VigorAccess

User Installation Guide

DrayTek

History Table

Date	Descriptions	Version	By
2005/7/22	Initial	V1.0	Jenny, Jimmy, Amy

Table of Contents

About This User's Manual

This manual is designed to assist users in using one of the series of high performance IP DSLAM. The information contained in this document is subject to change without notice. If you have any inquiries, please feel free to contact our support team via E-mail, Fax or phone. For the latest product information and features, please visit our website at **www.DrayTek.com.**

COPYRIGHT

Trademark

DrayTek is a registered trademark of DrayTek Corp. IP DSLAM product series are trademarks of DrayTek Corp. Other trademarks and registered trademarks of products mentioned in this manual may be the properties of their respective owners and only used for identification purposes.

Target Readers

This guide is intended for those responsible for hardware unpacking and installing for IP DSLAM.

DRAYTEK LIMITED WARRANTY

We warrant to the original end user (purchaser) that the IP DSLAM will be free from any defects in workmanship or materials for a period of three (3) years from the date of purchasing from the dealer. Please keep your purchase receipt in a safe place because it serves as the proof of purchase date.

During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, at our discretion, we will repair or replace the defective products or components, without charging for either parts or labor, to whatever extent we deem necessarily to restore the product in proper operating condition. Any replacement will consist of a new or remanufactured functionally equivalent product of equal value, and will be offered solely at our discretion. This warranty will not apply if the product is modified, misused, tampered with, damaged by an act of God, or subject to abnormal working conditions.

The warranty does not cover the bundled or licensed software of other vendors. Defects that do not significantly affect the usability of the product will not be covered by the warranty.

We reserve the right to revise the manual and online documentation to make changes from time to time in the contents here of without obligation to notify any person of such revisions or changes.

BE A REGISTERED OWNER

Online web registration at **www.DrayTek.com** is preferred. Alternatively, fill in the registration card and mail it to the address found on the reverse side of the card. Registered owners will receive our future product and update information.

CAUTION

There is the risk of explosion if an incorrect type of battery is replaced. Dispose of used batteries according to local environmental instructions.

SAFETY INSTRUCTIONS

Operation Environment

- Make sure that the AC power source is in the range of AC 100-240V.
  The IP DSLAM should be used in a sheltered area, within a temperature range from 0 to +50 °C and relative humidity in the range of 10% and 90%.
- DC power source operating condition: -42 to –56VDC. Do not expose the IP DSLAM to direct sunlight or other heat sources. The housing and electronic components may be damaged by direct sunlight or heat sources.

Installation

- Read the quick start guide and installation manual before turning on the power switch of device.
- Locate the emergency power-off switch near the device prior to power connection.
- Fixing the device on chassis to maintain air circulation and stable condition is recommended.
- Do not work alone if the operation environment is dangerous.
- Check and avoid the potential hazard for moist environment, and grounding issue for power cable.
- Please turn off the power switch when replacing fuse, installing or removing chassis.
- Do not place the device in a damp or humid place, e.g. a bathroom- (such as this environment).
- Avoid operating cable connection during lightning period.
- When you want to dispose of the IP DSLAM, please follow local regulations on conservation of the environment.

Maintenance

- Users can replace fuses by removing the module and replace it when necessary. Other components should be repaired by authorized and qualified personnel. Do not try to open or repair the device by yourself.
- The fuse for AC power inlet should be identical to the following standard: 250VAC, 2A

EUROPEAN COMMUNITY DECLARATIONS

DrayTek Corporation declares that the IP DSLAM is in compliance with the essential requirements and other relevant provisions of R&TTE Directive 99/5/EC.

CUSTOMER SUPPORT

Please prepare the following information before you contact your customer support.

- Product model and serial number.
- Warranty information.
- Date that you received IP DSLAM.
- Product configuration.
- Software release version number.
- Brief description of your problem.
- Steps that you may take to solve it and associate their SysLog messages.

The information of customer supports and sales representatives is in **www.DrayTek.com**, respectively.

ORGANIZATION

This document is separated into the following chapters:

Chapter	Title	Description	Page
1	Preface and Hardware Description	Provides a product overview and hardware architecture description.	**12**
2	Installation	Provides installation, LED indication and hardware installation.	**31**
3	IPDSLAM Product Feature Setup	Provides IPDSLAM product feature and setup.	**45**
4	General CLI command Instruction	Provides an instruction for command line interface.	**54**

CHAPTER 1
Preface and Hardware Architecture

This chapter is divided into the following sections,

- Section 1.1: Introduction
- Section 1.2: Hardware Architecture
- Section 1.3: Box Connections
- Section 1.4: Power Connection
- Section 1.5: ADSL Port Connection
- Section 1.6: Connector and Interface Description

1.1 Introduction

With the explosive growth of Internet, people are becoming more and more relying on Internet in daily life. The rapidly increase in bandwidth demanded by digital society has put pressure on the network therefore, bandwidth and performance management are becoming critical issue for ISP.

IP DSLAM, which is equipped with 24 ADSL2/+ ports, is designed for ISP (Internet Service Provider) to implement bandwidth management for multiple subscribers. As IP DSLAM supports high upstream and downstream bit-rates performance, therefore, IP DSLAM is being deployed primarily for residential customer for IPTV application or high speed Internet service or business customers to replace expensive T1/E1 leased line.

IP DSLAM is not only equipped with a console port being used for local management, but also provided excellent capabilities of SNMP, Telnet for remote management. In particular, IP DSLAM can be easily configured by EMS. The EMS system covers topology, configuration, deployment, security, alarm management and backed storage. Moreover, with the solution of port-based and tag-based VLAN, IP DSLAM can isolate traffic between different users and provide improved security.

The compact design of IP DSLAM is composed of two units. One is Slave for 24-port ADSL 2/+ with built-in POTS splitters connected to ADSL modems. The other is Master, which has DSL, optical interfaces, and 6 subtend interfaces. IP DSLAM provides lots of applications as below:

High speed Internet Service

IP DSLAM aggregates DSL subscribers and terminates the encapsulated type ATM cell. Users can easily access Internet through the IP backbone network.

Gaming application Service

By combining gaming server, IP DSLAM can provide gaming service.

Stream TV Service

IP DSLAM uses ADSL 2/+ high speed DSL technology, and supports stream TV Service.

Video on Demand Service

Service provider can offer multimedia services by setting up video or content server on the local side. By combining rich content video server, IP DSLAM also provides the video on demanded service. Users can easily access multimedia content based on IP DSLAM architecture.

Combined with VoIP Service

IP DSLAM can combine IAD, DSL/VoIP gateway with highest priority to provide toll quality voice communication in terms of voice quality and reliability for the users.

Mail or Portal Service

IP DSLAM provides the feasibility to connect mail or proxy server.

Application scenario of IP DSLAM for general users is shown in Figure 1-1.

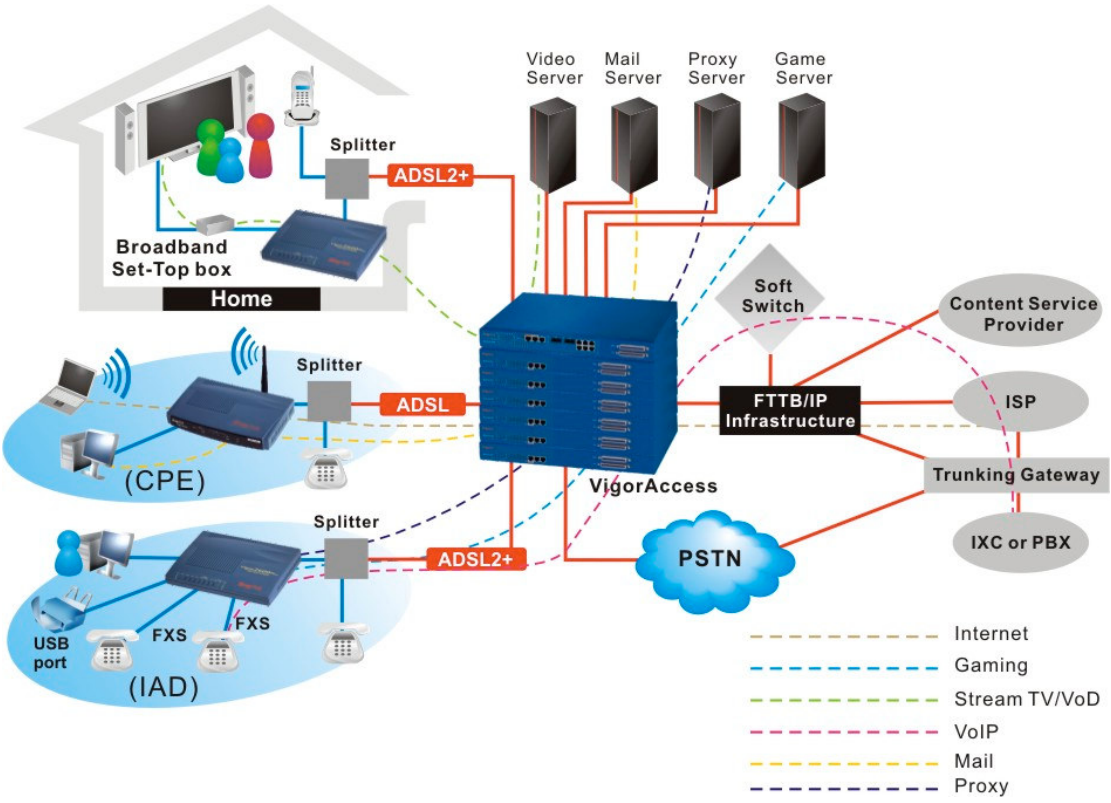


Figure 1-1. Application scenario of IP DSLAM

IP DSLAM is able to support enterprise customer with high-speed service request. Customers can subscribe multiple ADSL 2/+ lines by integrating security router with load balance feature. By combining VoIP devices, system integrator provides multiple services with VoIP, Video on Demand, and ADSL2/+ bundle solution.

The firewall and VPN security of VoIP security router is also provided by the architecture to meet business requirements. This application is suitable on Hotel and MTU applications. The entire system is managed by EMS system. Application scenario of IP DSLAM for enterprises is shown in Figure 1-2.

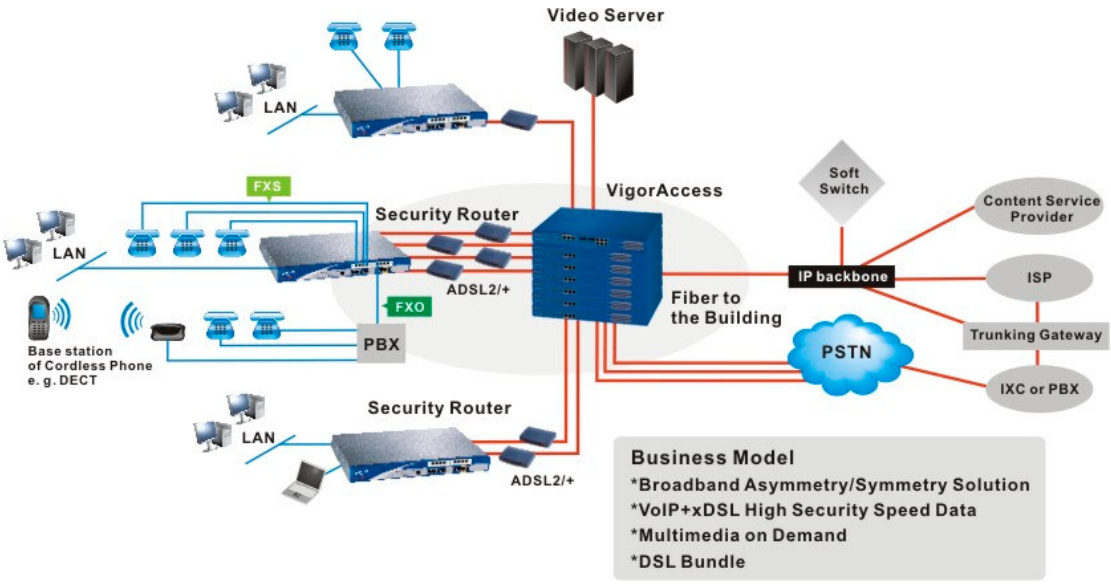


Figure 1-2. Application scenario of IP DSLAM for enterprises

1.2 Hardware Architecture

1.2.1 System Architecture Overview

The system architecture is shown in Figure 1-3. It has one Master to subtend up to 6 Slaves. The hardware interface of Master unit covers ARM relay, console, management with RJ45, Gigabits optical interface with SC connector, GE subtend interface with RJ45 connector, ADSL2/+ with RJ21 connector, and POTS with RJ21 connector. Users can connect the IP DSLAM slave to an subtend interface of Master, Ethernet WAN switch using a straight-through Category 5 UTP 8C8P cable with RJ-45 connectors. Then, connecting the other end of the cable to subtend interface, users can stack multiple IP DSLAM units up to the number of ports available on the Ethernet switch as shown in the following page.

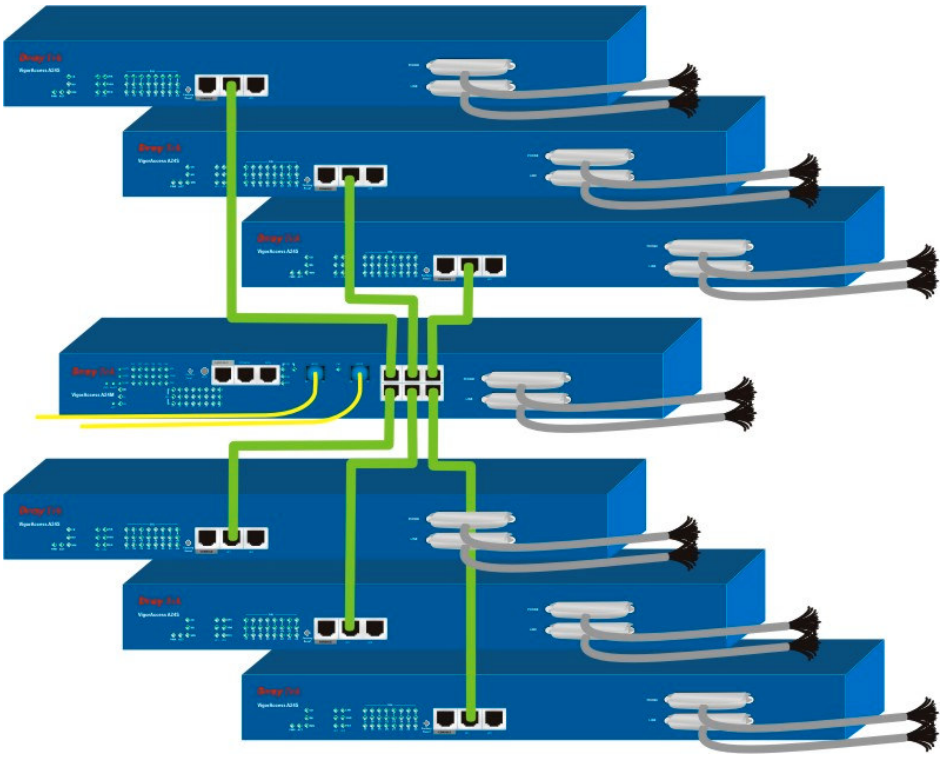


Figure 1-3. Stacking IP DSLAM architecture

1.2.2 Master Overview

The purpose of master unit is as a central unit in DSL application to manage all slave units connected with it. Master unit always collects related information from slave units. Moreover, users can manage slave units through master unit.
The picture of master unit is shown in Figure 1-4.

Figure 1-4. Master Device picture

Master unit supports some features as following –

Network Interface - The trunk should be 1000-Based LX, SX or GE Interface.

Cascade Interface - GE interfaces can be cascaded up to six IP DSLAM slave units.

Capacity – It supports ADSL 2/+ port range from 24 to 168 ports.

Security – It supports Packet filter, and password protection.

Splitter Build in – It supports 24-port xDSL/Splitter included module.

Redundancy – Optional uplink automatically switch of activity in the event of fiber failure.

Inventory savings - Common equipment across central office and outside plant deployments.

Management - Single IP Management.

Q.o.S - Packet filter and classification.

1.2.3 Slave Overview

The role of slave unit is to provide a high-performance; good services DSL feature in Internet environment. The picture of slave unit is shown in Figure 1-5.

Figure 1-5. Slave Device picture

A slave unit support some features is shown as follows –

Network Interface - Two 10/100M Fast Ethernet Interfaces or one Gigabit Copper interface for cascade link.

Capacity – It supports ADSL 2/+ 24 ports.

Security – It supports packet filter, and password protection.

Splitter Build in – It supports 24 port xDSL/Splitter included module.

Inventory savings - Common equipments across central office and outside plant deployments.

Management – It is managed by IP DSLAM master unit.

Q.o.S - Packet filter and classification.

1.3 Box Connections

1.3.1 Rack-Mounting the BOX

IP DSLAM can be installed on 19-, 23-inches racks by using standard brackets in 19-inch rack or optional larger brackets on 23-inch rack. The bracket for 19-, 23-inch racks are shown in Figure 1-6.

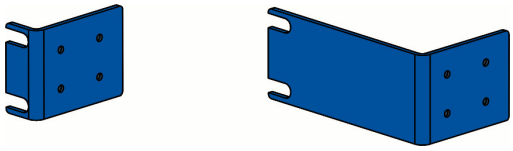


Figure 1-6. Brackets for 19-, 23-inch rack

Attach the brackets to the chassis in 19-, 23-inch rack as shown in Figure 1-7. The second bracket attaches the other side of the chassis as above procedure.

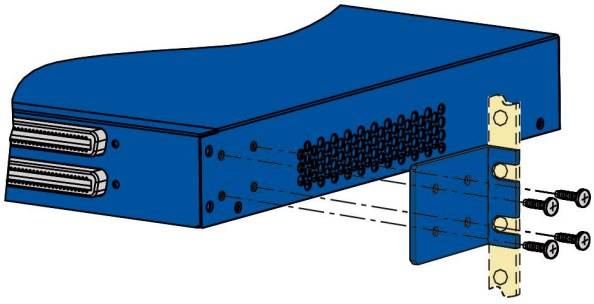


Figure 1-7. Bracket installation for Front mounting on 19-, 23-inch rack

1.3.1 Installing Chassis in Rack

After bracket installation, IP DSLAM chassis could be installed in the rack by using two screws for each side of rack.

1.3.2 Desktop Type Installation

Rubber feet in IP DSLAM package surports desktop installation. These rubber feet aims to improve the air circulation and at the same time decrease unnecessarily rubbing on desk.

1.3.3 Power, Ground Connections on the Rear Panel

The AC input and ground connections are on the rear panel and shown in Figure 1-8. You can connect the rack to ground by spring screws.

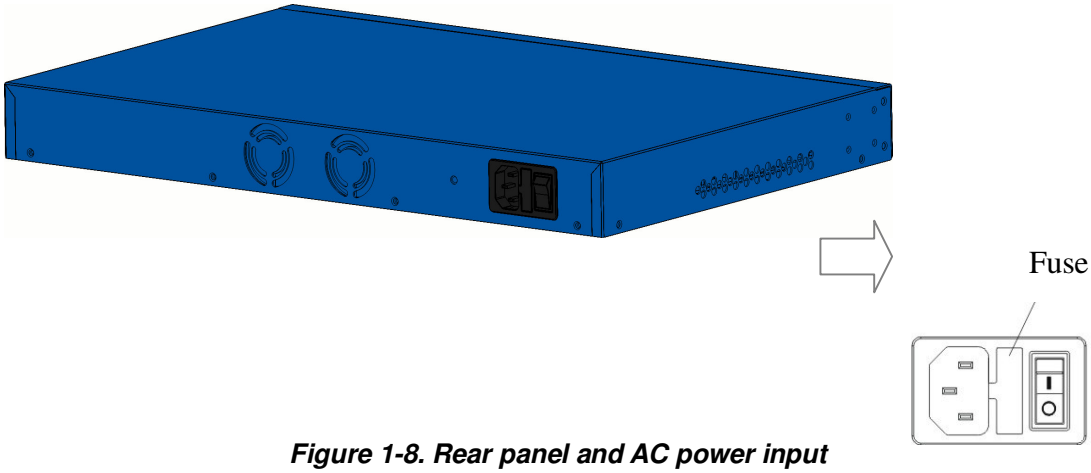


Figure 1-8. Rear panel and AC power input

The DC input and ground connections are on the rear panel and shown in Figure 1-9. You can connect the rack to ground by spring screws.

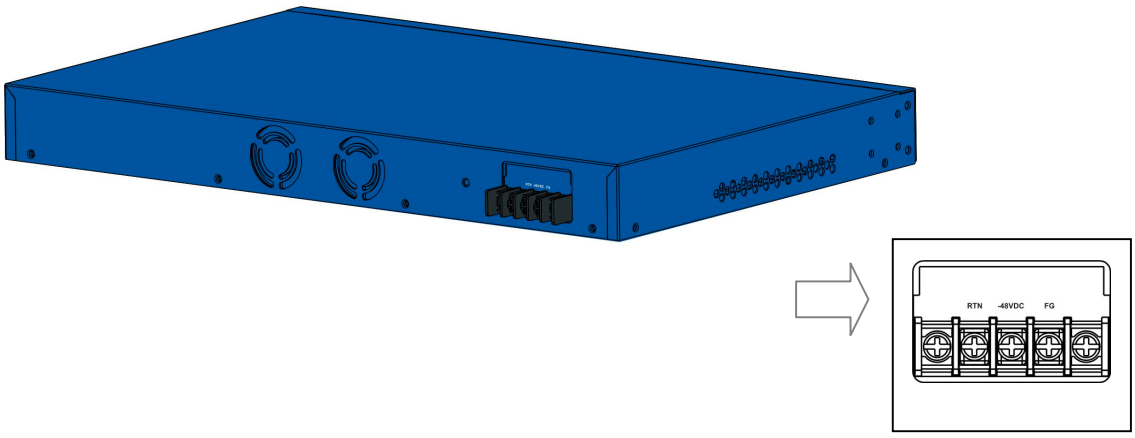


Figure 1-9. Rear panel and DC power input

1.4 Power Connection

1.4.1 AC Power Connection

Connect the female end of the power cord to the power socket on the rear panel of IP DSLAM as shown next. Connect the other end of the cord to a power outlet and make sure that no objects obstruct the airflow of the fans (located on the rear side of the unit).

1.4.2 DC Power Connection

There are following steps to setup DC power connection.

Step 1 Check and ensure that power in the DC source is OFF.
Step 2 Remove the cover of the DC power connector.
Step 3 Connect chassis ground to stud terminal labeled “FG”.
Step 4 Connect the power lead from the positive terminal of power source to the stud terminal labeled “RTN”.

Warning The Figure 1-10 shows the DC power supply terminal block. It is the lugs at the wiring end from the power source. The wiring procedure is for ground-to-ground, positive-to-positive, and negative-to-negative in order. The ground wire should always be connected first and disconnected last.

Step 5 Connect the power lead from the negative terminal of power source to the stud terminal labeled “(–) 48VDC”.

Step 6 put back the small plastic cover over the power terminals.

Step7 Check and turn on the power from power source. If the power is properly connected, a PWR green LED on the front panel of IP DSLAM lights up.

Figure 1-10. Rear panel and DC power input

1.5 ADSL Port Connection

1.5.1 MDF Connections (Main Distribution Frame)

The POTS splitter should be connected to MDF on building or CO side in Figure 1-11. An MDF is usually place in the building's telephony room or on central office room. It can terminate the outside telephone line into the building. Most MDF has surge protection feature to protect the equipment from damage. In general, The LINE and PHONE interface all connect to MDF and then to outside connection.

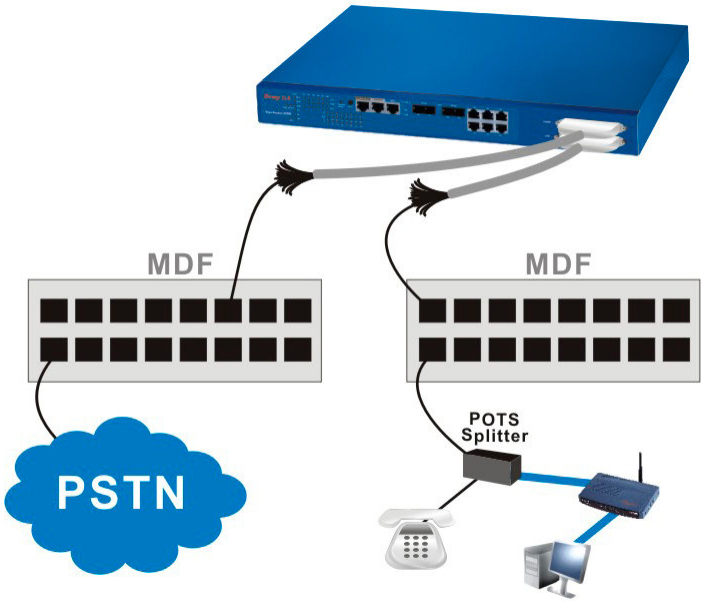


Figure 1-11. MDF connection architecture

1.5.2 Centric Patch Panel Connection

The IP DSLAM can provide ADSL and voice services over the same telephone wiring. It also has built in splitters internally that can save space and simplify installation.

If the application is using on building environment, the CPP (Centric Patch Panel) is preferred. The purpose of CPP module is to transfer RJ-21 jack in IP DSLAM to RJ-11 connector. The CPP front panels is shown in Figure 1-12. It is usually installed between end-users' equipment and telephone company in a basement or telephone room. The CPP is the point of termination for the outside telephone company lines coming into a building and the telephone lines in the building.

Figure 1-12. CPP front panels

The following figures give some examples of scenario for using IP DSLAM to combine voice and data signals.

The existing telephone wiring usually depends on user's region. Here are descriptions of two typical installation scenarios. Use telephone wires with RJ-11 jacks on one end for connecting to the CPP board.

1.5.2.1 Installation CPP Scenario A

Users can connect a cable from RJ-21 (LINE) attached in IP DSLAM to the CPP board. Then users can connect a RJ-11 jack port attached in a CPP to ADSL modem directly. The Data only CPP connection is shown in Figure 1-13.

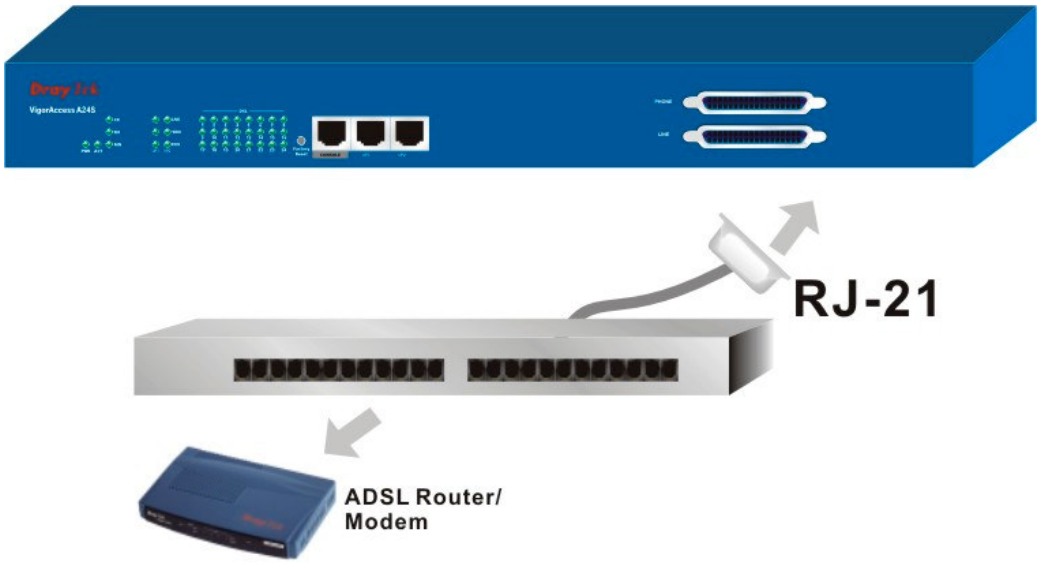


Figure 1-13. Data only CPP connection

1.5.2.2 Installation CPP Scenario B

Phone service is available in IP DSLAM. You can connect a RJ-11 jack port attached in a CPP to a telephone directly or applied in the same way shared in ADSL modem. The Data/Voice CPP connection is shown in Figure 1-14.

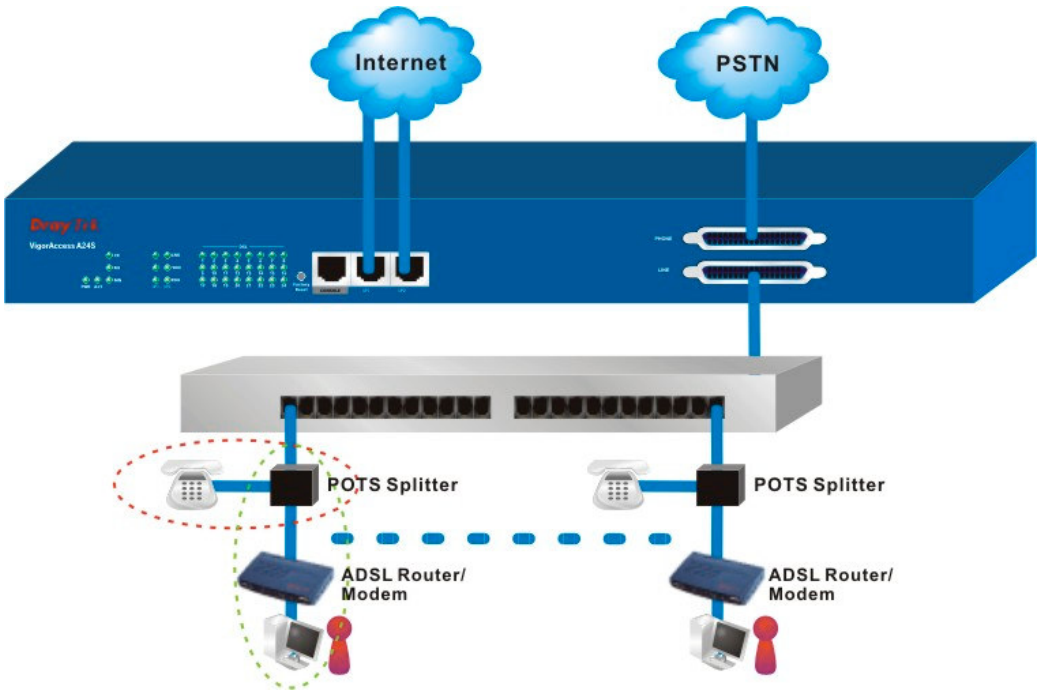


Figure 1-14. Data/Voice CPP connection

1.6 Connector and Interface Description

1.6.1 The RS232 Connector Description

The RJ45 connection jet is used for CLI commands for system configurations and controlling functions in the IP DSLAM. The jet is used for initialization of the IP DSLAM during the preliminary installation. The "management cable", as shown in Figure 1-15, converts the RJ45 to the RS232 interface. The RJ45 jet connects to a console interface in the IP DSLAM, while the RS232 DB9 connecting to a console port on the computer. The default setting of the console port is "**baud rate 9600, no parity, and 8 bit with 1 stop bit (N81)**".

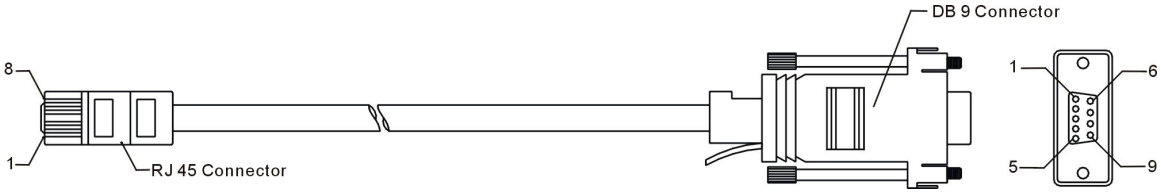


Figure 1-15. Console management cable

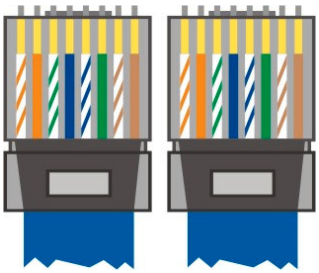
The pin-out for this connector is shown in Table 1-1 as follows.

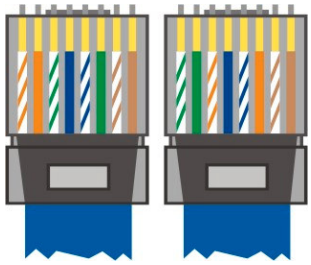
Table 1-1. The RS232 adaptor PINOUT

RJ45	DB9 (Female)	Signal
No connection	1	CD
3	2	TD
6	3	RD
7	4	DTR
5	5	GND
2	6	DSR
8	7	RTS
1	8	CTS
No connection	9	RI

1.6.2 Standard 10/100 Base-T Ethernet Interface Connector

RJ45 jets provide 10/100 Base-T Ethernet interfaces. The interface supports MDI/MDIX auto-detection of either straight or crossover RJ45 cables. These cables are used on UP1,UP2/MGN interfaces.





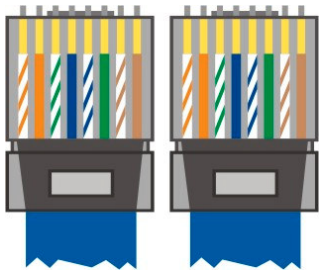
RJ-45 **Straight-through** Cable Pin-outs			
Signal	Pin	Pin	Signal
Tx+	1	1	Tx+
Tx-	2	2	Tx-
Rx+	3	3	Rx+
--	4	4	--
--	5	5	--
Rx-	6	6	Rx-
-	7	7	-
-	8	8	-

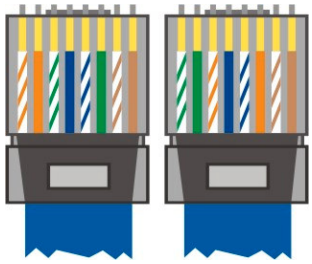
RJ-45 **Crossover** Cable Pin-outs			
Signal	Pin	Pin	Signal
Tx+	1	1	Rx+
Tx-	2	2	Rx-
Rx+	3	3	Tx+
--	4	4	--
--	5	5	--
Rx-	6	6	Tx-
-	7	7	-
-	8	8	-

Figure 1-16. Applicable on both straight-through and crossover RJ45 cables overview

1.6.3 Standard 10/100/1000 Base-T Ethernet Interface Connector

RJ45 jets provide 8P8C 10/100/1000 Base-T Ethernet interfaces. The interface supports MDI/MDIX auto-detection of either straight or crossover RJ45 cables. These cables are used on GE interfaces for subtending connection on Master and UP1, UP2/MGN port on Slave.





RJ-45 **Straight-through** Cable Pin-outs (8P8C)			
Signal	Pin	Pin	Signal
TP0+	1	1	TP0+
TP0-	2	2	TP0-
TP1+	3	3	TP1+
TP1-	6	6	TP1-
TP2+	4	4	TP2+
TP2-	5	5	TP2-
TP3+	7	7	TP3+
TP3-	8	8	TP3-

RJ-45 **Crossover** Cable Pin-outs (8P8C)			
Signal	Pin	Pin	Signal
TP0+	1	1	TP1+
TP0-	2	2	TP1-
TP1+	3	3	TP0+
TP1-	6	6	TP0-
TP2+	4	4	TP3+
TP2-	5	5	TP3-
TP3+	7	7	TP2+
TP3-	8	8	TP2-

Figure 1-17. Applicable on both straight-through and crossover RJ45 (8C8P[1]) cable

[1] *8C8P means the Ethernet cable with 8 wires connector in 1000M Ethernet physical ports.*

1.6.4 Optical Giga Ethernet Interface as Trunk Interface with SC Connector

The trunk interface is made with the SC connector, which is available in two types:

- Gigabits Ethernet optical long haul LX single mode interface.
- Gigabits Ethernet optical short haul SX multimode interface.

For each type of optical transceiver, they should connect with corresponding optical fiber with proper mode. Incorrect fiber mode may affect link distance or even link fail.
Fiber for long haul LX: Single-mode (SM), 9/125 micron.
Fiber for short haul SX: Multi-mode (MM), 50/125 or 62.5/125-micron.

The two types of interface are visually and functionally similar. Installation procedures are the same. This dual port has both connectors on transmit (upstream) and a receiving (downstream) as shown in Figure 1-18. There are warnings for the optical fiber connection.

Warning

- The laser energy of the fiber optic communication channels in the single-mode will be harmful when operate, especially to the eyes. During normal operation with cable connection, this energy is confined to the cable with no danger present.
- Because the laser radiation is invisible and may be emitted from the aperture of the port before connect the cable or protective cap, please avoid exposure to laser radiation and also do not fix the gaze to open apertures.
- The following precautions are to avoid injury when connecting or disconnecting optical channel.
- Always connecting optical cables before power on.
- Always keep the protective cap on the optic connector.
- Never stare into an optical cable or connector when the connector is not in use.

Connect the fiber channel using the following steps:

Step 1 Read and understand the previous warnings and alarm.

Step 2 Remove the protective caps from the fiber optic connector and from the external data cable.

Step 3 Attach the external cable to the recessed connector on the faceplate as shown on Figure 1-18.

Step 4 To avoid exposure to laser radiation by plug the protective cap. Store protective cap on the clear place to use when no optical fiber connection or on stock.

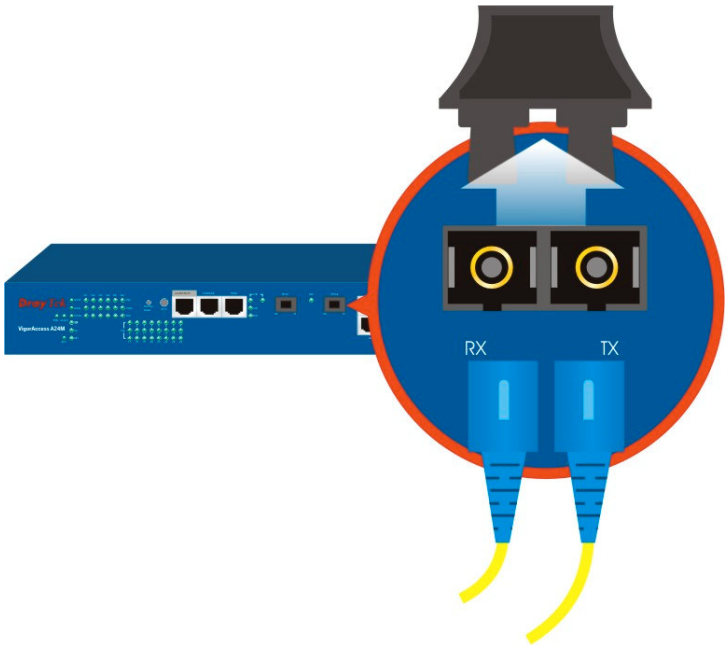


Figure 1-18. The optical uplink (SC type) trunk cable connection

1.6.5 RJ21 DSL and Phone Connector

Connections are made with two 50-pin champ cables (Figure 1-19) that are attached to the RJ21 interface on IP DSLAM. Each cable terminates with a 50-pin Telco straight champ connector. Refer to Table1-2 for cable pin assignments between the Line and the POTS splitter.

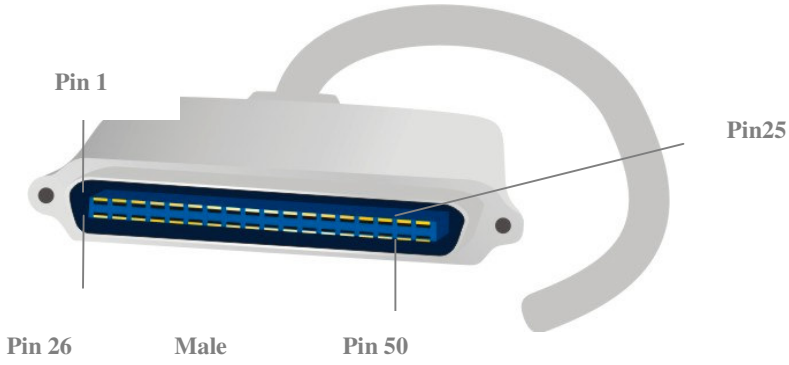


Figure 1-19. The RJ21 champ cable connection

Table 1-2. RJ21 Cables Pin assignment

Pin Number	Wire Color	TIP/RING	Port Number	Pin Number	Wire Color	TIP/RING	Port Number
26 1	White/blue Blue/white	TIP RING	1	38 13	Black/green Green/black	TIP RING	13
27 2	White/orange Orange/white	TIP RING	2	39 14	Black/brown Brown/black	TIP RING	14
28 3	White/green Green/white	TIP RING	3	40 15	Yellow/blue Blue/yellow	TIP RING	15
29 4	White/brown Brown/white	TIP RING	4	41 16	Black/gray Gray/black	TIP RING	16
30 5	White/gray Gray/white	TIP RING	5	42 17	Yellow/orange Orange/yellow	TIP RING	17
31 6	Red/blue Blue/red	TIP RING	6	43 18	Yellow/green Green/yellow	TIP RING	18
32 7	Red/orange Orange/red	TIP RING	7	44 19	Yellow/brown Brown/yellow	TIP RING	19
33 8	Red/green Green/red	TIP RING	8	45 20	Yellow/gray Gray/yellow	TIP RING	20
34 9	Red/brown Brown/red	TIP RING	9	46 21	Violet/blue Blue/violet	TIP RING	21
35 10	Red/gray Gray/red	TIP RING	10	47 22	Violet/orange Orange/violet	TIP RING	22
36 11	Black/blue Blue/black	TIP RING	11	48 23	Violet/green Green/violet	TIP RING	23
37 12	Black/orange Orange/black	TIP RING	12	49 24	Violet/brown Brown/violet	TIP RING	24
				50 25	Violet/gray Gray/violet	TIP RING	25 is dummy

1.6.6 Alarm Relay RJ45 Connector

RJ45 jets provide connection with an external alarm device to the alarm relay connector, Table 1-3 lists the pin assignments for backplane connector RJ45, the alarm relay connector. The alarm relays provide relay contact closures. If you connect the alarm relays, they transmit critical, major, and minor alarms to a separate, external alarm device. The alarm device uses a bell, light, or some other signal to alert people to the change in status. The alarm relay connector also provides one set of contacts for audible alarms and one set for visual alarms. The maximum contact rating is 30VDC, 2A 125VDC, 0.5A.

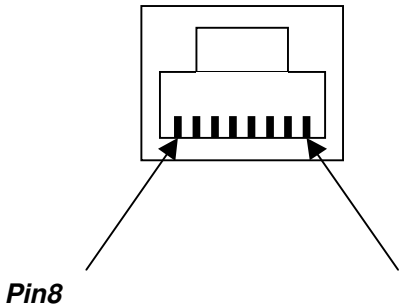


Figure1-20. Alarm Relay RJ45 connector front

Table 1-3. Pin assignments for the Alarm Relay connector

pin	Signal	Description
1	NC1	(NORMAL CLOSE CONTACT GROUP1)
2	COM1	(COMMON CONTACT GROUP1)
3	NO1	(NORMAL OPEN CONTACT GROUP1)
4		NOT USED
5		NOT USED
6	NC2	(NORMAL CLOSE CONTACT GROUP2)
7	COM2	(COMMON CONTACT GROUP2)
8	NO2	(NORMAL OPEN CONTACT GROUP2)

CHAPTER 2
Installation

In this chapter, we will introduce the installation, cable type, and LED indications in IP DSLAM.

This chapter is divided into the following sections,

- Section 2.1: System Connection Description
- Section 2.2: IP DSLAM Master Setup
- Section 2.3: IP DSLAM Slave Setup

2.1 System Connection Description

There are following steps to setup the IP DSLAM connection:

Master rack-mounting setup
Slave rack-mounting setup
Interconnect master and slaves
Line interface connection
Phone interface connection

After the previous steps, the system will construct as shown in Figure 2-1.

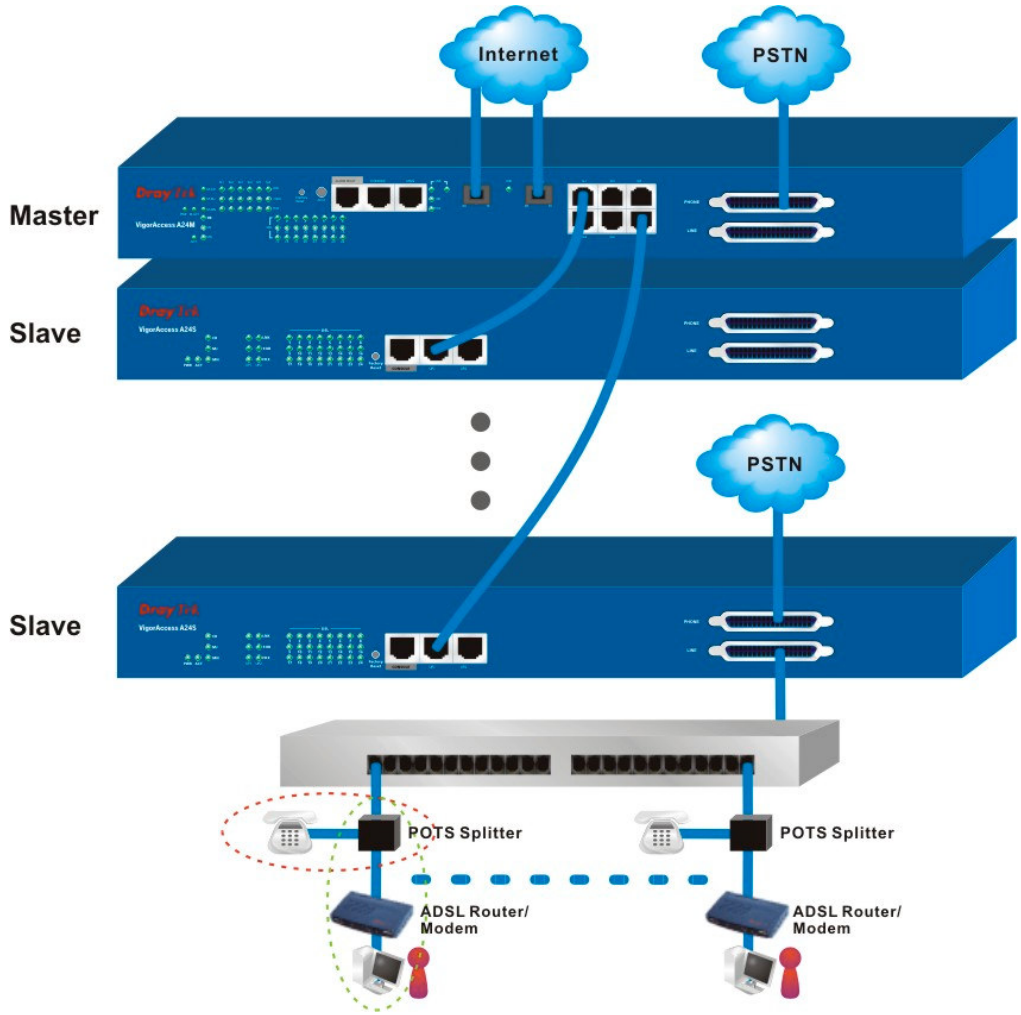


Figure 2-1. IP DSLAM network connection

2.2 IP DSLAM Master Setup

2.2.1 Master Front Panel Connection

All connections are made on the front panel of the IP DSLAM except power connector. The connections on the front panel of the IP DSLAM are shown in Figure 2-2. There are interfaces on Mater front panel.

Factory Reset – A reset button is used to reset system, and then IPDSLAM will operate by default configuration.

Alarm Relay – An alarm relay with RJ45 interface can connect to buzzer when the FAN is out of order.

Console – A RS232 serial interface is used to connect a local management computer.

MGN – A management interface with RJ45 interface is for Telnet management. Users can set local PC (personal computer) as the same subnet as IP DSLAM and to manage IP DSLAM by CLI command.

UPLINK – The uplink interface with SC connector should be long haul or short haul Gigabits optical connection.

Subtend – The subtend interface with RJ45 interface is Gigabit Ethernet connection; There are six interfaces to subtend six slaves to expend DSL capacity.

PHONE – Connected to PSTN normally.

LINE – Connected to twist pair of subscriber line which connects ADSL devices or telephones for users.

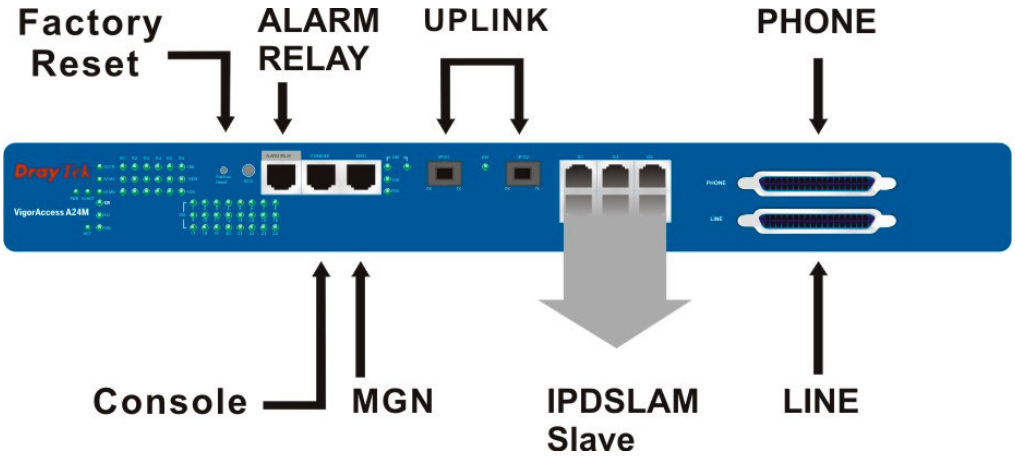


Figure 2-2. IP DSLAM master interface on front panel

From Figure 2-2, we can see that the IP DSLAM series has a lot of interfaces. The following section briefs these interface connection.

Table 2-1. IP DSLAM master connection

Port	Type, Color	Connected to	Remarks
Power Cord	Cord, Black Wire,	AC Outlet/ DC Outlet	100-240VAC -42 ~ 56VDC
Factory Reset		Push Bottom for Default Setting	
ACO		Push Bottom for reset alarm	
Alarm Relay	RJ45 connect to Buzzer	ALM Relay connection	
Serial (Console)	RS232, Grey	PC RS232 port for CLI	--
Uplink1 (Optical)	SC, Yellow/orange	Gigabits Fiber Optical Interface Interconnection	--
MGN	RJ-45, Blue	PC Ethernet Interface	
Gx	RJ-45 (8P8C), Blue	Connect to slave unit (UP1)	
PHONE	RJ-21,	MDF or Panel to PSTN	
LINE	RJ-21,	To subscriber copper line	

2.2.2 Master Console Port Connection

For the initial configuration, users need to use terminal emulator software on a computer and connect it to a network module through the console port. Users can connect the RJ-45 end of the console cable to the console port of the network module. On the other side, users can connect the other end to a serial port of a computer.

The default login is "**admin**", password is "**1234**"

```
**********************************************************
*                    Bootloader Version: V1.0.7                    *
**********************************************************
Press [ENTER] key within 5 sec. to download image...0
Please wait a minute...
Login:
```

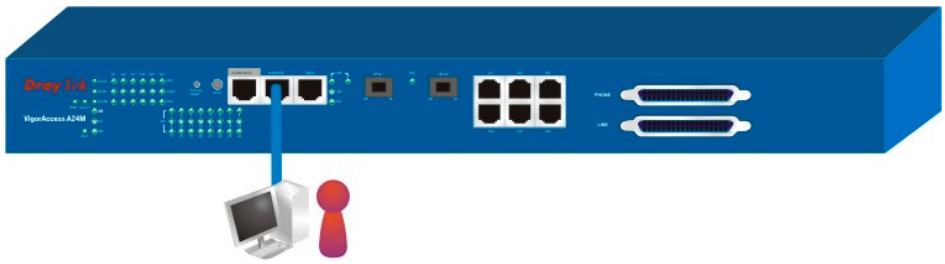


Figure 2-3. Master console port connection

2.2.3 Master Management Port Connection

Users can connect the RJ-45 cable to the Ethernet port of the computer. The IP address is 172.16.1.1 by default. The subnet of PC should be the same as default IP setting.

Admin> network outband

OUTBAND INTF CONFIGURATION

IP Address : 172.16.1.1
NetMask : 255.255.255.0
Vlan Id : 0

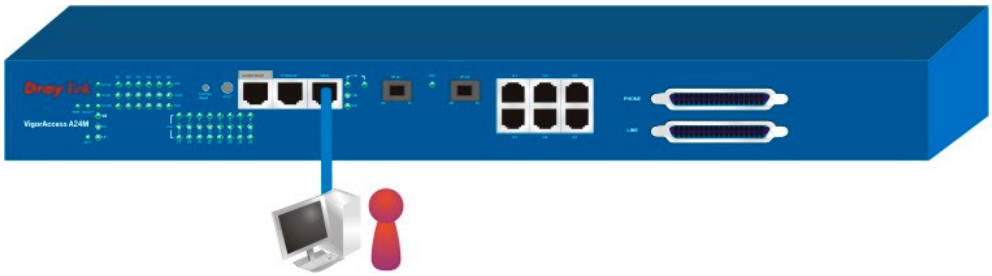


Figure 2-4. Master management port connection

2.2.4 Maser Subtend Port Connection

Users can connect the uplink of IPDSLAM Slave to subtend interface of IPDSLAM Master by plug and play.

Admin> dsl -m

Press 'exit' to return
Entering character mode
Escape character is '^]'.

[dsl-master]#

or

Admin> dsl -s <n>

Press 'exit' to return

Entering character mode
Escape character is '^]'.

[dsl-slave-n]#

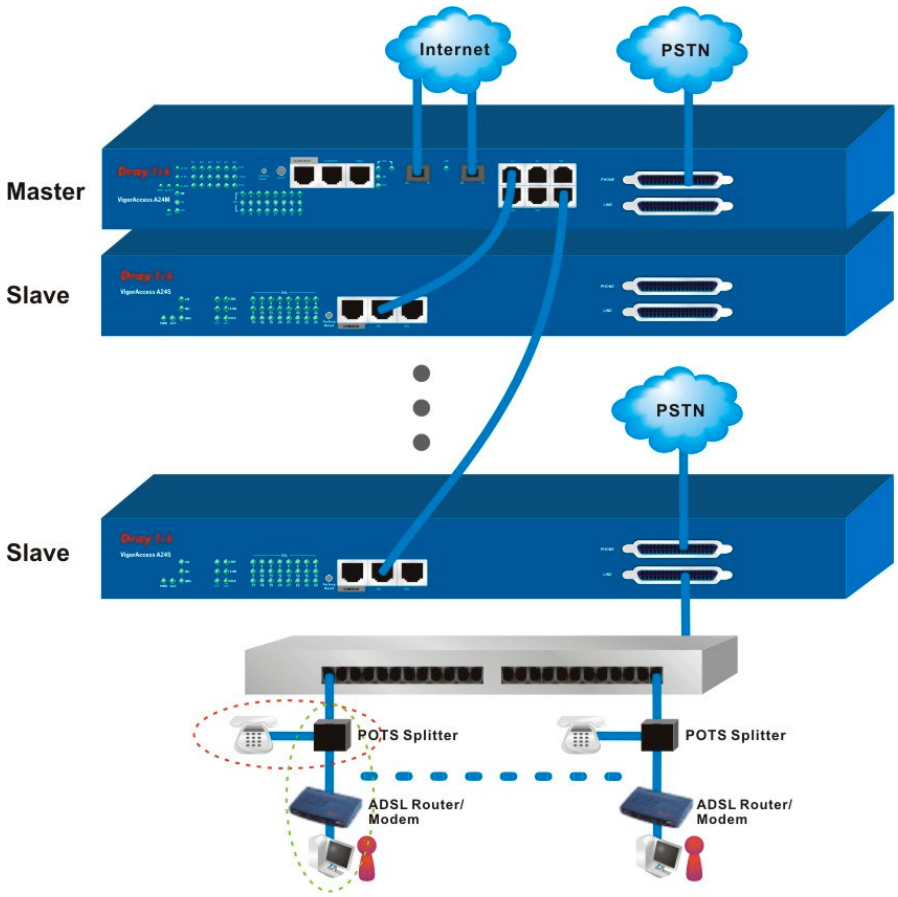


Figure 2-5. Master subtend connection

2.2.5 Master LED Indication

After completing the interface connection and power on the units, users can inspect the LED on the front panel. The Master is consisted of two parts of features. One is controller for alarm, subtend and optical feature. The others are DSL feature. The status of these features is shown in Table 2-2.

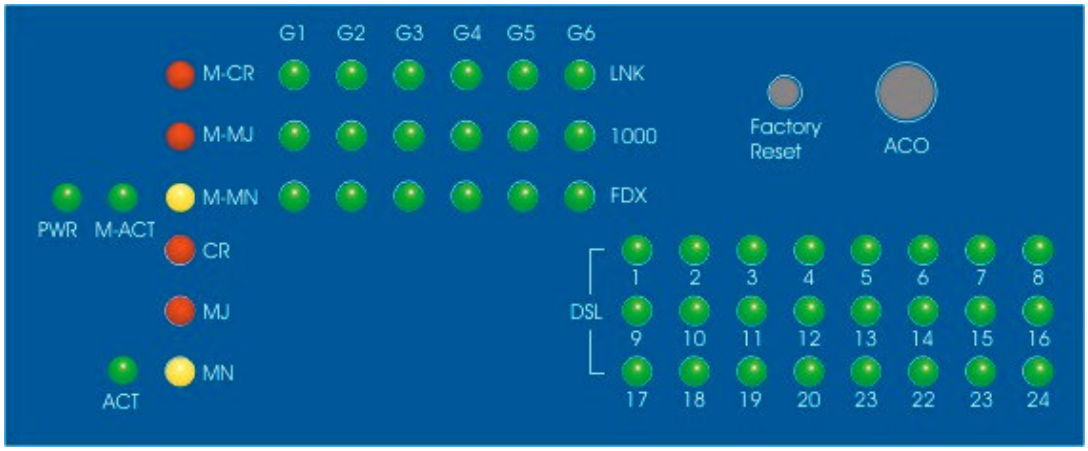


Figure 2-6. Master subtend connection

Table 2-2. IP DSLAM master DSL LED descriptions

PWR		Green	The Power LED is on when Power is applied.
		OFF	The Power is not applied.
M_ACT		Green	Blink when Master is active.
		OFF	OFF when system is hanged.
M_CR		Green	Master critical alarm is present.
		OFF	No critical alarm is present to system.
M_MJ		Green	Master Major Alarm is present.
		OFF	No major alarm is present to system.
M_MN		Green	Master Minor Alarm is present.
		OFF	No minor alarm is present to system.
Gx	LNK	Green	Subtend interface by GE Interface. Green when Ethernet link is established Blinks during data transmitting/receiving.
		OFF	OFF means No Ethernet link established.
	1000	Green	The speed for Ethernet is 1000Mbps when LNK LED is ON.
		OFF	The speed for Ethernet is 10/100Mbps when LNK LED is ON.
	FDX	Green	The Ethernet is in full duplex mode when LNK LED is ON.
		OFF	The Ethernet is in half duplex mode when LNK LED is ON.
ACT		Green	Blink: DSL board is Active.
		OFF	OFF or solid ON when system is inactive.
CR		Red	DSL critical alarm is present.
		OFF	No critical alarm is present to system.
MJ		Red	DSL Major Alarm is present.
		OFF	No major alarm is present to system.
MN		Yellow	DSL Minor Alarm is present.
		OFF	No minor alarm is present to system.
DSLx		Green	The DSL x Port link status is Up.
		Blinking	The DSL link is training.
		OFF	The DSL x Port link status is down.

2.3 IP DSLAM Slave Setup

2.3.1 IP DSLAM Slave Front Panel Connection

All connections are made on the front panel of the IP DSLAM except power connector. The following figure shows the connections on the front panel of the IP DSLAM.

Factory Reset – A reset button is used to reset system, and then IPDSLAM will reboot to factory default configuration.

Console – A RS232 serial interface is used to connect a local management computer.

UPLINK (UP1, UP2, MGN) – Support two 10/100M or one 1000M Ethernet ports to Internet MGN - 10/100M Ethernet ports. The interface can be used as for Telnet management. Users can set local PC (personal computer) as the same subnet as IP DSLAM and to manage IP DSLAM by CLI command.

PHONE – Connected to PSTN normally.

LINE – Connected to ADSL devices or telephones for users.

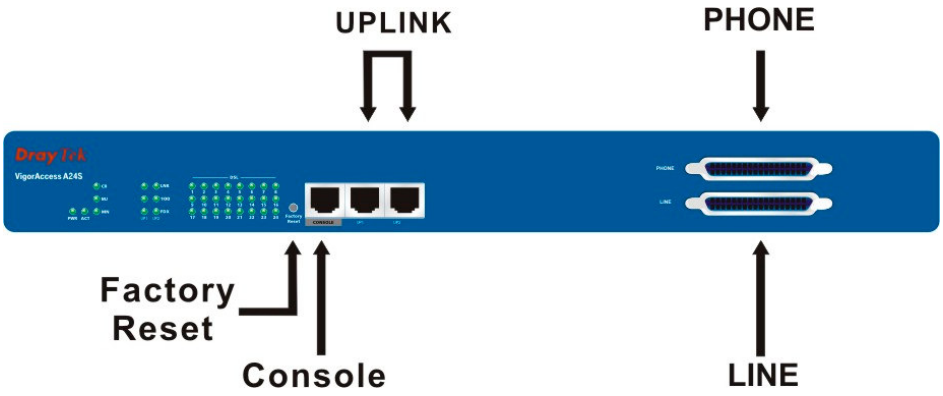


Figure 2-7. IP DSLAM slave front panel connections overview

Table 2-3. IP DSLAM slave connections

Port	Type, Color	Connected to	Remarks
Power Cord	Cord, Black Wire with lug terminal	AC Inlet DC Inlet	100-240VAC -42 ~ 56VDC
Serial (Console)	RS232, Grey	Connect to PC RS232 port for debug	--
Ethernet (UP1, UP2, or MGN)	RJ-45, Blue	Uplink interface to connect to Master subtend interface or to PC for management	
PHONE	RJ-21,	To PSTN	
LINE	RJ-21,	To subscriber copper line	

2.3.2 IP DSLAM Slave Console Port Setup

For the initial configuration, users need to use terminal emulator software on a computer and connect it to a network module through the console port. Users can connect the RJ-45 end of the console cable to the console port of the network module. On the other side, users can connect the other end to serial ports of a computer.

$help

Command	Description
-------	-----------
alias	To alias a command
commit	Commit the active configuration to the flash
create	Create a new entry of specified type
delete	Delete the specified entry
download	Download a file on to the Device
exit	To exit the CLI shell
get	Display info for the search
help	Provides help
modify	Modify information for specified entry
passwd	To modify user password
ping	The normal ping command
prompt	Change the user prompt
reboot	Reboot the device
reset	Reset info for the specified entry
traceroute	The normal traceroute command
unalias	To undefine previously defined alias
verbose	Switch ON/OFF the verbose mode

apply	Apply configuration/image file
list	List files
remove	Remove file
rdm	Read memory
rdf	Read flash
wrm	Write memory
memset	Memset
upgrade	Upgrade
upload	Upload a file on to the Device
<wizard>	A shortcut, Type 'wizard' for help

Figure 2-8. IP DSLAM slave console port connection

2.3.3 Slave Management Port Connection

The IP address is auto-configured from Master once the Slave is connected to any subtend port of Master.

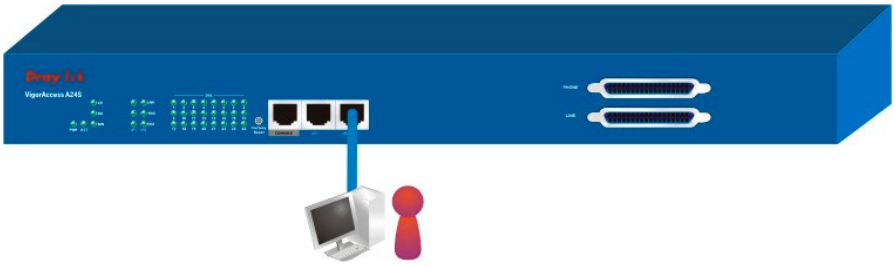


Figure 2-9. IP DSLAM slave management port connection

2.3.4 Line Interface Connection

IP DSLAM supports two RJ-21 interfaces with 24 ports DSL connection. One is "PHONE"; the other is "LINE". In general, the interface of "PHONE" is connected to PSTN. The interface of "LINE" is connected to ADSL CPE or telephone by copper wire. Users on CPE can connect into Internet for browsing Web or accessing emails and using traditional telephony services simultaneously. The "LINE" interface connection is shown in Section 1.5.

2.3.5 Slave LED Indication

After complete the interface installation, users can complete the connections by only 4 steps.

First, connect the power cord in the rear part of IP DSLAM to AC inlet or DC power source. As a result, the PWR LED will be lit.

Second, after system self testing is completed, the ACT LED will begin to blink. Then connects one of two uplink ports of IP DSLAM with a blue RJ-45 cable, and the UP1 or UP2 LED will blink.

Furthermore, IP DSLAM provides signal LED for CR (Critical), MS (Major Alarm), MN (Minor Alarm) and 24 ADSL ports. All these LEDs are depicted in Figure 2-10 and the function of each LED has been described in Table 2-4.

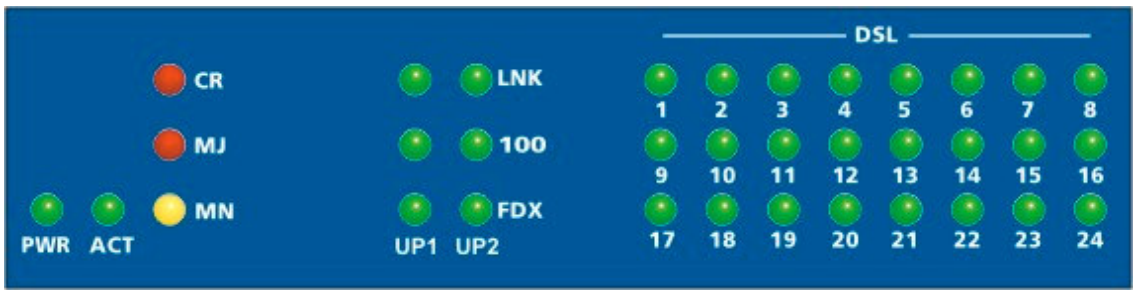


Figure 2-10. Slave LED indication

Table 2-4. IP DSLAM front panel LED and description

LED		Indication	Description	Remarks
PWR		Green	Power ON	100-240VAC/ -42V ~ 56VDC
		OFF	Power OFF	
ACT		Green	Blink when system is active	
		OFF	When System is inactive	
UP1/UP2 /MGN	LNK	Green	Ethernet link is established	
		OFF	No Ethernet link established	
		Blinking	Packets in incoming/outgoing	
	100	Green	The speed for Ethernet is 100M,when LNK LED is ON	
		OFF	The speed for Ethernet is 10M when LNK LED is ON	
	FDX	Green	The transmitted mode for Ethernet is in full duplex mode when LNK LED is ON	
		OFF	The transmitted mode for Ethernet is in half duplex mode when LNK LED is ON	
CR		Red	Critical Alarm is active	
		OFF	Critical Alarm is not active	
MJ		Red	Major Alarm is active	
		OFF	Major Alarm is not active	
MN		Yellow	Minor Alarm is active	
		OFF	Minor Alarm is not active	
DSL		Green	DSL link is established	1~24
		Blinking	The DSL link is training	
		OFF	DSL link is not established	

CHAPTER 3
IP DSLAM Product Feature

This chapter is divided into the following sections,

- Section 3.1: Introduction
- Section 3.2: Quality of Service (QoS)
- Section 3.3: Security
- Section 3.4: Packet Filtering
- Section 3.5: ATM Features
- Section 3.6: Miscellaneous

3.1 Introduction

The IP DSLAM (Integrated Ethernet Switch) is an IP-based DSLAM (Internet Digital Subscriber Line Access Multiplexer) that connects to 24 ADSL subscribers to the Internet. When deployed together with DSL modems and WAN routers, the combination forms are integrated solution for providing broadband services to multiple tenants such as apartments, hotels, offices and campus buildings. IP DSLAM supports a lot of features as listed below.

ADSL Access Module
The name marked "**Line**" on the front panel is a RJ-21 connector integrated 24 ADSL ports internally. It aggregates traffic from 24 lines to Ethernet port(s) and has integrated splitters to allow voice and ADSL to be carried over the same phone line wiring.

10/100 Mbps Auto-negotiating Ethernet Port
IP DSLAM supports two 10/100/1000 Mbps auto-negotiate Ethernet ports connects to an Ethernet network. It can be aggregated together as a logical port as the backbone, and provide ADSL service to lots of subscribers.

ADSL Compliance

- Multi-Mode ADSL standard
- G.dmt (ITU-T G.992.1)
- G.dmt.bis (ADSL2, G.992.3)
- G.dmt.bisplus (ADSL2plus, G.992.5)
- G.lite (ITU-T G.992.2)
- G.hs (ITU-T G.994.1)
- ANSI T1.413 issue 2

Ethernet Bridging

There are three features supported for bridge function.

- IEEE 802.1d STD transparent bridging
- Up to 4000 MAC entries address table
- Port-based VLAN

IEEE 802.1Q Tagged VLAN

IP DSLAM uses the IEEE 802.1Q Tagged VLAN; users can allow this device to deliver tagged/untagged frames in these ports. The IP DSLAM supports up to 512 VLAN groups and can be applied up to 4094 VLAN identifications.

IEEE 802.1p Priority

IP DSLAM supports IEEE 802.1p to assign priority levels to all individual ports. Users can set different quality of service for individual application.

For example, voice and video services can set high priority and Internet data service will be lower priority.

- Support 4 queues for per ATM port.
- Support 8 queues for per physical Ethernet port.

MAC Address (Media Access Control) Filter

IP DSLAM can let users use the MAC filter for incoming frames based on MAC (Media Access Control) addresses that specified by users. Users can enable/disable this function on specific port.

- Access Control List per port is up to 8 entries. If port receives a packet which source MAC address is met with one of the 8 entries, this packet can be forwarded to destination port.

- Access Control List per device is up to 1024 entries. If port receives a packet which source MAC address is met with one of these entries, this packet would not be forwarded to destination port.

The high priority of ACL rules is the allowing rule checking for per port.

MAC Address (Media Access Control) Count Filter

IP DSLAM supports users to limit the number of MAC addresses that may be dynamically learned or statically configured on a port. Users can enable/disable this function on individual ports.

The global static learning table has up to 512 entries. Each entry can be set to a specific port. In dynamic learning mode, there are 16 MAC address entries in DSL port and 256 entries in Ethernet uplink port.

Multi-Protocol Encapsulation

IP DSLAM supports multi-protocol encapsulation over ATM adaptation Layer 5 based on RFC2684.

Management

IP DSLAM supports some management method as listed below.

- Remote configuration backup/restore via EMS client/server.
- Remote firmware upgrade
- SNMP management
- Command Line Interface, it can be accessed by local Console or Telnet interface.

Multiple PVC on single port

IP DSLAM allows you to use different virtual connection also called PVC (Permanent Virtual Circuits) for different services or subscribers. Users can define up to 8 connections on each DSL port for different services or levels of service, and users can assign different priority for each connection.

IGMP Snooping

IGMP (Internet Group Management Protocol) snooping reduces multicast traffic for maximum performance. The feature is very popular for video multicast application for example IPTV service.

3.2 Quality of Service (QoS)

Quality of Service (QoS) refers to the capability of a network to provide better service to select network traffic over various technologies. The primary goal of QoS is to provide priority including dedicated bandwidth, controlled jitter and latency (required by some real-time and interactive traffic), and improved loss characteristics. Also it is important to make sure that providing priority for one or more flows does not make other flows fail. QoS technologies provide the elemental building blocks that will be used for future business applications in campus, WAN and service provider networks.

3.2.1 Prioritized Bridging

IP DSLAM supports for multiple queues per port. There are different queues both on ATM and Ethernet uplink.

- Four queues supported per ATM port.
- Eight queues supported per physical Ethernet port.

3.2.2 Scheduling Mechanisms

IP DSLAM supports multiple scheduling mechanisms.

- Strict Priority Scheduling
- Probabilistic Priority Scheduling

3.2.3 Rate Limiting

IP DSLAM supports rate-limiting function in input/output both direction.

- Input Rate Limiting (IRL) on a per-AAL5 interface.
- Output Rate Limiting (ORL) on a per ATM-port basis
- Output Rate Limiting (ORL) on a per-physical Ethernet Interface basis.

One feature supports for buffer admission control triggered using IRL. Moreover, it also supports for dynamic modification of ORL on ATM and Ethernet interfaces.

3.2.4 Mapping Table

IP DSLAM supports a packet priority to traffic class mapping table supported on a per egress bridge port.

3.2.5 Multiple Mechanisms

IP DSLAM supports two multiple mechanisms as below.

- Multiple mechanisms of prioritizing incoming traffic are based on a per-bridge port.

(1) Using Source Port configuration (for untagged packets)
(2) Using Packet Classifier actions
(3) Using priority regeneration table (mapping ingress priority to egress priority)
(4) Combination of the above

- Multiple mechanisms of 802.1p re-tagging of outgoing traffic is based on a per ingress bridge port.

(1) Using Source Port configuration (for untagged packets)
(2) Using Classifier actions
(3) Using priority regeneration table (mapping ingress priority to egress priority)
(4) Combinations of the above

3.2.6 Abilities

IP DSLAM can be able to create multiple scheduling profiles, either Strict Priority or Probabilistic Priority. It also can be able to share the same profile across multiple (similar) ports.

3.3 Security

IP DSLAM supports some different methods to implement this feature in following sections.

3.3.1 Rate Limitation

IP DSLAM supports a function for throttling flooded packets. Users can configure some limited rates by per-port.

3.3.2 Static Mac Address

IP DSLAM supports this feature to be configured with certain ports to learn MAC addresses on a semi-permanent basis. These learned entries would be treated similar to the static entries, but will not be subject to aging or overwriting. These only may be deleted explicitly by management or by making the ports, as non-static after aging will happen normally.

3.3.3 FDB Conflicting Traps

IP DSLAM will transmit a trap packet to central manager when any MAC address moves from one port to another port.

3.3.4 MAC Address Tracking

IP DSLAM can be configured to track a global list of MAC addresses. When these MAC addresses move from one port to another port, a trap is generated. Whether packets from a particular bridge port should be subjected to this tracking is configurable. This may be used to prevent denial of service from certain MAC addresses.

3.3.5 Access Control List by MAC address

This feature can be configured by per-port. It also supports a MAC address deny list, the application of the MAC address deny list can be enabled/disabled on a per bridge port basis.

3.3.6 Access Control List by IP Address

This feature still can be configured by per-port, and enabled/disabled on a per bridge port basis.

3.4 Packet Filtering

This function is provided for users to setup some rules to filter the specific packets while receiving packets from logical ports.

IP DSLAM supports for rule-based packet filtering, it can be used to implement filtering required of NetBeui, NetBIOS, DHCP, 802.1x and other protocols.

3.4.1 Filtering Modes

IP DSLAM supports for independent rule ordering and rule ID. It means that rule ID no longer determines the order in which the rule is applied. The rule can be modified easily; users can replace a rule sequence of a stage on an interface by another sequence in one step.

Moreover, IP DSLAM also supports for capturing unicast and multicast packets that fail lookup in the forwarding database is provided. Users may write their own applications to terminate and act on this information. On the other side, it also supports for capturing packets coming to Control Plane that do not match any registered filter.

3.4.2 Classifier Tree

IP DSLAM provides tree architecture for classification. This tree is now configurable as a generic filter sub-rule.

3.4.3 Multiple Filter Stages

IP DSLAM supports a concept of multiple filter stages are provided for ingress and egress filter rules. Moreover, IP DSLAM supports an Egress filtering for unicast, broadcast and multicast traffic. It also supports multiple actions configurations by per filter rule.

3.5 ATM Features

IP DSLAM supports some functions about ATM issue.

3.5.1 Remote CPE Management

IP DSLAM supports RAW AAL5 interface for remote CPE management.

3.5.2 Diagnostic Testing

IP DSLAM supports OAM-I.610 end-to-end and segment loop back and DELT.

3.5.3 Dynamic Modification

IP DSLAM supports a lot of dynamic modifications and is shown as below.

- VPI/VCI value (VC should be disabled)
- Transmit and receive PDU sizes
- Management mode modification per port
- Max VPI/VCI bits (interface must be disabled)
- Maximum number of VCCs supported
- OAM source ID

3.6 Miscellaneous

IP DSLAM supports some other important features as below.

- Load-sharing Redundancy

These two Ethernet uplinks of IP DSLAM can be used as a single load-shared uplink for data and management path, with a provision to fall back to single one, in the event one of the links failed.

- Active Standby Redundancy

These two Ethernet uplinks of IP DSLAM can be used in an active stand by mode for data and management path, with a provision to fall back to standby link, in the event of the active links failure.

- Redundancy

Redundancy function is also supported in BOOTP/TFTP whereby it shall try to fallback to redundant Ethernet interface if it detects a problem with the existing interface if the download fails.

- Configuration

Modification of Ethernet IP address, mask, speed, and duplex mode is supported.
Support for safe mode boot where the TE Image can be downloaded for field upgrade.

CHAPTER 4
General Line Commands

This chapter is divided into the following sections,

- Section 4.1: The general Configuration of IP DSLAM Controller
- Section 4.2: DSL Command List
- Section 4.3: Interface Stack (instance number)
- Section 4.4: How to Save the Latest Configuration
- Section 4.5: How to Remote Upgrade Full Image
- Section 4.6: Wizard Commands

4.1 The General Configuration of IP DSLAM Controller

In addition to the SNMP management, users can use commands to configure the IP DSLAM Controller. Users can do telnet on the IP DSLAM Controller and use the following two ways. One is console interface; another is telnet by management port.

The IP DSLAM Controller console interface will connect to PC console port. Users can use terminal emulation software configured by the following parameters.

- VT100 terminal emulation
- 9600 bps
- No parity, 8 data bits, 1 stop bit
- No hardware flow control

Users can call type '?' for help. The "Admin> " symbol is just only a prompt.

Another tools for command interface is telnet y management port. The PC should be the same subnet as IP DSLAM Controller. The default IP address is 172.16.1.1. Users can also use the following commands to check IP and MAC address in IP DSLAM Controller. The default login name is "**admin**", password is"**1234**".

4.1.1 Configure the IP Address

4.1.1.1 Inband IP Address

Users can use the following commands to configure the inband IP address for the UP-LINK interface or inband management.

- Enter network directory
Admin> network
- Help
Admin/network> inband ?
- Display the settings
Admin/network> inband -s
- Edit the inband IP address without VLAN
Admin/network> inband <IP_addr> <NetMask>
- Edit the inband IP address with VLAN
Admin/network> inband <IP_addr> <NetMask> <vlan_id>

4.1.1.2 Outband IP Address

Users can use the following commands to configure the outband IP address for outband management.

- Enter network directory
Admin> network
- Help
Admin/network> outband ?
- Display the settings
Admin/network> outband -s
- Edit the outband IP address without VLAN
Admin/network> outband <IP_addr> <NetMask>
- Edit the outband IP address with VLAN
Admin/network> outband <IP_addr> <NetMask> <vlan_id>

4.1.1.3 Routing Table

Users can use the following commands to configure the default route and some static routes.

- Enter network directory

Admin> network

- Help

Admin/network> route ?

- Display the routing table

Admin/network> route –r

- Display the static route entries.

Admin/network> route -s

- Add a default route

Admin/network> route default <RtIP>

- Delete the default route

Admin/network> route default 0.0.0.0

- Add a static route entry

Admin/network> route -a <TargetIP> <NetMask> <GatewayIP>

- Edit the static route entry

Admin/network> route -e <RtIdx> <TargetIP> <NetMask> <GatewayIP>

- Delete the static route entry

Admin/network> route -d <RtIdx>

- Delete all static route entries

Admin/network> route -D

4.1.2 Configure NTP and Time

Users can use the following commands to configure the NTP server IP and the polling interval or not to use the NTP by configuring the current time settings manually, including the time zone and the daylight saves time.

- Enter service directory

Admin> service

- Display the settings

Admin/service> ntp –s

- Help

Admin/service> ntp ?

- Display the current time

Admin/service> ntp now

- Edit the NTP server IP address and the polling interval

Admin/service> ntp -e <IP_addr> <interval>

- Edit the year, month, date, hour, and minute.

Admin/service> ntp -t <MMDDhhmmYYYY>

- Edit the time zone and the daylight saving time.

Admin/service> ntp -z <time_zone> <DST>

- Turn on/off the NTP

Admin/service> ntp on/off

4.1.3 Configure SNMP

Users can use the following commands to configure the SNMP settings, including SNMP community, SNMP Trap port, and SNMP Trap host. Let the EMS can communicate with IP-DSLAM via SNMP.

- Enter service directory

Admin> service

- Display the general SNMP settings

Admin/service> snmp -l

- Display the SNMP Trap host entries

Admin/service> snmp -s

- Edit the read-only, read-write, and trap community.

Admin/service> snmp -c <CommRO> <CommRW> <CommTrap>

- Add a trap host

Admin/service> snmp -a <HostIP>

- Edit the trap host

Admin/service> snmp -e <EntryIdx> <HostIP>

- Delete the trap host entry

Admin/service> snmp -d <EntryIdx>

- Delete all the trap host entries

Admin/service> snmp –D

4.1.4 Upgrade Firmware

Users can use the following commands to upgrade new firmware.
- Prepare a TFTP server on a host
- Put the firmware (ipdslam.all for example) in the right directory of the TFTP server

- Enter system directory
Admin> system
- Execute the firmware upgrading
Admin/system> upgrade <ServIP> <FirmName>
- Reboot the Controller to run the new firmware
Admin/system> reboot
- After rebooting, check the firmware version
Admin/system> basicInfo

4.1.5 Save the Configuration

Users can use the following command to save the current configuration.
Admin> commit

4.1.6 Enable/Disable the Port

Users can use the following commands to enable or disable the port on Controller. By default, G1 to G6 are off, but G0 and UP-G are on. If users find that when they connect the subtend slave machines to the master machine but the connection cannot be constructed, check the link status of the port connected to the master machine is enabled.

- Enter system directory
Admin> system
- Display the current status of all ports
Admin/system> link_state -s
- Turn on/off of the specific port
Admin/system> link_state -m <IntfName> on/off

4.1.7 Connect to DSL Module

Users can login to DSL module in master or slave units using the following command.

Once entering into DSL module, the command described in section "DSL Command List" can be used.

- Display the current connectivity with DSL modules
Admin> dsl
- Login to DSL module in master via serial channel
Admin> dsl –c
- Login to DSL modules in master via Ethernet channel
Admin> dsl –s m
- Login to DSL modules in slave via Ethernet channel
Admin> dsl –s <salveId>

4.2 DSL Command List

4.2.1 How to Monitor DSL Status

Users can use the following command to check the status of DSL. The commands are listed as below:
$get adsl atuc physical ifname dsl-* (for downstream)
$get adsl atur physical ifname dsl-* (for upstream)
(*: 0 ~ 23)

4.2.2 How to Enable/Disable a DSL Port

Commands are shown as below:
$modify adsl line intf ifname dsl-* enable
$modify adsl line intf ifname dsl-* disable

4.2.3 How to Read DSL Training Rate

Commands are shown as below:
$get adsl atuc channel ifname dsli-* (for downstream/interleave channel)
$get adsl atur channel ifname dslf-* (for upstream/fast channel)
$get adsl atuc channel ifname dsli-* (for downstream/interleave channel)
$get adsl atur channel ifname dslf-* (for upstream/fast channel)
(*: 0 ~ 23)

4.2.4 How to Change ADSL Line Profile

Commands are shown as below:
$modify adsl line intf ifname dsl-* disable
$modify adsl line profile ifname dsl-* ?
$modify adsl line intf ifname dsl-* enable

4.2.5 How to Change ADSL Line Rate

Commands are shown as below:
$modify adsl line intf ifname dsl-* disable
$modify adsl line profile ifname dsl-* atucintlmaxtxrate 0x7e0000
$modify adsl line intf ifname dsl-* enable

4.2.6 How to Change ADSL to Fast Channel/Rate

Commands are shown as below:
$modify adsl line intf ifname dsl-* disable
$modify adsl line profile ifname dsl-* type fastOnly
atucfastmaxtxrate 0x7e0000
$modify adsl line intf ifname dsl-* enable

4.2.7 How to Set ADSL Alarm Profile

Commands are shown as below:
$modify adsl line intf ifname dsl-* disable
$modify adsl alarm profile ifname dsl-* ?
$modify adsl line intf ifname dsl-* enable

4.2.8 How to Change VPI/VCI for Existing VCC

Commands are shown as below:
$modify atm vc intf ifname aal5-* disable
$modify atm vc intf ifname aal5-* vpi <new-vpi> vci <new-vci>
$modify atm vc intf ifname aal5-* enable
(*: Existing aal5 interface)

4.3 Interface Stack (instance number)

Commands are shown as below:

Bridge Port (1~193)

|__ Ethernet (1)

|__ EOA (Ethernet over ATM) (192)

|__ AAL5 (vpi/vci, fast/interleaved) (192)

|__ ATM (max VCs) (24)

|__ DSL (line/alarm profile, ...) (24)

4.3.1 How to Change Management IP Address for Existing Ethernet Port

Commands are shown as below:

// Aggregation Ethernet

$modify aggr intf ifname aggr-0 ip <new-ip> mask <new-mask>

or

// Non-Aggregarion Ethernet

$modify ethernet intf ifname eth-* ip <new-ip> mask <new-mask>

(*: 1 or 2)

4.3.2 How to Create more VC/EOA/Bridge

Commands are shown as below:

$create atm vc intf ifname aal5-* vpi <vpi> vci <vci> lowif atm-*

[vcmux/llcmux] [fast/interleaved]

$create eoa intf ifname eoa-* lowif aal5-*

$create bridge port intf portid <bridge-port-id> ifname eoa-*

4.3.3 How to Setup SNMP Community/Host/Trap

Commands are shown as below:

$create snmp comm community <community> RW

$create snmp host ip <host-ip> community <community>

$create snmp hosttrap ip <host-ip> community <community>

4.3.4 How to Create VLAN

Commands are shown as below:
$create vlan static vlanname <vlan-name> valnid <vlan-id>
[egressports <bridge ports>]

4.3.5 How to Setup Port VALN ID (PVID)

Commands are shown as below:
$modify gvrp port info portid <bridge-port-id> portvalnid <default-pvid>

4.3.6 How to filter MAC address by port

Commands are shown as below:
$create acl port macentry portId <bridge-port-id> macaddr 00:00:00:01:02:03
$create acl port macentry portId <bridge-port-id> macaddr 00:00:00:01:02:04
// allow source address 00:00:00:01:02:03/04 access from bridge port
<bridge-port-id>
// other source addresses from bridge port <bridge-port-id> are denied

4.3.7 How to deny MAC address globally

Commands are shown as below:
$create acl global macentry macaddr 00:00:00:01:02:03 deny enable
// mac aource address 00:00:00:01:02:03,04 access from any bridge ports is denied

4.3.8 How to Filter Net BIOS

Commands are shown as below:
// NETBIOS-NS Name Service 137 TCP/UDP
// NETBIOS-DGM Datagram Service 138 TCP/UDP
// NETBIOS-SSN Session Service 139 TCP/UDP
$create filter rule entry ruleid <id> action drop description NETBIOS-TCP
$create filter subrule tcp ruleid <id> subruleid 1
srcportfrom 137 srcportto 139 srcportcmp inrange
$modify filter rule entry ruleid <id> status enable
$create filter rule map ifname all ruleid <id> stageid 1
$create filter rule entry ruleid <id2> action drop description NETBIOS-UDP

$create filter subrule udp ruleid <id2> subruleid 1
srcportfrom 137 srcportto 139 srcportcmp inrange
$modify filter rule entry ruleid <id2> status enable
$create filter rule map ifname all ruleid <id2> stageid 1

4.3.9 How to enable Spanning Tree Protocol

Commands are shown as below:
// enable STP globally
$modify stp info enable

// bridge port id: 1~24, 193
$modify stp port info portid <bridge-port-id> enable
$get stp port info portid <bridge-port-id>

4.3.10 How to enable IGMP Snooping

Commands are shown as below:

// NOTE: IGMP Snooping is Factory Default Setting
$create filter rule entry ruleid <id> action sendtocontrol description IGMP
$create filter subrule ip ruleid <id> subruleid 1
prototypefrom 2 prototypecmp eq
$modify filter rule entry ruleid <id> status enable
$create filter rule map ifname all ruleid <id> stageid 1
$modify igmpsnoop cfg info status enable
$modify igmpsnoop port info portid <bridge-port-id> status enable
leavemode fastNormal
or
$modify igmpsnoop port info portid <bridge-port-id> status enable
leavemode Fast

4.3.11 How to Remote Upgrade Control Plane Code

Commands are shown as below:

- Prepare tftp server
- Prepare vendor supplied CP.bin.gz
- Put CP.bin.gz into root directory of tftp server

```
$list
Name                    Ver      Time                          Size        Acc State
-------------------------------------------------------------------------------------------------
/nvram/bin/bootptftp/
TftpBootp.bin            1       Mon Aug 23 16:52:58 2004      110008      RO  active
/nvram/bin/control/
CP.bin.gz                1       Mon Aug 23 16:52:58 2004      1467208     RW  active
/nvram/bin/dataplane/
DP.bin.gz                1       Mon Aug 23 16:52:58 2004      252784      RW  active
/nvram/bin/decompressor/
Decompressor.bin         1       Mon Aug 23 16:52:58 2004      81160       RO  active

$remove fname /nvram/bin/control/CP.bin.gz version 1        <-- depends on real status
$download src CP.bin.gz dest /nvram/bin/control/CP.bin.gz ip <server-ip>
$list

Name                    Ver     Time                          Size        Acc State
-------------------------------------------------------------------------------------------------
/nvram/bin/bootptftp/
TftpBootp.bin            1      Thu Aug 26 18:31:22 2004      110008      RO active
/nvram/bin/control/
CP.bin.gz                2      Thu Jan 01 00:13:28 1970      1467204     RW Latest
/nvram/bin/dataplane/
DP.bin.gz                1      Thu Aug 26 18:31:22 2004      252784      RW active
/nvram/bin/decompressor/
Decompressor.bin         1      Thu Aug 26 18:31:22 2004      81160       RO active
NOTE: the Ver of CP.bin.gz becomes 2
NOTE: the State of CP.bin.gz becomes "Latest"
$upgrade fname /nvram/bin/control/CP.bin.gz version 2       <-- depends on real status
NOTE: the State of CP.bin.gz becomes "active"
$reboot
```

4.4 How to Save the Latest Configuration

Commands are shown as below:
$commit

4.5. How to Remote Upgrade Full Image

Commands are shown as below:
1. Prepare tftp server
2. Prepare vendor supplied TEImage.bin.gz
3. Put TEImage.bin.gz into root directory of tftp server
$reboot config safe // reboot from Safe mode
// boot completely...
$create ethernet intf ifname eth-0 ip <ip_address> mask <mask>
$download src TEImage.bin.gz dest /nvram/TEImage.bin ip <server_ip>
Downloading the File.
.....
Download file size is 1991180
Check if TEImage.bin shall uncompress
Uncompressing "TEImage.bin.gz" (11990111->4194304) .....
TEImage.bin.gz is in proper format

Unlocking Flash.....
Unlock successful
Erasing Flash ....
Erasing successful

Starting to Uncompress TEImage.bin.gz and Burn Flash
Uncompressing "TEImage.bin.gz" (1990111->4194304) .....
##################################
Flash Programmed successfully
Done.
Download session Completed, Bytes received 1991180...
$

$reboot // reboot from Default mode

Note:
Please refer to the Command Line Interface manual for getting more commands IP DSLAM supports.

4.6. Wizard Commands

In addition to the primitive commands described as above. Several wizard commands are provided which is used easily. Type 'wizard' to see the command syntax.

$ wizard
<List of Wizard Commands>
---
dsl show [fast]
alarm show
pvc show
pvc create <dsl: 1~24> <vc: 1~8> <vpi> <vci> [<llcmux|vcmux>]
[<interleaved|fast>]
pvc delete <dsl: 1~24> <vc: 1~8>
bridge delete <bridge id: 1~193>
tca show <acked>
critical show <acked>
firmware upgrade [-]<source file> <CP|DP|FD|DSL> <server ip>
fd show

port <disable|enable|restart> <dsl: 1~24>

config backup <filename> <server ip>
config restore <filename> <server ip>

Use 'dsl show [fast]' to display all the 24 ports DSL status.
Use 'firmware upgrade' in an atomic and safer fashion to upgrade firmware without removing the existing one in advance.
Use 'config backup/restore' to backup or restore the current configuration.