarding packets. Options are: Agent Circuit ID, Agent Remote ID, or Both. Default is Agent Circuit ID.
Circuit ID Type	Select the type of Circuit ID. Options are: Default, SCBV, SCV, SC, and Customize. Default means our system-defined default type; Customize means the customer-defined type.
DSL Name	Type in the name of the DSLAM. Default is IPDSLAM.
DHCP Forwarding Method	Select DHCP forwarding method. This setting only takes effect when DHCP Mode is set to “Relay”. <b>Secured Forwarding Mode</b> (default mode) being selected, the system forwards downstream DHCP frames according to Option-82 content carried in each DHCP frame and discards DHCP frames without Option-82 tags in downstream direction. <b>Normal Forwarding Mode</b> being selected, the system forwards downstream DHCP frames according to MAC

	bridging mechanism regardless of Option-82 tagged/untagged or Option-82 content carried in each DHCP frame.
System-Wide	Select a DHCP Server Profile to be the system-wide profile. Default system-wide DHCP Server Profile is DEFVAL.

2. Click on Modify.

6.19 Configuration / DHCP / DHCP (PPPoE) Port

Use the Configuration/DHCP/DHCP (PPPoE) Port screen to configure DCHP (PPPoE) port including specifying the agent circuit ID and remote ID for the relay function.

Configuration / DHCP / DHCP (PPPoE) Port

Previous Command Result: Normal

Select page: 

page-1

☐ Check All ☐ Uncheck All

Modify

	Physical Port	Agent Circuit ID	Agent Remote ID	Trusted	PPPoE Mode
<input type="checkbox"/>	Port-2 -- PVC-1	IPDSLAM:1:002:005	IPDSLAM:1:002:005	FALSE	Transparent
<input type="checkbox"/>	Port-1 -- PacketMode	IPDSLAM:1:001:196	IPDSLAM:1:001:196	FALSE	Transparent

To configure DHCP (PPPeE) port:

1.

Click on the *Query Page Number* drop-down list and select the page to be displayed (if one page is not enough to display all entries).
2.

Click in the selection box next to the bridge port you want to modify. You can click in the Check All selection box to select all bridge ports at a time (To cancel the selection, click in UnCheck All selection box).
3.

Enter or select the following fields:

Field	Description
Physical Port	Shows the physical port number (and ATM PVC number for ADSL mode).
Agent Circuit ID	Agent circuit ID information. Type in the Circuit ID when 'Customize' is selected for the Circuit ID Type (refer to Configuration/DHCP/DHCP(PPPoE) Configuration Screen).
Agent Remote ID	Agent remote ID information.
Trusted	Select Trusted configuration for the port. TRUE means the port is to be trusted; FALSE means to be untrusted (the relay agent will discard the DHCP packets from an untrusted circuit).
PPPoE Mode	Select PPPoE mode (Transparent or Relay).

4.

Click on Modify.

### 6.20 Configuration / DHCP / DHCP Clients List

Use the Configuration/DHCP/DHCP Clients List screen to view current DHCP clients list including the information of assigned IP addresses and associated MAC addresses, expired time, and lease time.

Configuration / DHCP / DHCP Clients List

Select page: 

page-1

Physical Port

Index

IP

MAC

Expired Time

Lease Time

Click on the *Query Page Number* drop-down list and select the page to be displayed (if one page is not enough to display all entries).

The list displayed contains the following information:

Field	Description
Physical Port	Shows the physical port number (and ATM PVC number for ADSL mode).
Index	Shows the DHCP client index.
IP	Shows the IP address of the DHCP client.
MAC	Shows the MAC address of the DHCP client.
Expired Time	Shows the DHCP expired time.
Lease Time	Shows the DHCP lease time (the remaining time).



### 6.21 Configuration / DHCP / DHCP Server Profile Config

Use the Configuration/DHCP/DHCP Server Profile Config screen to configure the DHCP server profile used when DSLAM is set to act as DHCP server.

Configuration / DHCP / DHCP Server Profile Config

Previous Command Result: Success

Related: DHCP (PPPoE) Config

Create New

Delete Selected

Delete All

	Index	Start IP	End IP	Netmask	Gateway	DNS1	DNS2	Lease Time
<input type="checkbox"/>	1	192.168.1.10	192.168.1.10	255.255.255.0	192.168.1.254	0.0.0.0	0.0.0.0	300
<input checked="" type="checkbox"/>	2	192.168.5.2	192.168.5.13	255.255.255.0	255.255.255.0	0.0.0.0	0.0.0.0	300

To create a DHCP Server Profile:

- 1. Click on Create New.
- 2. Enter the following fields:

Field	Description
Index	Shows the DHCP server profile index. Valid value is 2 ~ 25. Index 1 is the default DHCP server profile.
Start IP	Type in the Start IP of the IP address range.
End IP	Type in the End IP of the IP address range.
Netmask	Type in the network mask.
Gateway	Type in the IP address of the default gateway.
DNS1	Type in the IP address of the DNS server 1.
DNS2	Type in the IP address of the DNS server 2.
Lease Time	Type in the DHCP lease time (sec). Valid value is 300 ~ 86400.

- 3. Click on Create.

To delete a DHCP Server Profile:

- 1. Click in the selection boxes next to the profile index of the profiles you want to delete. Note that the system default profile (profile index 1) cannot be deleted.
- 2. Click on Delete Selected.
- 3. You can click on Delete All to delete all profiles at a time.

## 6.22 Configuration / DHCP / DHCP Server Profile Select

Use the Configuration/DHCP/DHCP Server Profile Select screen to specify a DHCP Server Profile for a bridge port.

Configuration / DHCP / DHCP Server Profi

Previous Command Result: Normal

Select page: 

page-1

☐ Check All ☐ Uncheck All

Modify

	Physical Port	Profile Select
<input type="checkbox"/>	Port-2--PVC-1	System-Wide
<input type="checkbox"/>	Port-1--VDSLMode	profile-2

To modify the specified DHCP server profile for a port:

1. Click in the selection box next to the bridge port you want to modify. You can click in the Check All selection box to select all bridge ports at a time (To cancel the selection, click in UnCheck All selection box).

Field	Description
Physical Port	Shows the physical port number (and ATM PVC number for ADSL mode).
Profile Select	Select a new DHCP server profile. Default setting is System-Wide; it means the DHCP server profile for this port is the profile setup in the System-Wide field of Configuration/DHCP/DHCP (PPPoE) Config screen.

2. Click on Modify.

6.23 Configuration / DHCP / DHCP Static IP Config

Use the Configuration/DHCP/DHCP Static IP Config screen to configure DHCP fixed IP and MAC for a bridge port.

Configuration / DHCP / DHCP Static IP Config

Previous Command Result: Normal

Create

Index	Physical Port	IP	MAC
2	Port-2 -- PVC-1	00.00.00.00	00:00:00:00:00:00

Select page: page-1 ☐ Check All ☐ Uncheck All

Delete

	Index	Physical Port	IP	MAC
<input type="checkbox"/>	1	Port-1 -- PacketMode	192.168.5.10	EF:00:11:00:00:03

To create a fixed IP and MAC for a bridge port:

1. Enter or select the following fields:

Field	Description
Physical Port	Select the bridge port you want to create the static IP for.
IP	Type in the static IP address. The address must be within the range configured in the DHCP Server Profile specified for the bridge port.
MAC	Type in the static MAC address.

2. Click on Create.

To delete a the static IP for a bridge port:

1. Click in the selection box next to the bridge port you want to delete. You can click in the Check All selection box to select all bridge ports at a time (To cancel the selection, click in UnCheck All selection box).
2. Click on Delete.

### 6.24 Configuration / Filtering / Access Control List (ACL)

Use the Configuration/DHCP/DHCP Static IP Config screen to configure the Access Control List (specify certain types of packets to be passed or rejected).

Configuration / Filtering / Access Control L

Previous Command Result: Normal

Select page: 

page-1

☒ Check All ☐ Uncheck All

Modify

	Physical Port	NetBIOS	ARP
<input checked="" type="checkbox"/>	Gigabit-1	Pass	Pass
<input checked="" type="checkbox"/>	Gigabit-2	Pass	Pass
<input checked="" type="checkbox"/>	Port-2--PVC-1	Pass	Pass
<input checked="" type="checkbox"/>	Port-1--VDSLMode	Pass	Pass

To modify Access Control List:

1. Click on the *Query Page* drop-down list and select the page to be displayed (if one page is not enough to display all entries).
2. Click in the selection box next to the bridge port you want to modify. You can click in the Check All selection box to select all bridge ports at a time (To cancel the selection, click in UnCheck All selection box).
3. Select the following fields:

Field	Description
NetBios	Select to Pass or Discard NetBios packets.
ARP	Select to Pass or Discard ARP packets.

4. Click on Modify.

### 6.25 Configuration / Filtering / Anti Arp Spoofing (per Port)

Use the Configuration/Filtering/Anti Arp Spoofing (per Port) screen to configure static mapping between IP address and MAC address on a per port basis for the system to determine the validity of an ARP packet. Up to 8 entries (static IP/MAC mappings) can be supported per port.

Configuration / Filtering / Anti Arp Spoofing (

Previous Command Result: Normal

Create

Index	Physical Port	IP	MAC
2	Port-2 -- PVC-1	00.00.00.00	FF:FF:FF:FF:FF:FF

Select page: page-1 ☐ Check All ☐ Uncheck All

ModifyDelete

	Index	Physical Port	IP	MAC
<input type="checkbox"/>	1	Port-2 -- PVC-1	192.168.7.15	FF:FF:FF:FF:FF:FF

**To create a mapping rule between IP and MAC:**

1. Enter or select the following fields:

Field	Description
Physical Port	Select the bridge port you want to create an IP-MAC mapping for.
IP	Enter the IP address.
MAC	Enter the MAC address.

2. Click on Create.

**To modify a mapping rule between IP and MAC:**

3. Click in the selection box next to the bridge port you want to modify. You can click in the Check All selection box to select all bridge ports at a time (To cancel the selection, click in UnCheck All selection box).
4. Modify the fields as required.
5. Click on Modify.

**To delete a mapping rule between IP and MAC:**

1. Click in the selection box next to the bridge port you want to delete. You can click in the Check All selection box to select all bridge ports at a time (To cancel the

selection, click in UnCheck All selection box).

2. Click on Delete.



6.26 Configuration / Filtering / Filter Rules

Use the Configuration/Filtering/Filter Rules screen to setup filter rules for packets.

Configuration / Filtering / Filter Rules

Previous Command Result: Success

Filtering Type Protocol

Create

Index	Physical Port	Protocol
3	Gigabit-1	UDP

Select page: page-1

☐ Check All

☐ Uncheck All

Delete

	Index	Physical Port	Protocol
<input type="checkbox"/>	1	Gigabit-1	17:UDP
<input type="checkbox"/>	2	Port-1--VDSLMode	6:TCP

To create a filter rule:

1. Click on Filtering Type drop-down list and select a filtering type. Available filtering types include: Protocol, Source MAC, Source IP, L4 Dest Port, Destination IP, L4 Src Port, and Destination MAC. For each filtering type, up to 200 filter rules can be created.
2. Select the bridge port you want to create the filter rule for.
3. Set the values for different parameters depending on the filtering type you choose.

Filtering Type	Field	Description
Protocol	Protocol	Click on this drop-down list and select a protocol: UDP, TCP, OSPF, IGMP, IGP, GRP, EIGRP, IP in IP, GRE, and ICMP. <i>Note:</i> the IGMP protocol filtering can only work when IGMP ACL mode is disabled (refer to Configuration/IGMP/ Configure IGMP screen).
Source MAC	Source MAC	Type in the MAC Address of the source.
Source IP	Source IP	Type in the MAC Address of the source.
	Source MAC	Type in the subnet mask of the source.
L4 Dest Port	Destination Port	Type in the Layer 4 Destination Port number (1 ~ 65535). <i>Note:</i> The L4 destination port number

		represents the name of the application that is to receive the data contained within the IP packet.
Destination IP	Destination IP	Type in the Destination IP address.
	Destination MASK	Type in the Destination subnet mask.
L4 Src Port	Source Port	Type in the Layer 4 Source Port number (1 ~ 65535). <i>Note:</i> The L4 source port number represents the name of the application that sent the data in the IP packet.
Destination MAC	Destination MAC	Type in the MAC address of the destination.

4. Click on Create.

**To delete a filter rule:**

1. Click in the selection box next to the bridge port you want to delete. You can click in the Check All selection box to select all bridge ports at a time (To cancel the selection, click in UnCheck All selection box).
2. Click on Delete.

6.27 Configuration / Filtering / IP Filtering

Use the Configuration/Filtering/IP Filtering screen to manually configure the system allowed IP list.

Configuration / Filtering / IP Filtering

Previous Command Result: Normal

Create New

Modify Selected

Delete Selected

Delete All

	Index	Physical Port	IP Filter Mode	Src IP
<input checked="" type="checkbox"/>	1	Port-2 -- PVC-1	Manual	192.168.7.22

5224AV-2GBE/2SFP supports 20 allowed IPs per bridge port, ten static (manually configured) and ten dynamic rules.

To create an allowed IP:

- Click on Create New. The IP Filtering - Create screen appears.
- Enter or select the following fields:

Field	Description
Index	This field shows the index of the created entry. Value range is 1 ~ 1920.
Physical Port	Select the bridge port you want to create the allowed source IP for. Users can create up to 10 allowed IP per port.
IP Filter Mode	Only Manual mode is supported.
Src IP	Type the allowed source IP address here.

- Click on Create.

To modify an allowed IP:

- Click in the selection box next to the entry index you want to modify.
- Click on Modify Selected.
- Enter the new source IP address.
- Click on Modify

To delete an allowed IP:

- Click in the selection box next to the entry index you want to delete.
- Click on Delete Selected.
- Your can click on Delete All to delete all entries at a time.

### 6.28 Configuration / Forwarding / Bridge

Use the Configuration/Forwarding/Bridge screen to set the aging time of MAC learning per system.

Configuration / Forwarding / Bridge

Previous Command Result: Normal

Modify

Aging Time(Sec)

300

To modify the aging time of MAC learning:

1. Enter the following field:

Field	Description
Aging Time	Type in the aging time in seconds. An entry will be removed from the FDB (aged-out) if the device does not transmit for a specified period of time (the aging time). Value range: 10 ~ 1M (sec), default is 300 (sec).

2. Click on Modify.

6.29 Configuration / Forwarding / Bridge Table - Static

Use the Configuration/Forwarding/Bridge Table - Static screen to configure the static MAC address forwarding entries on a specific bridge port.

Configuration / Forwarding / Bridge Table - S

Previous Command Result: Normal

Create

Index	Physical Port	MAC	VID	Process
2	GigaBit-1	00:00:00:00:00:00	1	Deny

Select page: page-1 ☐ Check All ☐ Uncheck All

Delete

	Index	Physical Port	MAC	VID	Process
<input type="checkbox"/>	1	GigaBit-1	12:00:00:ef:00:00	1	Deny

To create a static MAC:

1. Enter or select the following fields:

Field	Description
Index	This field shows the index of the created static MAC.
Physical Port	Select the output bridge port.
MAC	Type in the MAC address for the static entry.
VID	Type in the VID for the static entry (1 ~ 4094).
Process	Click on the drop-down list and select "Deny" or "Pass". "Pass" means to forward the packets with destination MAC address matching one of the static forwarding MAC addresses to a specified output bridge port. "Deny" means to drop the packets.

2. Click on Create.

To delete a static MAC:

1. Click in the selection box next to the bridge port you want to delete. You can click in the Check All selection box to select all bridge ports at a time (To cancel the selection, click in UnCheck All selection box).
2. Click on Delete.

### 6.30 Configuration / Forwarding / Fdb Delete Control

Use the Configuration/Forwarding/Fdb Delete Control screen to manually delete MAC forwarding entries that are dynamically learned.

Configuration / Forwarding / Fdb Delete C

Previous Command Result: Normal

Modify

FDB Delete Control Type	All
Control Port	Gigabit-1
Control VLAN	1
Control MAC	FF:FF:FF:FF:FF:FF

To delete dynamically learned MAC forwarding entries:

1. Enter or select the following fields:

Field	Description
FDB Delete Control Type	Select the type to specify entries to be deleted. Options are: All: delete all entries PORT: delete entries per specific bridge port VLAN: delete entries belonging to a specific VLAN MAC: delete entry of a specific MAC address
Control Port	Select a bridge port if PORT is selected for FDB Delete Control Type
Control VLAN	Enter a VLAN ID if VLAN is selected for FDB Delete Control Type
Control MAC	Enter a MAC address if MAC is selected for FDB Delete Control Type

2. Click on Modify.



### 6.31 Configuration / Forwarding / Secure Forwarding

Use the Configuration/Forwarding/Secure Forwarding screen to configure the Secured Forwarding function, which means traffic directly forwarding between two DSLAMs is not allowed. The forwarding among DSLAMs must be forwarded through the gateway. The 5224AV-2GBE/2SFP supports secured forwarding (forced forwarding) that forces upstream traffic to the specific gateway by means of replying upstream ARP request with MAC address of default gateway.

Configuration / Forwarding / Secure Forwa

Previous Command Result: Normal

Submit

Secured Forwarding

Disable

Default Gateway MAC

FF:FF:FF:FF:FF:FF

Select page:

page-1

☐ Check All

☐ Uncheck All

Modify

	Physical Port	Learn By DHCP	Default Gateway MAC
<input type="checkbox"/>	Port-2 -- PVC-1	Preconfigured	FF:FF:FF:FF:FF:FF
<input type="checkbox"/>	Port-1 -- PacketMode	Preconfigured	FF:FF:FF:FF:FF:FF

To enable/disable Secure Forwarding function and setup default gateway:

1. Enter or select the following fields:

Field	Description
Secure Forwarding	Select to enable/disable Secured Forwarding.
Default Gateway MAC	Type in the MAC address of the default forwarding gateway.

2. Click on Submit.

To modify secure forwarding configuration for a bridge port:

1. Enter or select the following fields:

Field	Description
Physical Port	Shows the line physical port number (and ATM PVC number for ADSL mode).
Learn By DHCP	Click on the drop-down list and select the way of setting

	default gateway MAC address: <b>Preconfigured:</b> manual configuration <b>LearnByDHCP:</b> learned from DHCP snooping
Default Gateway MAC	Type in the MAC address of the default forwarding gateway.

2. Click on Modify.

6.32 Configuration / IGMP / Configure IGMP

Use the Configuration/IGMP/Configure IGMP screen to configure the IGMP Snooping and IGMP Proxy features for IP Multicast.

Select a tab (IGMP Config or IGMP Route) on top of the screen first.

IGMP Config:

IGMP Config

IGMP Route

Previous Command Result: Normal

Modify

IGMP Version	IGMP V2
IGMP Mode	Normal Snooping
IGMP ACL Mode	Disable
IGMP Leave Mode	Normal Leave
IGMP Message Priority	Reserved
IGMP ACL System_wide	DEFVAL
Timeout Parameters	Value Range 1~500(sec)
Query (Query Interval)	125
URI (Unsolicited Report Interval)	1
BC (Older Host Present Interval)	400
MRT(Max Response Time)	10
LMQT(Last Member Query Time)	1
GMT (Group Membership Timeout)	260

The Query and MRT times are configured as follows : Query Interval > Max R

To configure IGMP parameters:

1. Enter or select the following fields:

Field	Description
IGMP Version	Select the IGMP version. Options are: IGMP OFF, IGMP V1, IGMP V2, and IGMP V3.
IGMP Mode	Select the IGMP mode. Options are: Normal Snooping and Proxy Snooping.
IGMP ACL Mode	Disable or enable ACL mode. IGMP ACL profiles will be

	referred to only when ACL mode is enabled.
IGMP Leave Mode	Select the mode of leaving a multicast group. Options are: Normal Leave and Fast Leave.
IGMP Message Priority	Select the processes for user priority. 0 ~ 7: The DSLAM overwrites the priority with the value set here when frames including IGMP messages are sent. Reserved: The DSLAM keeps priority value of received frames including IGMP messages when sending.
IGMP ACL System_wide	Select a profile to be the system-wide IGMP ACL profile, which is to bind with all bridge ports whose IGMP ACL profile select is set to "system-wide" (refer to Configuration/IGMP/IGMP ACL Profile Select screen). With this configuration, all ports can be set to a common set of multicast VLAN translations and multicast groups allowed. The default system-wide IGMP ACL profile is the IGMP ACL default profile DEFVAL, which does not allow any multicast group and does not have any multicast translation.
Query (Query Interval)	The interval between General Queries sent by the Querier. By varying this value, an administrator may tune the number of IGMP messages on the network; larger values cause IGMP Queries to be sent less often. Value range is 1 ~ 500 (s). Default is 125 seconds.
URI (Unsolicited Report Interval)	The time between repetitions of a host's initial report of membership in a group. Value range is 1 ~ 500 (s). Default: 1 second.
BC (Older Host Present Interval)	This interval represents how long a host must wait after hearing a Version 1 Query before it may send any IGMPv2 messages. Value range is 1 ~ 500 (s). Default is 400 (sec).
MRT (Max Response Time)	The burstiness of IGMP traffic is inversely proportional to the Max Response Time. A longer Max Response Time will spread Report messages over a longer interval. However, a longer Max Response Time in Group-Specific and Source-and-Group-Specific Queries extends the leave latency. (The leave latency is the time between when the last member stops listening to a source or group and when the traffic stops flowing.). Value range is 1 ~ 500 (s). Default is 10.
LMQT (Last Member Query Time)	This interval is the Max Response Time used to calculate the Max Resp Code inserted into Group-Specific Queries sent in response to Leave Group messages. It is also the Max Response Time used in calculating the Max Resp Code for Group-and-Source-Specific Query messages. Value range is 1 ~ 500 (s). Default is 1.
GMT (Group Membership Timeout)	Read-only value. The GMT is the amount of time that must pass before a multicast router decides there are no more members of a group or a particular source on a network.

	This value MUST be ((the Robustness Variable) times (the Query Interval)) plus (one Query Response Interval).
--	---------------------------------------------------------------------------------------------------------------

2. Click on Modify.

IGMP Route:

IGMP Config

IGMP Route

Previous Command Result: Success

Add

Physical Port	VLAN ID	Multicast Stream Priority	Router IP	Report IP
GigaBit-1	1	Reserved	00.00.00.00	00.00.00.00

☐ Check All ☐ Uncheck All

Delete

	Physical Port	VLAN ID	Multicast Stream Priority	Router IP	Report IP
<input type="checkbox"/>	GigaBit-1	1	Reserved	192.168.5.101	0.0.0.0

To specify the interface through which IGMP packets are forwarded:

1. Enter or select the following fields:

Field	Description
Physical Port	Select a physical port to be the IGMP router port. Options are: GigaBit-1, GigaBit-2, or LACP-3.
VLAN ID	Select the VLAN ID you want to add the IGMP route for.
Multicast Stream Priority	Set this priority value (0 ~ 7) or keep the original priority (Reserved) in IGMP multicast streams.
Router IP	When working in IGMP proxy mode, DSLAM will send IGMP general query whose source IP address is 0.0.0.0. But PCs with Windows OS do not receive this kind of packets. So user can assign an IP address here for proxy mode IGMP general query packet reference.
Report IP	Type in source IP address in IGMP report packet when working in proxy mode.

2. Click on Add.

To delete an IGMP route:

1. Click in the selection box next to the IGMP route you want to delete. You can click in the Check All selection box to select all routes at a time (To cancel the selection, click in UnCheck All selection box).

2. Click on Delete.



6.33 Configuration / IGMP / IGMP ACL Profiles

Use the Configuration/IGMP/IGMP ACL Profiles screen to configure IGMP ACL Profiles. The profiles define the IGMP multicast channels, which are allowed to join for each VDSL port. That is, a multicast stream will be copied to a VDSL port only if that multicast stream is registered in the ACL profile that is bound to this VDSL port. The maximum number of IGMP multicast channels in an ACL profile is 512 (64 x 8 banks). The 5224AV-2GBE/2SFP supports 24 configurable IGMP ACL profiles plus one default profile for bridge port binding. Note that the same multicast channel can be existed concurrently in two or more ACL profiles.

The ACL profile will be referred to only when IGMP ACL mode is enabled in the IGMP Config page. When ACL mode is disabled, all the bridge ports can freely join any multicast channel without limitation.

Configuration / IGMP / IGMP ACL Profiles

Previous Command Result: Normal

Related: [IGMP Stats](#) [Services](#)

Query Profile Selection: 

profile-2

bank 1(1~64)

Profile Index: 2

Max Channel Count: 

10

Max IGMP Message Count: 

128

Create

Delete

Modify

Quickly Assign

Start IP Address

End IP Address

SVID

Tag

UVID

☐ Select All

Assign

Channel	Start IP Address	End IP Address	SVID	Tag	UVID
<input type="checkbox"/> 1	224 . 0 . 0 . 0	224 . 0 . 0 . 1	1	<input checked="" type="checkbox"/>	1
<input type="checkbox"/> 2	224 . 0 . 0 . 2	224 . 0 . 0 . 3	1	<input checked="" type="checkbox"/>	1
<input type="checkbox"/> 3	224 . 0 . 0 . 4	224 . 0 . 0 . 5	1	<input checked="" type="checkbox"/>	1

To create an IGMP ACL profile:

1. Click on *Query Profile Selection* drop-down list and select CREATE\_NEW.

2. Enter the following fields:

Field	Description
Profile Index	Shows the index of the created IGMP ACL profile.
Max Channel Count	Type in the maximum allowed number of concurrently active channels. Valid value is 0 ~ 20.
Max IGMP Message Count	Set the maximum number of IGMP messages per second that are allowed to pass through the port (0 ~ 65535, default 128).

3. Click on Create.

143

DATA CONNECT ENTERPRISE

3405 OLANDWOOD COURT

OLNEY, MD 20832

O: 301.924.7400 EXT. 17

F: 301.924.7403

[www.dataconnectus.com](http://www.dataconnectus.com)

To modify an IGMP ACL profile:

1.

Click on *Query Profile Selection* drop-down list and select the profile you want to modify. Note that the system default profile DEFVAL cannot be modified.
2.

Select the bank you want to modify.
3.

Modify the fields as required. To quickly assign values to multiple channels that have the similar settings:

(a)

Click in the selection box next to the channels you want to assign values to, or you can click in the All Select checkbox to select all channels at a time.

(b)

Enter or select the following fields as required:

Field	Description
Quickly IP Assign	Type in the portion of IGMP group address that is applied to each channel. Valid value for an IGMP group address is between 224.0.0.0 and 239.255.255.255. The range of addresses from 224.0.0.0 to 224.0.0.255 is reserved for the use of routing protocols and other low-level topology discovery or maintenance protocols.
Quickly Start IP	IGMP group IP is a range of IP address, this parameter is the start of the range. Type the IGMP group IP address here for quick assignment. Click on Assign button to put the value into the table. Then you can modify parts of the IP addresses directly in the table.
Quickly End IP	IGMP group IP is a range of IP address, this parameter is the end of the range. Type the IGMP group IP address here for quick assignment. Click on Assign button to put the value into the table. Then you can modify parts of the IP addresses directly in the table.
Quickly SVID Assign	Type in the VLAN ID that the video server is within. Valid value is 1 ~ 4094. 0: leaving the field ignored.
Quickly UVID Assign	Type in the VLAN ID that the video user (subscriber) is within. Valid value is 1 ~ 4094. 0: leaving the field ignored.
Quickly Tag Assign	This checkbox is for selecting VLAN tagged/un-tagged option of the downstream-multicast packets.
Start IP Address (End IP Address)	<div>You can type the IGMP group address here and then click on Create button to save. Valid values: 224.0.0.0 ~ 239.255.255.255. The range of addresses from 224.0.0.0 to 224.0.0.255 is reserved for the use of routing protocols and other low-level topology discovery or maintenance protocols.</div> <div>Note: the range between start/end should NOT exceed 255 entries.</div> <div>Example:</div>

	224.0.0.1 ~ 224.0.0.255	→ allowed
	224.0.0.1 ~ 224.0.1.1	→ NOT allowed

- (c) Click on Assign.
- (d) Continue to enter values for the fields in which these channels have different settings.
4. Click on Modify.

**To delete an IGMP ACL profile:**

1. Click on *Query Profile Selection* drop-down list and select the profile you want to delete. Note that the system default profile DEFVAL cannot be deleted.
2. Click on Delete.

### 6.34 Configuration / IGMP / IGMP ACL Profile Select

Use the Configuration/IGMP/IGMP ACL Profile Select screen to bind an IGMP ACL profile to a bridge port.

Configuration / IGMP / IGMP ACL Profile Select

Previous Command Result: Normal

Select page: 

page-1

☐ Check All ☐ Uncheck All

Modify

	Physical Port	ACL Index	Modify
<input type="checkbox"/>	Port-2 -- PVC-1	System-wide	System-wide
<input type="checkbox"/>	Port-1 -- PacketMode	System-wide	System-wide

**To select an IGMP ACL profile for a bridge port:**

1. Click in the selection box next to the bridge port you want to modify the selection for. You can click in the Check All selection box to select all ports at a time (To cancel the selection, click in UnCheck All selection box).
2. Select the ACL profile you want to bind in 'Modify' field. Note that if you select "System-wide", the port will automatically bind to the ACL profile specified in 'IGMP ACL System\_wide' field of Configuration/IGMP/Configure IGMP screen.
3. Click on Modify.

### 6.35 Configuration / Management / Mgmt Link Config

Use the Configuration/Management/Mgmt Link Config screen to configure the address and default gateway for the Management Inband and Out of band interfaces.

Configuration / Management / Mgmt Link

Previous Command Result: Normal

Modify

Gigabit Ethernet Configuration & Status

	Config Status	Admin Status	Op Status	Determine First
GBE1	(1)Auto Negotiate	Enable	Down	SFP first
GBE2	(1)Auto Negotiate	Enable	Down	SFP first

MGMT Speed

Remote IP Address

HTTP Port

AutoNegotiate

192.168.7.29

80


Address Management

GBE (In Band)		MGMT (Out Band)	
IP Address	192 . 168 . 5 . 3	IP Address	172 . 16 . 10 . 106
Subnet Mask	255 . 255 . 255 . 0	Subnet Mask	255 . 255 . 0 . 0
MAC	00:FF:59:06:64:D8	Gateway	172 . 16 . 10 . 254
Inband VID	0		
Priority	0		

Route Table

Add

Delete

	Destination	NetMask	Gateway
	0 . 0 . 0 . 0	0 . 0 . 0 . 0	0 . 0 . 0 . 0

#### Gigabit Interface Setup:

1. Enter or select the following fields:

Field	Description
Gigabit Ethernet Configuration & Status	

147

DATA CONNECT ENTERPRISE

3405 OLANDWOOD COURT

OLNEY, MD 20832

O: 301.924.7400 EXT. 17

F: 301.924.7403

www.dataconnectus.com

Config Status		Click on the drop-down list and select the speed mode of the Gigabit interfaces. Available options are: Auto Negotiate, 10Mbps Half duplex, 10Mbps Full duplex, 100Mbps Half duplex, 100Mbps Full duplex, 1000Mbps.
Admin Status		Click on the drop-down list and select the administrative state (Enable/Disable) for the Gigabit interfaces.
Op Status		This field shows the operational state of the Gigabit interfaces.
Determine First		Click on the drop-down list and select the cable mode for Gigabit interfaces. Options are: SFP First: when both optical and electrical uplinks are connected, optical interface is chosen to transport data. Copper First: when both optical and electrical uplinks
MGMT Speed		Shows current speed / mode of the MGMT port.
Remote IP Address		Shows the IP address of the management PC currently connected to this DLSAM.
HTTP Port		Shows current HTTP port setting for Web access. You can modify http port setting in this field.
Address Management		
GBE (In Band)	IP Address	Type in the in-band IP address of the DSLAM.
	Subnet Mask	Type in the in-band subnet mask of the DSLAM.
	MAC	This field shows the MAC address of the DSLAM.
	Inband VID	The VLAN ID for individual in-band management
	Priority	Type in the VLAN priority level (0 ~ 7) of the in-band
MGMT (Out Band)	IP Address	Type in the out-band IP address of the DSLAM.
	Subnet Mask	Type in the out-band subnet mask of the DSLAM.
	Gateway	Type in the out-band IP address of the gateway.

2. Click on Modify.

Route Table:

Route Table			
Add		Delete	
	Destination	NetMask	Gateway
<input checked="" type="radio"/>	0 . 0 . 0 . 0	0 . 0 . 0 . 0	0 . 0 . 0 . 0
<input type="radio"/>	192.168.5.0	255.255.255.0	172.16.10.73

To create an IP route:

1. Enter the following fields:



Field	Description
Destination	Type in the destination IP address for the new IP route.
Net Mask	Type in the subnet mask for the new IP route.
Gateway	Type in the IP address of the gateway for the new IP route.

2. Click on Add.

To delete an IP route:

1. Click in the radio button next to the route you want to delete.
2. Click on Delete.

6.36 Configuration / Management / SNMP

Use the Configuration/Management/SNMP screen to configure the SNMP (Simple Network Management Protocol) agent in the system.

Select a tab (Community, Notify, or Traps) on top of the screen first.

Community:

Community

Notify

Traps

Previous Command Result: Normal

Create

Index	Community Name	Access Mode
2	SnmpCommunityName2	read-only

Select page: page-1

☐ Check All

☐ Uncheck All

ModifyDelete

	Index	Community Name	Access Mode
<input type="checkbox"/>	1	public	read-write

This page allows you to configure the SNMP community that is the group the 5224AV-2GBE/2SFP and management stations running SNMP belong to. It helps define where information is sent. The community name is used to identify the group and serve as form of authentication.

To create a SNMP community:

1. Enter or select the following fields:

Field	Description
Community Name	Type in the community name (1 ~ 31 characters).
Access Mode	Click on the drop-down list and select the access mode of this SNMP community. Options are: read-only, or read-write.

2. Click on Create.

To modify a SNMP community:

1. Click in the selection box next to the SNMP community index you want to modify. You can click in the Check All selection box to select all communities at a time (To cancel the selection, click in UnCheck All selection box).
2. Modify the fields as required.

3. Click on Modify.

To delete a SNMP community:

1. Click in the selection box next to the SNMP community index you want to delete.  
You can click in the Check All selection box to select all communities at a time (To cancel the selection, click in UnCheck All selection box). Note that the system default SNMP community cannot be deleted.
2. Click on Delete.

Notify:

Community

Notify

Traps

Previous Command Result: Normal

Create

Index	Notify Name	Notify Tag
3	SnmpNotifyName3	SnmpNotifyTag3

Select page: page-1

☐ Check All

☐ Uncheck All

Modify

Delete

	Index	Notify Name	Notify Tag
<input type="checkbox"/>	1	SnmpNotifyName1	DDT
<input type="checkbox"/>	2	SnmpNotifyName2	CS-1

This page allows you to configure the SNMP Notification (In SNMPv1, asynchronous event reports are called traps while they are called notifications in later versions of SNMP).

To create a SNMP Trap Setup:

1. Enter or select the following fields:

Field	Description
Notify Name	Type in the name of the SNMP Notify (1 ~ 31 characters). Once a Notify entry is created in the table, the Notify Name cannot be modified (you can only delete the entry).
Notify Tag	Type in the Notify Tag (1 ~ 31 characters). The SNMP notification with the Notify Tag is sent to the Target that has the same tag.

2. Click on Create.

To modify a SNMP Trap setup:

1. Click in the selection box next to the SNMP Trap setup index you want to modify.

You can click in the Check All selection box to select all traps at a time (To cancel the selection, click in UnCheck All selection box).

2. Modify the Notify Tag as required.
3. Click on Modify.

To delete a SNMP Trap setup:

1. Click in the selection box next to the SNMP Trap setup index you want to delete.  
You can click in the Check All selection box to select all traps at a time (To cancel the selection, click in UnCheck All selection box).
2. Click on Delete.

Traps:

This page allows you to configure the SNMP target to control where the SNMP traps (notifications) are sent. Traps are used to report an alarm or other asynchronous event about a managed 5224AV-2GBE/2SFP system.

Community

Notify

Traps

Previous Command Result: Success

Create

Index	IP	Target Name	Notify Tag	Address Port	Trap Version
2	00.00.00.00	SnmpTargetName2	DDT	162	V1

Select page: page-1

☐ Check All

☐ Uncheck All

ModifyDelete

	Index	IP	Target Name	Notify Tag	Address Port	Trap Version	New Notify Tag
<input type="checkbox"/>	1	192.168.9.60	SnmpTargetName1	DDT	162	V1	DDT

To create a SNMP Target:

1. Enter or select the following fields:

Field	Description
IP	Type in the IP address where the SNMP trap (notification) is sent.
Target Name	Type in the name of the SNMP target (1 ~ 31 characters).
Notify Tag	Select the Notify Tag, which is configured in the 'Traps' page. The SNMP notification with a Notify Tag is sent to the Target that has the same tag.
Address Port	Type in the Address Port (usually SNMP uses UDP port 161 for general SNMP messages and UDP port 162 for SNMP trap messages).
Trap Version	Select the SNMP Trap version. Currently V1 and V2c are supported.

2. Click on Create.

To modify a SNMP Target:

1. Click in the selection box next to the SNMP target index you want to modify. You can click in the Check All selection box to select all Targets at a time (To cancel the selection, click in UnCheck All selection box).
2. Modify the fields as required.
3. Click on Modify.

To delete a SNMP Target:

1. Click in the selection box next to the SNMP target index you want to delete. You can click in the Check All selection box to select all Targets at a time (To cancel the selection, click in UnCheck All selection box).
2. Click on Delete.

6.37 Configuration / Management / SNTP

Use the Configuration/Management/SNTP screen to establish the address of a Simple Network Time Protocol (SNTP) server. The server is queried to establish the system date and time at startup and to update them at specified intervals.

Configuration / Management / SNTP

Previous Command Result: Normal

Modify

Select Time Zone: GMT +00:00 Greenwich Mean Time

Time Zone	GMT
System Date	04 / 13 / 2010
System Time	19 : 42 : 28
Polling Interval	0
SNTP Server Address	0 . 0 . 0 . 0

To set the SNTP server parameters:

1. Enter or select the following fields:

Field	Description
Select Time Zone	Sets the local time zone by selecting in the Time Zone drop-down list. Sixty-six of the world’s time zones are presented (including those using standard time and summer/daylight savings time).
System Date	Sets system date (mm/dd/yyyy).
System Time	Sets system time (hh:mm:ss).
Polling Interval	Sets the polling interval (in seconds) that SNTP client will sync with a designated SNTP server.
SNTP Server address	Sets the dedicated unicast server IP address for which the SNTP client can synchronize its time.

2. Click on Modify.



6.38 Configuration / Management / Syslog

Use the Configuration/Management/Syslog screen to configure the IP address of the SYS Log server which listens for incoming Syslog messages.

Configuration / Management / Syslog

Previous Command Result: Normal

Action: 

Stop

Modify

Current Server IP	192.168.1.1
Change Server Address	192 . 168 . 1 . 1
Log Size	<div>16</div> KBytes

5224AV-2GBE/2SFP supports UNIX syslog functionality per RFC 3164. The syslog messages are sent via UDP and the source port number is 1027. All events/alarms defined in Appendix Table A-1 and Table B-1 will trigger the system sending syslog messages to the provisioned syslog server. The syslog message format is as follows:

For events:

<timestamp> <process name>: Event: <event description>: <position>

Example: Apr 1 08:25:31 oamp: Event: XDSL Port Link Up: XDSL-PHY/1

For alarms:

<timestamp> <process name>: Alarm Set: <alarm description>: <position>

or

<timestamp> <process name>: Alarm Clear: <alarm description>: <position>

Example: Apr 1 08:24:36 oamp: Alarm Clear: Gigabit Ethernet Loss of Signal: GBE 1

To configure the Syslog parameters:

1. Enter or select the following fields:

Field	Description
Action	Click on this drop-down list and select <b>Start</b> to start sending the Syslog messages to the server or <b>Stop</b> to stop sending the Syslog messages to the server.
Current Server IP	This field shows the IP address of current Sys Log server.
Change Server Address	Type in the new IP address of Sys Log server. The server must be a remote host.
Log Size	Type in the maximum size of the log file for SysLog (16 ~ 1024 Kbytes).

2. Click on Modify.

6.39 Configuration / STP / STP Bridge

Use the Configuration/STP/STP Bridge screen to setup the STP Bridge.

Configuration / STP / STP Bridge

Previous Command Result: Normal

Modify

STP

Disabled ☒

Enabled ☐

Version

RSTP ☒

STP ☐

Priority

61440

MaxAge

20

HelloTime

2

ForwardDelay

15

Current Status

[STP:Disabled]

The MaxAge, HelloTime and ForwardDelay times are constrained as follows:

2 x (ForwardDelay - 1) >= MaxAge >= 2 x (HelloTime + 1)

1. Enter or select the following fields:

Field	Description
STP: Disable / Enable	Specify whether or not the system is to implement the spanning tree protocol.
Version	Select RSTP (IEEE 802.1W), STP (IEEE 802.1D), or MSTP (IEEE 802.1Q).
Priority	Sets the spanning tree protocol priority. The lower the priority number, the more significant the bridge becomes in protocol terms. Where two bridges have the same priority, their MAC address is compared and the smaller MAC address is treated as the most significant. The priority can be any value between 0 and 61440 in step of 4096. Default value is 61440.

MaxAge	<p>Sets the maximum age of received spanning tree protocol information before it is discarded. This is used when the bridge is or is attempting to become the root bridge.</p> <p>This can be any value (in seconds) between 6 and 40. BUT it is constrained by the hellotime and forwarddelay times.</p> <p>Default value is 20.</p>
Hello Time	<p>Sets the time after which the spanning tree process sends notification of topology changes to the root bridge. This is used when the bridge is or is attempting to become the root bridge.</p> <p>This can be any value (in seconds) between 1 and 10. BUT it is constrained by the maximum age and forwarddelay times.</p> <p>Default value is 2.</p>
Forward Delay	<p>Sets the time that the bridge spends in listening or learning states when the bridge is or is attempting to become the root bridge. This can be any value (in seconds) between 4 and 30. BUT it is constrained by the maxage and hellotimes.</p> <p>The maxage, hellotime and forwarddelay times are constrained as follows:</p> <p><math>2 \times (\text{forwarddelay} - 1) \geq \text{maxage}</math></p> <p><math>\text{maxage} \geq 2 \times (\text{hellotime} + 1)</math></p> <p>For example, the default settings are:</p> <p><math>2 \times (15 - 1) \geq 20</math></p> <p><math>20 \geq 2 \times (2 + 1)</math></p>
Current Status	<p>Shows current system STP setting and status.</p>

2. Click on Modify.

6.40 Configuration / STP / STP Port

Use the Configuration/STP/STP Port screen to setup the STP ports.

Configuration / STP / STP Port

Previous Command Result: Normal

Related: STP Bridge

☐ Check All ☐ Uncheck All

Modify

	Physical Port	Priority	Edge	P2P	State	STP Port	Path Cost	Designated				Forward Transitions
								Root	Cost	Bridge	Port	
<input type="checkbox"/>	Gigabit-1	128	True	Auto	DISABLED	Enabled	100	F00000FF590664D8	0	F00000FF590664D8	8001	4
<input type="checkbox"/>	Gigabit-2	128	True	Auto	DISABLED	Enabled	100	F00000FF590664D8	0	F00000FF590664D8	8002	4
<input type="checkbox"/>	Port-1--VDSLMode	128	True	Auto	DISABLED	Enabled	100	F00000FF590664D8	0	F00000FF590664D8	80C4	4

1. Click in the selection box next to the bridge port you want to modify. You can click in the Check All selection box to select all bridge ports at a time (To cancel the selection, click in UnCheck All selection box).

Field	Description
Physical Port	Lists the physical ports.
P2P	Indicates the point-to-point status of the LAN segment attached to this port.
State	Shows the port's current state as defined by application of the Spanning Tree Protocol. This state controls what action a port takes on reception of a frame. If the bridge has detected a port that is malfunctioning it will place that port into the Broken state. Valid States are: Disabled, Blocking, Listening, Learning, Forwarding, Broken.
Designated Root	Shows the unique Bridge Identifier of the Bridge recorded as the Root in the Configuration BPDUs transmitted by the Designated Bridge for the segment to which the port is attached.
Designated Cost	Shows the path cost of the Designated Port of the segment connected to this port. This value is compared to the Root Path Cost field in received bridge PDUs.
Designated Bridge	Shows the Bridge Identifier of the bridge, which this port considers to be the Designated Bridge for this port's segment.
Designated Port	Shows the Port Identifier of the port on the Designated Bridge for this port's segment.
Forward Transactions	Shows the number of times this port has transitioned from the Learning state to the Forwarding state.

2. Enter or select the following fields:

Field	Description
-------	-------------

Priority	Type in the priority level of the port (0 ~ 240 in step of 16).
Edge	Click on drop-down list and select Edge-True or Edge-False. True indicates that this port must be treated as an edge port; False indicates that this port should be treated as a non-edge port.
STP Port	Select Disabled or Enabled. (This configuration is currently disabled.). The enabled/disabled status of the port.
Path Cost	Type in the Path Cost through the port (integer number). The contribution of this port to the path cost of paths towards the spanning tree root, which include this port. 802.1D-1990 recommends that the default value of this parameter be in inverse proportion to the speed of the attached LAN.

3. Click on Modify.

### 6.41 Configuration / Traffic Prioritization / ADSL Traffic Desc Select

Use the Configuration/Traffic Prioritization/ADSL Traffic Desc Select screen to bind Traffic Descriptor profile to an ADSL bridge port.

Configuration / Traffic Prioritization / ADSL T

Previous Command Result: Normal

Select page: page-1

☐ Check All

☐ Uncheck All

Modify

	Physical Port	VPI	VCI	Traffic Descriptor
<input type="checkbox"/>	Port-2 -- PVC-1	0	35	1

1. Click in the selection box next to the bridge port you want to modify the setting for. You can click in the Check All selection box to select all ports at a time (To cancel the selection, click in UnCheck All selection box).

2. Enter or select the following fields:

Field	Description
VPI	Type in the VPI value: 0 ~ 255. Default value is 0.
VCI	Type in the VCI value: 21, 32 ~ 65535. Default value is 35.
Traffic Descriptor	Select the desired Traffic Descriptor profile.

3. Click on Modify.



## 6.42 Configuration / Traffic Prioritization / Traffic Desc Profile

Use the Configuration/Traffic Prioritization/Traffic Desc Profile screen to configure Traffic Descriptor profiles.

Configuration / Traffic Prioritization / Traffic Desc Profile

Previous Command Result: SuccessRelated: Select

Create New

Table View

Delete Selected

Delete All

	Profile Index	Ether Type Descriptor	ADSL Traffic Policer Type
<input checked="" type="checkbox"/>	1	WFQ	CBR
<input type="checkbox"/>	2	PPR	CBR
<input type="checkbox"/>	3	WFQ	CBR
<input type="checkbox"/>	4	CIREIR	CBR

To create a Traffic Desc Profile:

1. Click on Create New. The Traffic Desc Profile – Create screen appears.

Create

Profile Index

5

Descriptor Type

VDSL Descriptor

Ether Type Descriptor

WFQ

Weight

1

2. Enter or select the following fields:

Field	Description
Descriptor Type	Select VDSL Descriptor or ADSL Descriptor.
<b>VDSL Descriptor</b>	
Ether Type Descriptor	Click on this drop-down list and select a descriptor type. After you select a descriptor type, the configurable parameters will be displayed on the page. Available descriptor types are: WFQ (weighted fair queuing), PPR (peak packet rate), CIR (committed information rate), CIREIR.
Weight	This parameter is for descriptor type: WFQ. Type in the value of Weight (1 ~ 42).
PPR	This parameter is for descriptor type: PPR. Type in Peak Packet Rate (bits/sec).
Polling Speed	Polling speed determines the treatment of this channel when its data queue becomes empty.

PPR auto-polling speed mode	Select the checkbox to enable auto-polling speed mode.
CIR	This parameter is for descriptor type: CIR and CIREIR. Type in Committed Information Rate (bits/sec).
CBS	This parameter is for descriptor type: CIR and CIREIR. Type in Committed Burst Size (bits).
CIR Polling Speed	Polling speed determines the treatment of this channel when its data queue becomes empty.
CIR auto-polling speed mode	Select the checkbox to enable auto-polling speed mode (CIREIR traffic type doesn't support this mode).
EIR	This parameter is for descriptor type: CIREIR. Type in Excess Information Rate (bits/sec).
EBS	This parameter is for descriptor type: CIREIR. Type in Excess Burst Size (bits).
EIR Polling Speed	Currently not supported.
EIR auto-polling speed mode	Currently only auto-polling speed mode is supported.
<b>ADSL Descriptor</b>	
ATM Traffic Policer Type	Available options are: CBR(CLP transparent, no Scr), UBR(No CLP, No Src)
PCR	Type in the Peak Cell Rate (this parameter is for ATM traffic policer type CBR only). Value range is 0 ~ 65536 (cells/second).

3. Click on Create.

**To view detail information of Traffic Desc Profiles:**

1. Click on Table View.

Return											
Index	VDSL Layer Profile								ADSL Bridge Port Policer		
	Type	Weight	PPR	CIR	EIR	CBS	EBS	Polling Speed	Policer(ADSL only)	PCR(ADSL only)	
1	WFQ	1	N/A	N/A	N/A	N/A	N/A	NA	CBR	65536	
2	PPR	N/A	1000000	N/A	N/A	N/A	N/A	PPR PS=Auto	CBR	8000	
3	WFQ	1	N/A	N/A	N/A	N/A	N/A	NA	CBR	8000	
4	CIREIR	N/A	N/A	1000000	1000000	12144	12144	CIR PS=1000000; EIR PS=Auto	CBR	8000	

2. Click on Return to go back previous screen.

**To delete a Traffic Desc Profile:**

1. Click in the selection box next to the profile index you want to delete. Note that the system default profile with profile index 1 cannot be deleted.
2. Click on Delete Selected.
3. You can click on Delete All to delete all profiles at a time.

### 6.43 Configuration / Traffic Prioritization / Uplink VPMT Configure

Use the Configuration/Traffic Prioritization/Uplink VPMT Configure screen to configure the VLAN Priority Mapping Table (VPMT) for uplink bridge ports. There are 8 COS (priority) for an uplink bridge port; each of them has to be assigned "Queue Type". Queue Types include SPQ(0), SPQ(1), SPQ(2), and WFQ(3). SPQ(0) is the fastest Queue; data which is saved in this queue can be output first.

Configuration / Traffic Prioritization / Uplink VPMT Configure

Trunk Port VLAN Priority & Queue Mapping Table

Previous Command Result: Normal

Modify

Physical Port	CoS-0	CoS-1	CoS-2	CoS-3	CoS-4	CoS-5	CoS-6	CoS-7
GigaBit-1	WFQ(3)	WFQ(3)	SPQ(2)	SPQ(2)	SPQ(1)	SPQ(1)	SPQ(0)	SPQ(0)
	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass
GigaBit-2	WFQ(3)	WFQ(3)	SPQ(2)	SPQ(2)	SPQ(1)	SPQ(1)	SPQ(0)	SPQ(0)
	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass

To modify the uplink VPMT configuration:

1. Select the following fields:

Field	Description
WFQ(3), SPQ(0)~(2)	Select a Queue Type
Pass or Deny	Select Pass or Deny the packet

2. Click on Modify.

### 6.44 Configuration / Traffic Prioritization / VDSL VPMT Profile

Use the Configuration/Traffic Prioritization/VDSL VPMT Profile screen to configure the VLAN Priority Mapping Table (VPMT) profile for VDSL bridge ports.

Configuration / Traffic Prioritization / VDSL VPMT Profile

Previous Command Result: NormalRelated: Config Select

Create NewModify SelectedDelete SelectedDelete All

	Profile Index	CoS-0: TDesc	CoS-1: TDesc	CoS-2: TDesc	CoS-3: TDesc	CoS-4: TDesc	CoS-5: TDesc	CoS-6: TDesc	CoS-7: TDesc
<input type="checkbox"/>	1	WFQ(3): 1(WFQ)	WFQ(3): 1(WFQ)	WFQ(3): 1(WFQ)	WFQ(3): 1(WFQ)	WFQ(3): 1(WFQ)	WFQ(3): 1(WFQ)	WFQ(3): 1(WFQ)	WFQ(3): 1(WFQ)
<input checked="" type="checkbox"/>	2	SPQ(0): 2(SPQ)	SPQ(0): 2(SPQ)	SPQ(1): 2(SPQ)	SPQ(1): 2(SPQ)	SPQ(2): 4(SPQ)	SPQ(2): 4(SPQ)	WFQ(3): 1(WFQ)	WFQ(3): 3(WFQ)

A VDSL VPMT Profile has 8 COS (priority); each of them has to be assigned Ethernet traffic profile (descriptor) and "Queue Type". The types of Ethernet traffic profile are WFQ, PPR, CIR, and CIREIR. WFQ is WFQ-type profile. PPR, CIR, and CIREIR are SPQ-type profile. Queue Types are SPQ(0), SPQ(1), SPQ(2), and WFQ(3). SPQ(0) is the fastest Queue; data which is saved in this queue can be output first.

When the COS (priority) is assigned a SPQ-type profile, only SPQ(0)/SPQ(1)/SPQ(2) queue can be selected. When the COS (priority) is assigned to a WFQ-type profile, only WFQ(3) queue can be selected.

To create a VDSL VPMT profile:

1. Click on Create New. The VDSL VPMT Profile – Create screen appears.

Create

Items	CoS-0	CoS-1	CoS-2	CoS-3	CoS-4	CoS-5	CoS-6	CoS-7
Queue	WFQ(3)	WFQ(3)	WFQ(3)	WFQ(3)	WFQ(3)	WFQ(3)	WFQ(3)	WFQ(3)
Deny Mode	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass
Traffic Descriptor	1(WFQ)	1(WFQ)	1(WFQ)	1(WFQ)	1(WFQ)	1(WFQ)	1(WFQ)	1(WFQ)

2. For CoS-0 ~ CoS-7, enter or select the following fields:

Field	Description
Queue	Click on the drop-down list and select the internal queue for mapping. Options are: SPQ(0), SPQ(1), SPQ(2), WFQ(3).
Deny Mode	Select to Pass or Deny the packet.
Traffic Descriptor	Click on this drop-down list and select a traffic descriptor.

3. Click on Create.

**To modify a VDSL VPMT profile:**

1. Click in the selection box next to the profile you want to modify. Note that the system default profile with profile index 1 cannot be modified.
2. Click on Modify Selected.
3. Modify the fields as required.
4. Click on Modify.

**To delete a VDSL VPMT profile:**

1. Click in the selection box next to the profile you want to delete. Note that the system default profile with profile index 1 cannot be deleted.
2. Click on Delete Selected.
3. You can click on Delete All to delete all profiles at a time.

## 6.45 Configuration / Traffic Prioritization / VDSL VPMT Select

Use the Configuration/Traffic Prioritization/VDSL VPMT Select screen to bind VDSL VPMT profile to a VDSL physical port.

Configuration / Traffic Prioritization / V

Previous Command Result: Normal

Select page: page-1

Modify

Physical Port

VPMT Profile

Port-1

1

1. Enter or select the following fields:

Field	Description
VPMT Profile	Select the desired VDSL VPMT profile.

2. Click on Modify.



6.46 Configuration / VLAN / Static Multicast Pass Through

In this page, user can configure the Static Multicast Pass-through by VLAN ID. There are 2 types for data input – L2 (MAC Address) or L3 (IPv4 Address). This table supports Add and Delete for entry, not allow modify, maximum 64 entries. The entry can be defined with L2 or L3 address as per user expectation. This is just for user-friendly purpose, no matter configuring it with L2 or L3 type, they could achieve the same result.

Configuration / VLAN Configuration /Static Multicast Pass Through

Previous Command Result: Success

Input Data Type L2 (MAC)

Create

Index	VID	MAC Address
3	1	01:00:5E:00:00:00

Select page: page-1

☐ Check All

☐ Uncheck All

Delete

	Index	VID	MAC Address
<input type="checkbox"/>	1	1	01:00:5E:00:00:00
<input type="checkbox"/>	2	1	01:00:5E:00:00:01

Configuration / VLAN Configuration /Static Multicast Pass Through

Previous Command Result: Normal

Input Data Type L3 (IP Address)

Create

Index	VID	IP Address
3	1	224.0.0.0

Select page: page-1

☐ Check All

☐ Uncheck All

Delete

	Index	VID	IP Address
<input type="checkbox"/>	1	1	224.0.0.0
<input type="checkbox"/>	2	1	224.0.0.1

Field/Button information:

Field	Description
Index	Show the row number (1~64). Max 64 entries.
VID	VLAN ID. 1~4094
MAC Address	Layer 2 MAC Address. Range 01:00:5E:00:00:00 ~ 01:00:5E:7F:FF:FF
IP Address	IPv4 Address. Range <224~239>.<0~127>.<0~255>.<0~255>
Create	To create new entry. In same VID, duplicated MAC or IP Address is not allowed.
Delete	To delete selected entry(s).

### 6.47 Configuration / VLAN Configuration / VLAN – Egress Rate Limit

Use the Configuration/VLAN Configuration/VLAN – Egress Rate Limit screen to modify egress rate limit rule per VLAN per bridge port.

Configuration / VLAN Configuration / VLAN - Egress Rate Limit

Previous Command Result: Normal

Related: Members Remark Protocol Rate Limit Translation

Modify

Broadcast:

	Physical Port	VID	Policer Index	Block
<input type="checkbox"/>	Gigabit-1	1	DEFVAL	Do Rate Limit
<input type="checkbox"/>	Gigabit-2	1	DEFVAL	Do Rate Limit
<input type="checkbox"/>	Port-1--PVC-1	1	DEFVAL	Do Rate Limit
<input type="checkbox"/>	Port-4--PVC-1	1	DEFVAL	Do Rate Limit
<input type="checkbox"/>	Port-1--PVC-2	1	DEFVAL	Do Rate Limit

Unknown Unicast:

	Physical Port	VID	Policer Index	Block
<input type="checkbox"/>	Gigabit-1	1	DEFVAL	Do Rate Limit
<input type="checkbox"/>	Gigabit-2	1	DEFVAL	Do Rate Limit
<input type="checkbox"/>	Port-1--PVC-1	1	DEFVAL	Do Rate Limit
<input type="checkbox"/>	Port-4--PVC-1	1	DEFVAL	Do Rate Limit
<input type="checkbox"/>	Port-1--PVC-2	1	DEFVAL	Do Rate Limit

To modify a VLAN egress rate limit rule:

1. Click in the selection box next to the entry you want to modify.

2. Click on Modify Selected. The Egress Rate Limit – Modify screen appears.

Modify

Unicast

Physical Port

Gigabit-2

VID

1

Policer Index

DEFVAL

Block

Do Rate Limit

3. Enter or select the following fields:

Field	Description
Policer Index	Select the desired Policer profile index. Default is DEFVAL.
Block	Select Do Rate Limit or Block Traffic. Default is Do Rate Limit.

4. Click on Modify.

6.48 Configuration / VLAN Configuration / VLAN – Members & State

Use the VLAN Configuration screen to create, delete, or modify VLANs.

Related: Egress Rate LimitRemarkProtocolRate LimitTranslation

MembersState

Previous Command Result: Normal

VLANs: VDSL Mode

Create New VLANModify SelectedDelete Selected

	VLAN ID	Tagged Members(port:priority)	Untagged Members(port:priority)
<input type="checkbox"/>	1		G1:0,G2:0,1:0
<input checked="" type="checkbox"/>	2	G1:8	
<input type="checkbox"/>	3	1:8	

The currently configured VLANs are displayed in the table on this page. Set Default VLAN member and Static VLAN member with this function. The VLAN priority, Isolation are also available here.

VLANs	
ADSL/VDSL Mode	If ADSL Mode is selected, the VLAN setting/configuration will be for ATM Mode DSL Port only. If VDSL Mode is selected, the VLAN setting/configuration will be for Packet Mode DSL Port only.
VLAN ID	The VLAN ID for the VLAN
Tagged Member Port(s)	A list of ports that are tagged members of the VLAN. DSL ports are listed as numbers (1–24). Ethernet ports are shown as G1 and G2, or LACP. The number after : (colon), is the VLAN priority number.

Create a New VLAN

To create a new VLAN:

1.

In the VLANs box click on Create New VLAN button.
2.

The page will change to page for creation. Input the VLAN ID in the page for creation. Click Apply button. If no any bridge port created/exist for DSL port, then there is no port for VLAN Member assignment. An empty VLAN is allowed to create.
3.

The modification tips, just follow the steps of modification below.
4.

**Static VLAN/Default VLAN:** If the check box Default VLAN is checked up, it

means you're going to assign DSL port(s) to this VLAN and as Default VLAN of selected DSL port(s). If the check box is unchecked, it means you're going to assign DSL Port to a Static VLAN. Whenever the check box is checked up or unchecked, the member assignment list will refresh (it takes some time).

5. **Note:** If you remove member (DSL port) from a Static VLAN, the DSL port will go back to Default VLAN 1 (it is system default setting). But if you remove member from a Default VLAN 1, the bridge port will be deleted.

## Modify VLAN

To modify a VLAN:

1. In the VLANs box, select/check up an existing VLAN then click on Modify Selected.
2. The page will change to page for modification and it display the current configuration for the selected VLAN. If bridge ports are created, a black dash symbol will be shown for the DSL port, and then can start the VLAN member assignment.
3. Click on the dash for the port you want, the dash will change to T/U, which stands for Tag/Untag. BTW, the isolation will also change to Y, stands for Yes.
4. By default, priority number is 0 when you set T/U to the port. If you need other priority, change the Priority list under the VLAN ID field. If priority selection is changed, say pri-3, the tagged/untagged port will be shown in 0. And this moment, you can start to set T/U to other DSL ports with priority 3. [Tips: A DSL port has been assigned with T/U and pri-0, then it can't be assigned with other priority, unless you remove the T/U assignment and change it back to dash "-".]
5. To change the Isolation, the DSL port should be in T/U status, and then the Isolation can be changed between Y/N (Yes/No).
6. Click Apply button to submit the member assignment to selected VLAN.

## Delete a VLAN

To delete a VLAN:

1. In the VLANs box, select/check up an existing VLAN then click on Delete Selected. All the member assignment will be removed. If the VLAN is Static VLAN, all the ports will be removed, but they still belong to Default VLAN 1.

VLAN State

Members

State

Related: [Egress Rate Limit](#) [Remark](#) [Protocol](#) [Rate Limit](#) [Translat](#)

Previous Command Result: Normal

Select page: 

page-1

 VLAN ID Index: 

1

☐ Check All ☐ Uncheck All

Modify

	Physical Port	VLAN ID	VLAN Priority	Isolated	Default VLAN	IGMP Value
<input type="checkbox"/>	Gigabit-1	1	<div>Priority-0</div>	<div>Yes</div>	Yes	No
<input type="checkbox"/>	Gigabit-2	1	<div>Priority-0</div>	<div>Yes</div>	Yes	No
<input type="checkbox"/>	Port-2--PVC-1	1	<div>Priority-0</div>	<div>Yes</div>	Yes	No
<input type="checkbox"/>	Port-1--VDSLMode	1	<div>Priority-0</div>	<div>Yes</div>	Yes	No

Field	Description
VLAN Priority	Set VLAN priority for egress traffic. Value range is 0 ~ 7 if this VLAN is the default VLAN of the bridge port; value range is 0 ~ 7 or Reserved (reserve the original priority) if this VLAN is not the default VLAN.
Isolated	Yes/No. When port isolation is enabled (Yes), packets received from a trunk port (if both trunk interfaces are configured as up-link) cannot be forwarded to the other trunk port even for broadcasting. Also, packets received from a line bridge port (including trunk interface configured as a user link) cannot be forwarded to any other line bridge port even for broadcasting.
Default VLAN	Shows whether the entry's VID is the default port VID of the bridge port of this entry. Yes: the entry's VID is the default port VID of the bridge port. No: the entry's VID is not the default port VID of the bridge port.
IGMP Value	Shows whether this entry (row) in the table is created by the system automatically due to IGMP ACL profile binding to this port or not (if yes, the value is "Yes"). Because when a bridge port is binding to an ACL profile, the system will automatically add this bridge port to the members of the VLANs configured in IGMP ACL profile (SVID/UVID). And when the bridge port is no longer binding to the ACL profile, it will be removed from those VLANs by the system automatically. If this IGMP value is "No", it means that this entry is added by the user manually.



6.49 Configuration / VLAN Configuration / VLAN – Priority Remark

Use the Configuration/VLAN Configuration/VLAN – Priority Remark screen to configure the VLAN priority mapping.

**Note:** when system is in LACP mode, do not set DSCP and TOS priority remark at the same time for the same bridge port. Because some bits of DSCP and of TOS overlap.

Configuration / VLAN Configuration / VLAN – Priority Remark

Previous Command Result: Success

VLAN Priority Remark : TOS

Create

Index	Physical Port	TOS	Priority(Out)
2	Gigabit-1	0	0

Select page: page-1 ☐ Check All ☐ Uncheck All

Delete

	Index	Physical Port	TOS	Priority(Out)
<input type="checkbox"/>	1	Gigabit-1	0	1

To create a VLAN Priority Remark:

1.

Click on the drop-down list and select a type of VLAN Priority Remark. Available types include: TOS (Type of Service), IP Source, IP Destination, MAC Source, MAC Destination, VLAN ID, VLAN Priority Regeneration, and DSCP Priority Regeneration.
2.

Select the bridge port you want to create a priority remark rule for.
3.

Enter or select the following fields:

Priority Remark Type	Field	Description
TOS	TOS	In order to provide basic support for classes of service to the Internet Protocol. The IP protocol header contains what is known as the ToS (Type of Service) bits. Click on the drop-down list and select incoming TOS (value range 0 ~ 7), then you can create the mapping between TOS and VLAN priority.
	Priority (Out)	Click on the drop-down list and select the outgoing VLAN priority (0 ~ 7).

IP Source	Priority (Out)	Click on the drop-down list and select the outgoing VLAN priority (0 ~ 7).
	Source IP	Type in the IP address of the coming source.
	MASK	Type in the subnet mask.
IP Destination	Priority (Out)	Click on the drop-down list and select the outgoing VLAN priority (0 ~ 7).
	Destination IP	Type in the IP address of the destination.
	MASK	Type in the subnet mask.
MAC Source	Priority (Out)	Click on the drop-down list and select the outgoing VLAN priority (0 ~ 7).
	Source MAC	Type in the MAC Address of the coming source.
MAC Destination	Priority (Out)	Click on the drop-down list and select the outgoing VLAN priority (0 ~ 7).
	Destination MAC	Type in the MAC Address of the destination.
VLAN ID	VLAN	Type in the VLAN ID (1 ~ 4094).
	Priority (Out)	Click on the drop-down list and select the outgoing VLAN priority (0 ~ 7).
VLAN Priority Regen	Priority (In)	Click on the drop-down list and select the incoming VLAN Priority (0 ~ 7).
	Priority (Out)	Click on the drop-down list and select the outgoing VLAN priority (0 ~ 7).

DSCP	DSCP	<div>Click on the drop-down list and select the incoming DSCP (Differentiated Services Code Points, which is a 6-bit number). The standardized combinations are listed below:</div> <div><div>default</div><div>Default value (bits:000000)</div></div> <div><div>af11</div><div>Assured Forwarding Class 1:Low Drop (bits:001010)</div></div> <div><div>af12</div><div>Assured Forwarding Class 1:Medium Drop (bits:001100)</div></div> <div><div>af13</div><div>Assured Forwarding Class 1:High Drop (bits:001110)</div></div> <div><div>af21</div><div>Assured Forwarding Class 2:Low Drop (bits:010010)</div></div> <div><div>af22</div><div>Assured Forwarding Class 2:Medium Drop (bits:010100)</div></div> <div><div>af23</div><div>Assured Forwarding Class 2:High Drop (bits:010110)</div></div> <div><div>af31</div><div>Assured Forwarding Class 3:Low Drop (bits:011010)</div></div> <div><div>af32</div><div>Assured Forwarding Class 3:Medium Drop (bits:011100)</div></div> <div><div>af33</div><div>Assured Forwarding Class 3:High Drop (bits:011110)</div></div> <div><div>af41</div><div>Assured Forwarding Class 4:Low Drop (bits:100010)</div></div> <div><div>af42</div><div>Assured Forwarding Class 4:Medium Drop (bits:100100)</div></div> <div><div>af43</div><div>Assured Forwarding Class 4:High Drop (bits:100110)</div></div> <div><div>ef</div><div>Expedited Forwarding (bits:101110)</div></div>
	Priority (Out)	<div>Click on the drop-down list and select the outgoing VLAN priority (0 ~ 7).</div>

4. Click on Create.

**To delete a VLAN Priority Remark:**

1. Click in the selection box next to the entry you want to delete. You can click in the Check All selection box to select all entries at a time (To cancel the selection, click in UnCheck All selection box).
2. Click on Delete.

6.50 Configuration / VLAN Configuration / VLAN – Protocol Based

Use the Configuration/VLAN Configuration/VLAN – Protocol Based screen to configure the protocol based VLAN table. 5224AV-2GBE/2SFP supports protocol-based VLAN function in a many-to-one (N:1) VLAN model. It is able to classify streams with different EtherType for protocol-based VLAN function in upstream direction and sends out the frames classified by protocol-based VLAN function as untagged frames in downstream direction.

5224AV-2GBE/2SFP adds S-tag on received untagged and priority tagged frames in upstream direction. For received priority tagged frames, S-tag will replace the original priority tag. The S-tag can be an operator-configured value or “reserve” the original priority. Note that when “reserve” is selected for the priority assigning option, the system will by default assign ‘0’ to the priority of S-tag added for the classified untagged frames in upstream direction.

5224AV-2GBE/2SFP supports multiplexed protocol-based VLAN filtered streams, VLAN translation streams, and general IEEE 802.1Q streams over one line bridge port. When the configuration of protocol-based VLAN function conflicts with VLAN translation function, the system supports protocol-based VLAN setting/rules with higher priority than the setting/rules of VLAN translation function.

Configuration / VLAN Configuration / VLAN - Protocol Based

Previous Command Result: Success

Related: Egress Rate Limit Members Remark Rate Limit Static Translation

Create

Index	Physical Port	VlanEthType	Ingress VLAN ID	Ingress Priority	Egress VLAN ID	Egress Priority
2	Port-2--PVC-1	PPPoE Discovery Stage	0x8863	1	Reserved	1

Select page: page-1

☐ Check All ☐ Uncheck All

Delete

	Index	Physical Port	VlanEthType	Ingress VLAN ID	Ingress Priority	Egress VLAN ID	Egress Priority
<input type="checkbox"/>	1	Port-2--PVC-1	PPPoE Discovery Stage	0x8863	1	Reserved	1

To create a Protocol Based VLAN:

1. Enter or select the following fields:

Field	Description
Physical Port	Select the bridge port you want to create protocol based VLAN for.
VlanEthType	Select the EtherType (protocol). If you select <b>Other</b> , type the EtherType value in the right field.
Ingress VLAN ID	Enter Ingress VLAN ID for the protocol based VLAN rule.

	Value range: 1 ~ 4094, or 65535 for untagged.
Ingress Priority	Enter Ingress VLAN priority (Reserved or 0 ~ 7).
Egress VLAN ID	Enter Egress VLAN ID for the protocol based VLAN rule. Value range: 1 ~ 4094.
Egress Priority	Enter Egress VLAN priority (Reserved or 0 ~ 7).

2. Click on Create.

**To delete a Protocol Based VLAN:**

1. Click in the selection box next to the entry you want to delete. You can click in the Check All selection box to select all entries at a time (To cancel the selection, click in UnCheck All selection box).
2. Click on Delete.

6.51 Configuration / VLAN Configuration / VLAN – Rate Limit

Use the Configuration/VLAN Configuration/VLAN – Rate Limit screen to limit the rate of broadcast/unicast packets that are received on a VLAN.

Configuration / VLAN Configuration / VLAN - Rate Limit

Previous Command Result: Normal

Related: Egress Rate LimitMembersRemarkProtocolStaticTranslation

Create NewModify SelectedDelete Selected

Broadcast:

	VID	CIR	LSBL	Block
<input checked="" type="checkbox"/>	1	10000	80	Do Rate Limit

Unicast:

	VID	CIR	LSBL	Block
<input type="checkbox"/>	1	1000000	800	Block Traffic

To create a VLAN rate limit rule:

- 1. Click on Create New. The Rate Limit – Create screen appears.
- 2. Enter or select the following fields:

Field	Description
Broadcast	Select Broadcast or Unicast packets to be limited.
VID	Type in VLAN ID (1 ~ 4094).
CIR	Committed Information Rate (1536 ~ 1G bits/second). The threshold rate to turn on the rate-limit mechanism.
LSBL	Leakage bucket size. Set the sustained rate at which broadcast packets can be accommodated (1 ~ 1024 milliseconds).
Block	Select Do Rate Limit or Block Traffic.

- 3. Click on Create.

To modify a VLAN rate limit rule:

- 1. Click in the selection box next to the entry you want to modify.
- 2. Click on Modify Selected. The Rate Limit – Modify screen appears.
- 3. Modify the fields as required.
- 4. Click on Modify.

To delete a VLAN rate limit rule:

- 1. Click in the selection box next to the entry you want to delete.
- 2. Click on Delete Selected.



6.52 Configuration / VLAN Configuration / VLAN – Translation

Use the Configuration/VLAN Configuration/VLAN – Translation screen to configure the translation VLAN table, which defines some special VLAN working rules such as VLAN stack, VLAN cross-connect, etc. Before you configure the Translation VLAN table for a line (user) bridge port, you shall configure the Static VLAN table for this line bridge port and the GIGA bridge port in advance. Also, you must select **Non-TLS** for the line bridge port’s VLAN mode specified in the VDSL or ADSL bridge port interface setup page, otherwise the VLAN translation rule will not take effect.

Configuration / VLAN Configuration / VLAN - Translation

Previous Command Result: Normal

Related: Egress Rate LimitMembersRemarkProtocolRate LimitStatic

Create

Index	Physical Port	User VLAN ID	User Priority	Uplink VLAN ID	Uplink Priority	Translation VLAN Mode	Uplink Port	Ingress Policer	Egress Policer	New User VLAN ID	New User Priority
4	Port-1 -- PVC-1	1	0	1	0	one-to-one-stacking	1	1	1	1	0

Select page: page-1

☐ Check All☐ Uncheck All

Delete

	Index	Physical Port	User VLAN ID	User Priority	Uplink VLAN ID	Uplink Priority	Translation VLAN Mode	Uplink Port	Ingress Policer	Egress Policer	New User VLAN ID	New User Priority
<input type="checkbox"/>	1	Port-1 -- PVC-1	10	0	100	0	one-to-one-replaced	1	2	3	--	--
<input type="checkbox"/>	2	Port-9 -- PacketMode	20	0	200	0	one-to-one-stacking	1	1	3	1	0
<input type="checkbox"/>	3	Port-2 -- PVC-2	30	0	300	0	many-to-one-stacking	1	--	--	1	0

5224AV-2GBE/2SFP provides four translation modes: two for one-to-one (1:1) VLAN model, two for many-to-one (N:1) VLAN model (refer to DSL Forum TR-101). For 1:1 VLAN model, each S-VID or S-VID + C-VID (double tagged scheme) pair of line bridge port is unique in one system. As for N:1 VLAN model, a group of line bridge ports could have the same S-VID or S-VID + C-VID (if C-tag applicable) pair.

One-to-One VLAN:

If the user bridge port only has 1:1 VLAN, then MAC learning function of this bridge port can be disabled.

1. Replaced

In this mode, the system will change the user port’s C-Tag to the Uplink port’s S-Tag. And the mapping is one to one, that is, one user port’s C-Tag (one VID) can only translate to one uplink port’s S-Tag (one VID), and vice versa. For example, for ADSL Port1-PVC1, if ADSL VID 5 translates to GIGA1 VID 1, then you cannot make ADSL VID 5 translate to another GIGA VID. You cannot make another ADSL VID translate to GIGA VID1, either.

Upstream:

C-Tag→(User port)----->(Uplink port)→S-Tag

Downstream:  
S-Tag→(Uplink port)----->(User port)→C-Tag

2. Stacking

In this mode, the system will replace the user port’s C-Tag to C’-Tag and add S-Tag before C’-Tag. Note that the mapping from C-Tag to S-Tag+C’-Tag is still one to one. So a user port’s C-Tag can’t be used for another translation rule, as well as an uplink port’s S-Tag+C’-Tag.

Upstream:  
C-Tag→(User port)----->(Uplink port)→S-Tag+C’-Tag

Downstream:  
S-Tag+C’-Tag→(Uplink port)----->(User port)→C-Tag

Many-to-One VLAN:

N:1 can also be called shared VLAN, so in this mode MAC learning function of the bridge ports must not be disabled.

1. Replaced

In this mode, the system will change the user port’s C-Tag to the Uplink port’s S-Tag. And the mapping is N to 1, so a user port’s C-Tag can’t be used for another VLAN translation rule. But an uplink port’s S-Tag can be used for another N:1 VLAN translation rule.

So in this mode several bridge ports can have the same VLAN cross-connect rule.

2. Stacking

In this mode, the system will replace the user port’s C-Tag to C’-Tag and add S-Tag before C’-Tag. Note that the mapping from C-Tag to S-Tag+C’-Tag is many to one. A user port’s C-Tag can’t be used for another translation rule, but an uplink port’s S-Tag+ C’-Tag can be used for another N:1 VLAN translation rule.

To create a VLAN Translation rule:

1. Select an option for the field **Translation VLAN Mode**. Options are:  
one-to-one-replaced, one-to-one-stacking, many-to-one-replaced, and many-to-one-stacking
2. Enter or select the following fields (the fields displayed depend on which Translation VLAN Mode you choose):

Field	Description
Index	Indicates the index of the next created entry in the VLAN Translation table.
Physical Port	Select the line bridge port you want to create a VLAN translation rule for.
User VLAN ID	Enter the VLAN ID of the user port.

User Priority	Select the user priority (0 ~ 7 or Reserved)
Uplink VLAN ID	Enter the VLAN ID of the uplink port.
Uplink Priority	Select the uplink priority (0 ~ 7 or Reserved)
Uplink Port	Select the uplink port.
New User VLAN ID	Type in the new User VLAN ID for stacking mode.
New User Priority	Type in the new User priority for stacking mode.

3. Click on Create.

**To delete a VLAN Translation rule:**

1. Click in the selection box next to the entry you want to delete. You can click in the Check All selection box to select all entries at a time (To cancel the selection, click in UnCheck All selection box).
2. Click on Delete.

# DATA-CONNECT

*The Right Connection!*

Configuration

---

7 Diagnostics

7.1 Diagnostics / DELT

Use the Diagnostics/DELT screen to perform ADSL2 DELT (Dual-Ended Line Test, as definition in G.992.3) and display the result of test. This function also provides the graphical view for HLin and Carrier Data (Hlog/QIn/Hlin Scale/Snr) when the test is done and test result is available.

Auto Refresh Interval: 30 seconds

Previous Command Result: Normal

Refresh

Physical Port	Op Status	Loopback State	DELT State	DELT Timeout	Activate loopback	Activate DELT	Carrier Data	HLin	DELT & Band Parameter
Port-6	Handshake	Idle	Off	0	Loopback	DELT	Query	Query	Query
Port-7	Handshake	Idle	Off	0	Loopback	DELT	Query	Query	Query
Port-8	Handshake	Idle	Off	0	Loopback	DELT	Query	Query	Query
Port-9	Handshake	Idle	Off	0	Loopback	DELT	Query	Query	Query
Port-10	Handshake	Idle	Off	0	Loopback	DELT	Query	Query	Query
Port-11	Handshake	Idle	Off	0	Loopback	DELT	Query	Query	Query
Port-12	Handshake	Idle	Off	0	Loopback	DELT	Query	Query	Query
Port-13	Data	Idle	Off	0	Loopback	DELT	Query	Query	Query
Port-14	Handshake	Idle	Off	0	Loopback	DELT	Query	Query	Query
Port-15	Handshake	Idle	Off	0	Loopback	DELT	Query	Query	Query
Port-16	Handshake	Idle	Off	0	Loopback	DELT	Query	Query	Query

Field/Button Information:

Field	Description
Physical Port	Show the line port number (1 ~ 24).
Op Status	Show current operational state of the circuit.
Loopback Test	
Loopback State	Show the status of loopback test. Possible states are: Idle, Progress, Success, and Fail.
Activate loopback	If this port is in operation and connected to a modem successfully, "Loopback" appears on this button. Click on this button to start a loopback test. The system will send a specific data string to the VDSL modem. If the data string comes back successfully, the loopback test



# DATA-CONNECT

The Right Connection!

	succeeds.
<b>DELT Test</b>	
DELT State	Shows the status of DELT. Possible states are: Off, Init, Complete, Progress, and Failure.
Activate DELT	Click on <b>Delt</b> to start a DELT. After the test starts, click on <b>Refresh</b> to query current testing status, and the button <b>Delt</b> will turn into <b>Abort</b> button. If you want to discontinue a test or make the loop go back to the normal state after the test has finished, just click on <b>Abort</b> . (When DELT is finished successfully, the <i>Delt State</i> will show 'Complete' and the Op Status will show 'delt done'.)
DELT Timeout	Shows the allowed time period to perform DELT test after DELT is activated. If exceed the time and DELT has not completed, test should be stated as Failure. Valid values: 1 ~ 60 (minutes), 0 for no timeout.
<b>DELT Test Result</b>	
Carrier Data	Click on Query to view the carrier data. <b>Hlog</b> : Channel characteristics function per sub-carrier group (a format providing magnitude values on a base 10 logarithmic scale.) <b>Qln</b> : Quiet line noise for a particular sub-carrier is the rms level of the noise present on the loop when no VDSL2 signals are present on the loop. <b>Hlin Scale</b> : The scale factor used for Hlin (channel characteristics function per sub-carrier group; it is represented in linear format by a scale factor and a normalized complex number.) <b>Snr</b> : The signal-to-noise ratio for a particular sub-carrier is a real value that shall represent the ratio between the received signal power and the received noise power for that sub-carrier.
Hlin	Click on Query to view detail Hlin data.
DELT & Band Parameter	Click on Query to view DELT & Band Parameter.

### Get DELT Graph

- Step 1: Enable the DSL Port service and connect the CPE modem.
- Step 2: Once the CPE modem is under operational status (link is up). Click button Activate DELT, around 1 minute the page will turn as below picture.
- Step 3: Select the Carrier Data or HLin to show the result data and graphical view.



# DATA-CONNECT

The Right Connection!

## Diagnostics / DELT

Auto Refresh Interval: 15 seconds

Previous Command Result: Normal

Refresh									
Physical Port	Op Status	Loopback State	DELT State	DELT Timeout	Activate loopback	Activate DELT	Carrier Data	HLin	DELT & Band Parameter
Port-1	Data	Idle	Off	0	Loopback	DELT	Query	Query	Query
Port-2	Handshake	Idle	Progress	0	Loopback	Abort	Query	Query	Query
Port-3	Data	Idle	Off	0	Loopback	DELT	Query	Query	Query
Port-4	Data	Idle	Off	0	Loopback	DELT	Query	Query	Query
Port-5	delt done	Idle	Complete	0	Loopback	Abort	Query	Query	Query
Port-6	Data	Idle	Off	0	Loopback	DELT	Query	Query	Query
Port-7	Data	Idle	Off	0	Loopback	DELT	Query	Query	Query

The page options have 1~8 and all, if 1~8 is selected, there would be a data table and a graph shown. But if select the "all", there would be only one graph for overall data, no table view.

Example: [Select Carrier Data Hlog – All](#)

Carrier Data

Circuit Number:1

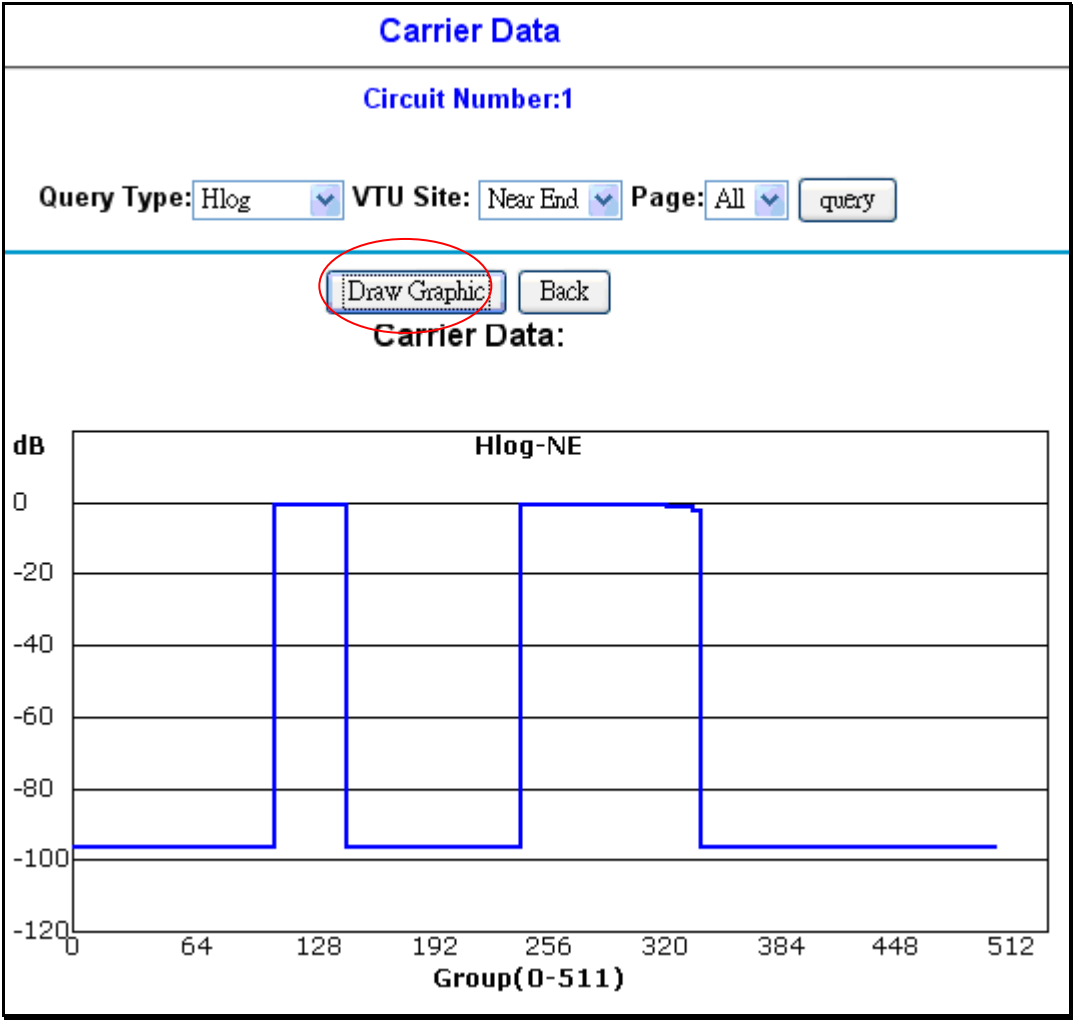
Query Type: Hlog VTU Site: Near End Page: All query

Draw Graphic Back

Carrier Data:

# DATA-CONNECT

The Right Connection!



### 7.2 Diagnostics / Power Mode

Use the Diagnostics/Power Mode screen to view the VDSL power management mode of each line port.

Diagnostics / Power Mode

Previous Command Result: Normal

Physical Port	PM State	Forced PM State	Select
Port-1	L3 Mode	False	Force L3 Mode
Port-2	L3 Mode	False	Force L3 Mode
Port-3	L3 Mode	False	Force L3 Mode
Port-4	L3 Mode	False	Force L3 Mode
Port-5	L3 Mode	False	Force L3 Mode
Port-6	L3 Mode	False	Force L3 Mode
Port-7	L3 Mode	False	Force L3 Mode
Port-8	L3 Mode	False	Force L3 Mode
Port-9	L3 Mode	False	Force L3 Mode
Port-10	L3 Mode	False	Force L3 Mode

The following information is displayed:

Field	Description
Physical Port	Shows the line port number (1 ~ 24).
PM State	Shows current power management state of the port. Possible values are: Off, L0 Mode (full on), L2 Mode (low power), and L3 Mode (idle).
Forced PM State	Shows whether the VDSL port is forced to enter power management L3 mode or not. False: not forced to L3 mode True: forced to L3 mode
Select	Click on <b>Force L3 Mode</b> (when Force L3 Mode is shown in this field) if you want to force the port to enter L3 power mode.

### 7.3 Diagnostics / Power-On Self-Test (POST)

Use the Diagnostics/Power-On Self-Test screen to view the VDSL POST (power-on self-test) state of the three DSP chips in the system.

Diagnostics / Power-On Self-Test(POST)			
Item	Chip 1	Chip 2	Chip 3
POST State	NO TEST(2)		
BME Status	EQUIPED	EQUIPED	EQUIPED
HIC Host-BME Connection Test	NO TEST	NO TEST	NO TEST
BME Core & Mem Clk, EMI Initialization	NO TEST	NO TEST	NO TEST
HIC PIO SDRAM Read/Write Tests	NO TEST	NO TEST	NO TEST
BSDRAM Address & Data Bus Connection Tests	NO TEST	NO TEST	NO TEST
Memory to Memory BME DMA Tests	NO TEST	NO TEST	NO TEST
External Memory Interface Test	NO TEST	NO TEST	NO TEST
BME-AFE DDR Bus Connection Tests	NO TEST	NO TEST	NO TEST
AFE Register Read/Write Tests	NO TEST	NO TEST	NO TEST
IFE Register Read/Write Tests	NO TEST	NO TEST	NO TEST

Column	Description
Item	This column lists different POST testing items.
Chip 1	This column shows test results of DSP Chip 1.
Chip 2	This column shows test results of DSP Chip 2.
Chip 3	This column shows test results of DSP Chip 3.

Appendix

A. Alarm Table

190

B. Event Table

192

A. Alarm Table

Table A-1 Alarm Table

Alarm ID	Alarm Name	Description
101	SYS_HOUSEKEEP1	House Keeping 1
102	SYS_HOUSEKEEP2	House Keeping 2
103	SYS_HOUSEKEEP3	House Keeping 3
104	SYS_HOUSEKEEP4	House Keeping 4
105	SYS_FAN	Fan Error
106	SYS_SELFTESTFAILED	Self Test Failed
107	SYS_ABOVETEMP	Temperature Above Threshold
108	SYS_BELOWTEMP	Temperature Below Threshold
109	SYS_PIV	Product Identification Violation
201	GBE_LOS	Gigabit Ethernet Loss of Signal
301	Cluster_MasterDuplication	Cluster has duplicate Master (two Masters exist)
302	Cluster_MasterOutOfCapacity	Cluster is out of capacity
303	Cluster_HostUnmanaged	Cluster node enter unmanaged state
601	XDSL_LOF	XDSL Loss Of Framing
602	XDSL_LOS	XDSL Loss Of Signal
603	XDSL_LOSQ	XDSL Loss Of Signal Quality
604	XDSL_LOL	XDSL Loss Of Link
605	XDSL_DATA_INIT_FAILURE	XDSL Data Init Failure
606	XDSL_BELOW_SLA_DS	XDSL actual data rate is less than the configured Service Level Agreement threshold for downstream direction
607	XDSL_BELOW_SLA_US	XDSL actual data rate is less than the configured Service Level Agreement threshold for upstream direction
608	XDSL_ESE	XDSL Excessive Severely Errored Seconds
609	XDSL_NCD_SLOW	XDSL No Cell Delineation on the slow channel
610	XDSL_LCD_SLOW	XDSL Loss of Cell Delineation on the slow channel
611	XDSL_NCD_FAST	XDSL No Cell Delineation on the fast channel
612	XDSL_LCD_FAST	XDSL Loss of Cell Delineation on the fast channel



613	XDSL_LOF_FE	XDSL FE Loss Of Framing
614	XDSL_LOS_FE	XDSL FE Loss Of Signal
615	XDSL_LPR_FE	XDSL FE Loss Of Power Failure
616	XDSL_LOSQ_FE	XDSL FE Loss Of Signal Qualtiy
617	XDSL_NO_PEER_VTU_PRESENT_FE	XDSL FE No Peer VTU Present
618	XDSL_ESE_FE	XDSL FE Excessive Severely Errored Seconds
619	XDSL-NCD-SLOW-FE	XDSL FE No Cell Delineation on the slow channel
620	XDSL-LCD-SLOW-FE	XDSL FE Loss of Cell Delineation on the slow channel
621	XDSL_NCD_FAST_FE	XDSL FE No Cell Delineation on the fast channel
622	XDSL_LCD_FAST_FE	XDSL FE Loss of Cell Delineation on the fast channel

B. Event Table

Table B-1    Event Table

Event ID	Event Name	Description
1	SYSTEMRESTART	System Restart
2	SYSTEMDOWNLOADBEGIN	Download Begin
3	SYSTEMDOWNLOADSUCCESS	Download Success
4	SYSTEMDOWNLOADFAIL	Download Failed
5	SYSTEMPROVISIONDATAEXPORT	Provision Data Exported
6	SYSTEMPROVISIONDATAIMPORT	Provision Data Imported
7	SYSTEMPROVISIONDATASETDEFAULT	Provision Data Set To Default
9	SYSTEMALARMLOGCLEAR	Alarm Log Cleared
10	SYSTEMEVENTLOGCLEAR	Event Log Cleared
11	SYSTEMRTCDATETIMECHANGE	RTC date/time changed
12	SYSTEMSOFTWAREACOBUTTONSET	Software ACO Set
13	SYSTEMSOFTWAREACOBUTTONCLEAR	Software ACO Cleared
14	SYSTEMALARMLEVELMASKFLAGCHANGE	Alarm Profile changed
15	SYSTEMSNMPAUTHFAIL	SNMP Auth Failed
17	SYSTEMFTPRECEPTIONSTART	FTP Reception Started
18	SYSTEMFTPRECEPTIONCOMPLETE	FTP Reception Completed
19	SYSTEMFTPRECEPTIONINCOMPLETE	FTP Reception Incomplete
21	SYSTEMSNTPTIMEZONECHANGE	SNTP Time zone Changed
23	SYSTEMSNTPPROVISIONCHANGED	SNTP Provision Changed
25	SYSTEMDATABASESAVINGFAILED	Database Saving Failed
26	SYSTEMUSERLOGINSUCCESS	User login success
27	SYSTEMUSERLOGINFAILURE	User login fail
28	SYSTEMUSERLOGOUT	User logout
29	SYSTEMUSERTIMEOUTLOGOUT	User logout due to timeout
30	SYSTEMUNAVAILABLERADIUSSERVER	Unavailable RADIUS server
102	ATMCREATEVCL	ATM VCL Created
103	ATMMODIFYVCL	ATM VCL Modified
104	ATMDELETEVCL	ATM VCL Deleted

Event ID	Event Name	Description
301	CLUSTER_INFO_CHANGED	Cluster Info Changed
501	XDSL_PORT_INFO_CHANGED	XDSL Port Info Changed
601	XDSL_PORT_BINDING_CHANGED	XDSL Port Binding Changed
602	XDSL_PORT_ENABLED	XDSL Port Enabled
603	XDSL_PORT_DISABLED	XDSL Port Disabled
604	XDSL_PORT_REENABLED	XDSL Port Re-enabled
605	XDSL_PORT_LINKUP	XDSL Port Link Up
606	XDSL_PORT_LINKDOWN	XDSL Port Link Down
607	VDSL_LINE_CONF_PROFILE_CREATED	VDSL Line Configuration Profile Created
608	VDSL_LINE_CONF_PROFILE_DELETED	VDSL Line Configuration Profile Deleted
609	VDSL_LINE_CONF_PROFILE_CHANGED	VDSL Line Configuration Profile Changed
610	VDSL_LINE_ALARM_CONF_PROFILE_CREATED	VDSL Line Alarm Configuration Profile Created
611	VDSL_LINE_ALARM_CONF_PROFILE_DELETED	VDSL Line Alarm Configuration Profile Deleted
612	VDSL_LINE_ALARM_CONF_PROFILE_CHANGED	VDSL Line Alarm Configuration Profile Changed
613	XDSL_PORT_PROFILE_TRANSFER_FAILED	XDSL Port Profile Transfer Failed
614	XDSL_LOOPBACK_SET	XDSL Loopback Set
615	XDSL_DELT_SET	DELT (dual end loop test) is activated.
616	XDSL_DELT_DONE	DELT (dual end loop test) is done.
625	XDSL-NE-FORCE-TO-L3-MODE	PMSF (power management state force) perform a transition into L3 by CO.
626	XDSL-FE-FORCE-TO-L3-MODE	PMSF (power management state force) perform a transition into L3 by CPE.
627	XDSL-NE-LEAVE-L3-MODE	PMSF (power management state force) perform a transition from L3 to L0 by CO.
628	XDSL-FE-LEAVE-L3-MODE	PMSF (power management state force) perform a transition from L3 to L0 by CPE.
651	XDSL_PERF_NE_ES	Near End 15-min Error Second threshold has been reached
652	XDSL_PERF_NE_SES	Near End 15-min Severe Error Second

Event ID	Event Name	Description
		threshold has been reached
653	XDSL_PERF_NE_UAS	Near End 15-min Unavailable Seconds threshold has been reached
654	XDSL_PERF_FE_ES	Far End 15-min Error Second threshold has been reached
655	XDSL_PERF_FE_SES	Far End 15-min Severe Error Second threshold has been reached
656	XDSL_PERF_FE_UAS	Far End 15-min Unavailable Seconds threshold has been reached
657	XDSL_PERF_NE_DAY_ES	Near End Day Error Second threshold has been reached
658	XDSL_PERF_NE_DAY_SES	Near End Day Severe Error Second threshold has been reached
659	XDSL_PERF_NE_DAY_UAS	Near End Day Unavailable Seconds threshold has been reached
660	XDSL_PERF_FE_DAY_ES	Far End Day Error Second threshold has been reached
661	XDSL_PERF_FE_DAY_SES	Far End Day Severe Error Second threshold has been reached
662	XDSL_PERF_FE_DAY_UAS	Far End Day Unavailable Seconds threshold has been reached
663	XDSL_DOWN_MAX_SNR_MGN	Downstream maximum SNR margin has been reached.
664	XDSL_DOWN_MIN_SNR_MGN	Downstream minimum SNR margin has been reached.
665	XDSL_UP_MAX_SNR_MGN	Upstream maximum SNR margin has been reached.
666	XDSL_UP_MIN_SNR_MGN	Upstream minimum SNR margin has been reached.
667	XDSL_INIT_FAILURE_TRAP	Failed initializations threshold has been reached