IVD

Integrated Voice and Data
User Guide

Release 1.5

Trademark

DrayTek is a registered trademark of DrayTek Corp. IVD products 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 IVD.

Contents

Introduction 8

Conventions 8

Notice 8

Text 8

Figures and Screen Captures 9

1.1 Introduction 11

1.2 Hardware Architecture 17

1.2.1 System Architecture Overview 17

1.2.2 IVD Master Overview 18

1.2.3 IVD Slave Overview 19

1.3 Box Connections 20

1.3.1 Rack-Mounting the BOX 20

1.3.2 Installing Chassis in Rack 20

1.3.3 Desktop Type Installation 20

1.3.4 Power, Ground Connections on the Rear Panel 21

1.4 Power Connection 22

1.4.1 AC Power Connection 22

1.4.2 DC Power Connection 22

1.5 ADSL Port Connection 23

1.5.1 MDF Connections (Main Distribution Frame) 23

1.5.2 Centric Patch Panel Connection 23

1.6 Connector and Interface Description 25

1.6.1 The RS232 Connector Description 25

1.6.2 Standard 10/100 Base-T Ethernet Interface Connector 26

1.6.3 Standard 10/100/1000 Base-T Ethernet Interface Connector 27

1.6.4 Optical Giga Ethernet Interface as Trunk Interface with SC Connector 28

1.6.5 RJ21 DSL and Phone Connector 29

2.1 System Connection Description 30

2.2 IVD Master Device Setup 31

2.2.1 IVD Master Front Panel Connection 31

2.2.2 Master Console Port Connection 33
2.2.3 Master Management Port Connection 33
2.2.4 Maser Subtend Port Connection 34
2.2.5 Master LED Indication 35
2.3 IVD Slave Device Setup 36
2.3.1 IVD Slave Front Panel Connection 36
2.3.2 IVD Console Port Setup 37
2.3.3 IVD Management Port Connection 38
2.3.4 Line Interface Connection 38
2.3.5 IVD LED Indication 38
3.1 Introduction 41
3.2 Quality of Service (QoS) 43
3.2.1 Prioritized Bridging 43
3.2.2 Scheduling Mechanisms 43
3.2.3 Rate Limiting 43
3.2.4 Mapping Table 44
3.2.5 Multiple Mechanisms 44
3.2.6 Abilities 44
3.3 Security 44
3.3.1 Static Mac Address 44
3.3.2 FDB Conflicting Traps 45
3.3.3 MAC Address Tracking 45
3.3.4 Access Control List by MAC address 45
3.3.5 Access Control List by IP Address 45
3.4 Packet Filtering 45
3.4.1 Filtering Modes 46
3.4.2 Classifier Tree 46
3.4.3 Multiple Filter Stages 46
3.5 ATM Features 46
3.5.1 Remote CPE Management 47
3.5.2 Diagnostic Testing 47

3.5.3 Dynamic Modification 47
3.6 Multicast Modes 47
3.7 VoIP Features 48
3.8 Miscellaneous 49

A Power Spectral Density 50
A.1 The ADSL PSD Mask 51
A.2 The ADSL2 PSD Mask 51
A.3 The ADSL2+ PSD Mask 52

B Performance 53

C Splitter Specification 54

List of Tables

Table 1-1. The RS232 adaptor PINOUT 26
Table 1-2. RJ21 Cables Pin assignment 29
Table 2-1. IVD master connection 32
Table 2-2. IP DSLAM master DSL LED descriptions 36
Table 2-3. IVD connections 37
Table 2-4. IVD front panel LED and description 39

List of Figures

Figure1-1. Application scenario of IVD 12
Figure 1-2. Stacking IVD architecture 17
Figure 1-3. IVD Master Device Picture 18
Figure 1-4. IVD Slave device picture 19
Figure 1-5. Brackets for 19-, 23-inch rack 20
Figure 1-6. Bracket installation for front mounting on 19-, 23-inch rack 20
Figure 1-7. Rear panel and AC power input 21
Figure 1-8. Rear panel and DC power input 21
Figure 1-9. Rear panel and DC power input 22
Figure 1-10. MDF connection architecture 23
Figure 1-11. CPP front panels 24
Figure 1-12. Data only CPP connection 24
Figure 1-13. Data/Voice CPP connection 25
Figure 1-14. Console management cable 25
Figure 1-15. Applicable on both straight-through and crossover RJ45 cables overview 26
Figure 1-16. Applicable on both straight-through and crossover RJ45 (8C8P) cable 27
Figure 1-17. The RJ21 champ cable connection 29
Figure 2-1. IVD network connections overview 31
Figure 2-2. IVD master interface on front panel 32
Figure 2-3. Master console port connection 33
Figure 2-4. Master management port connection 34
Figure 2-5. Master subtend connection 35
Figure 2-6. Master subtend connection 36
Figure 2-7. IVD front panel connections overview 37
Figure 2-8. IVD slave console port connection 38
Figure 2-9. IVD management port connection 38
Figure 2-10. IVD LED indication 39
Figure A.1 The IVD ADSL PSD mask 51
Figure A.1 The IVD ADSL2 PSD mask 52

Figure A.1 The IVD ADSL2+ PSD mask 52

History Table

Date	Descriptions	Version	By
2006/07/11	Initialize	V1.0	Jenny, Jimmy, Amy
2006/07/21	1. Add default baud rate values in 2.2.2 2. Remove 3.3.1 Rate Limit 3. Add detailed description in 3.5.1	V1.1	Jimmy
2006/8/16	1. Revise Section 4.3.4 to add a example	V1.2	Jimmy
2007/1/16	1. Add Master parts. 2. Revise pictures of manual. 3. Remove commands to CLI manual.	V1.3	Jenny, Amy, Jimmy, Eric, Steven, Ken
2007/5/8	1. Add section 1.6.6 about ECB cable	V1.4	Amy, Jimmy
2007/5/15	1. Revise section 1.6.6 with detailed scenario 2. Add section 1.6.7 about air flow graph	V1.5	Jimmy

About This Guide

Introduction

This document is designed to assist users in using one of the series of high performance IVD device. It provides a product overview and hardware architecture descriptions, installation procedures and product features. The command line interface description is also given in this document.

Conventions

This guide may contain notices, figures, screen captures, and certain text conventions.

Notice

The following table lists notices icons used in this guide.

Icon	Notice Type	Description
	Note	Information that contains important features or instructions but is not hazard-related.
	Caution	Information to alert of potential damage to a program, data, system, or device. If not avoided, may result in minor or moderate damage. It may also alert against unsafe practices and potential program, data, system, device damage.
	Warning	Information to alert of operations that may cause potential accident, casualty, personal injury, fatality or potential electrical hazard. If not avoided, could result in death or serious injury.
	ESD	Information that indicates proper grounding precautions is required before handling a product.

Text

The following table lists text conventions in this guide.

Convention	Description
Text represented by `Courier New Font`	`This typeface` represents text that appears on a terminal screen, including, configuration file names (only for system output file names), and command names, for example `login`. Commands entered by users are represented by **`bold`**, for example, **`cd $HOME`**.
Text represented by **bold**	This typeface represents window names, dialog box names, tabs, field names, function names, directory, file names, process names, and commands in text, for example, set the **Time** field.
Text represented by [Menu] and [Menu/Sub-menu]	This square brackets represents menus such as [File], and [File/New]
Text represented by <Button>	This angle bracket represents button on screen, function key on the keyboard and icon names for example, click <OK>.
Text represented by *Document Name*	This typeface represents documents for reference, for example, *Netman 2020 Installation Guide*

Convention	Description
Text represented by `# File format:`	This typeface represents files in Unix/Linux system files.

Figures and Screen Captures

This guide provides figures and screen captures as example. These examples contain sample data. This data may vary from the actual data on an installed system.

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

This document describes the new generation type integrated voice and data IVD, named IVD. The IVD solution supports DSL and VoIP services and supplies high-speed Internet access and voice/video streaming. It provides multicast, quality of service (QoS), security, SNMP-based EMS (Element Management System), and user-friendly command line interface. With this powerful management tool, both of the service providers and consumers can benefit from lower operating costs and rapid deployment.

To meet the increasing demand for voice over IP services, the next generation network offers this feasible functionality with the most cost effective architecture. IVD network is used to provide VoIP service on traditional copper wire infrastructure. The type of service will be supported on NGN (Next Generation Network) system architecture. IP DSLAM (IP based DSL Access Multiplexer) to fast extend the coverage of xDSL services and to facilitate DSL deployment.

IVD is a remote type IP based VoIP Gateway provides toll quality voice communication in terms of voice quality and reliability for the user. The type of service and application scenario is supported on NGN system architecture and shown on following picture.

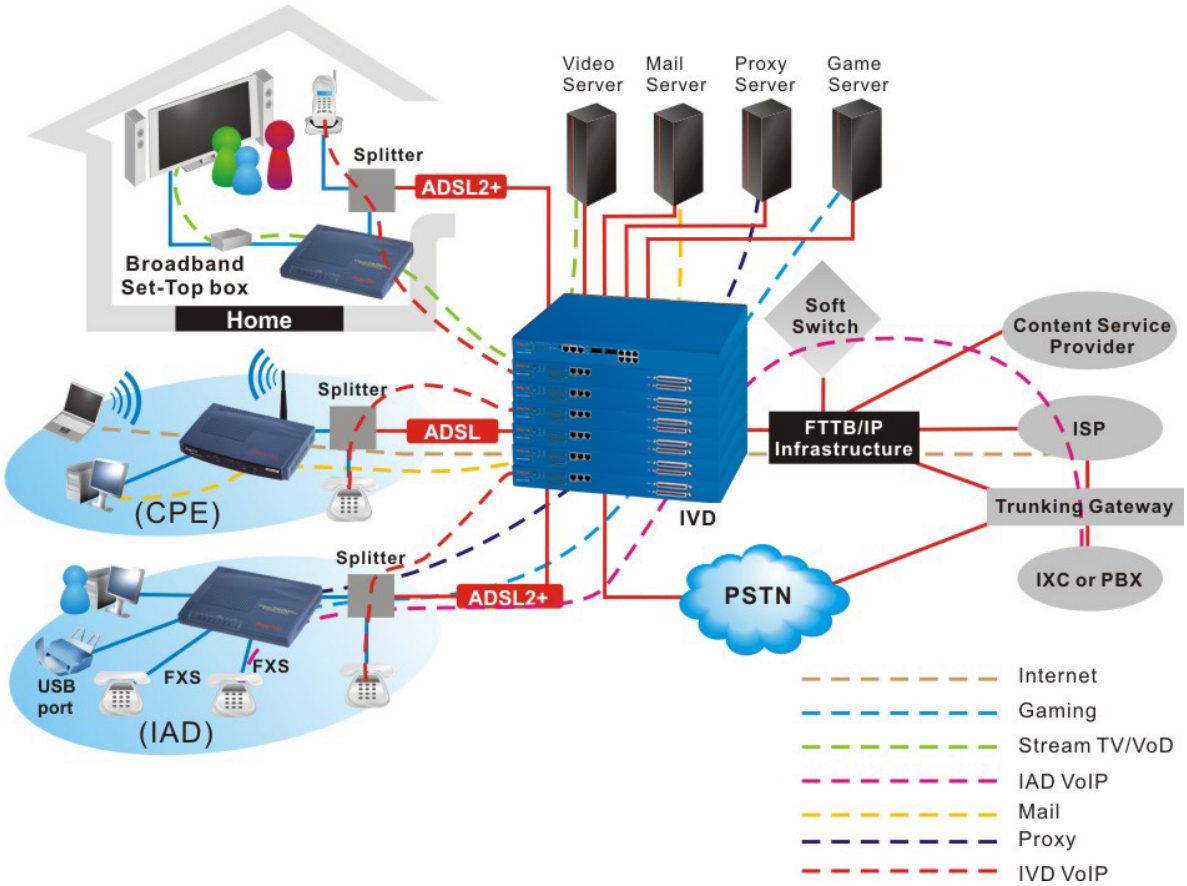


Figure1-1. Application scenario of IVD

In this application scenario, IVD connects to IP backbone network through Gigabit Ethernet interfaces to minimize the investment of service provider. System provider can easily install and scale the network with the same framework. IVD provides mini or middle scale system architecture to system provider a very cost effective solution and deploy VoIP service without spending extra line installing fee.

As IVD supports high upstream and downstream bit-rates performance, therefore, IVD 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 and use convenient VoIP application.

IVD 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, IVD can be easily configured by EMS. The EMS system covers topology, configuration, deployment, security, alarm management and backup storage. Moreover, with the solution of port-based and tag-based VLAN, IVD can isolate traffic between different users and provide improved security.

The compact design of IVD is for 24-port ADSL 2/+ with built-in POTS splitters connected to ADSL modems and 24-port FXS VoIP.

High speed Internet Service

IVD aggregates DSL subscribers and terminates the encapsulated type ATM cell. Users can easily access Internet through the IP backbone network. IPDSLAM supports PPPoE, DHCP, static IP connection methods and provides Transparent LAN connection methods. IVD can support simultaneously PPPoE and DHCP connection methods on the same PVC.

PPPoE Connection Mode

- IVD supports bridged encapsulation at U interface defined by DSL Forum in WT-101 (Migration to Ethernet Based DSL Aggregation, Rev.7, May. 2005) on Figure 4 stack b.
- IVD supports filtering options in order to prevent L2 traffic between DSL customers connected to the same DSLAM considering PPPoE environment (Intra-DSLAM filtering).
- DSLAM part supports filtering options in order to prevent L2 traffic between DSL customers connected to different DSLAMs considering PPPoE environment (Inter-DSLAM filtering) considering N:1 VLAN forwarding.
- Intra-DSLAM and Inter-DSLAM filters of the DSLAM is capable to be disabled partly or entirely

- IVD provides positive Ethertype filtering with the following Ethertype values in upstream direction:
  - 0x8863: PPPoE discovery
  - 0x8864: PPPoE session

  Positive filtering means, that DSLAM transmits Ethernet frames only with the defined Intertype values.
- IVD can filter Ethernet Broadcast frames in downstream direction.
- IVD provides capabilities to prevent BRAS MAC spoofing.
- IVD provides capabilities to prevent end user spoofing and end user blocking.

DHCP Access method

- The DSLAM supports bridged encapsulation at U interface defined by DSL Forum in WT-101(Migration to Ethernet Based DSL Aggregation, Rev.7, May. 2005) on Figure 4 stack a.

- DSLAM supports filtering options in order to prevent L2 traffic between DSL customers connected to the same DSLAM considering DHCP environment (Intra-DSLAM filtering).
- DSLAM supports filtering options in order to prevent L2 traffic between DSL customers connected to different DSLAMs considering DHCP environment (Inter-DSLAM filteringconsidering N:1 VLAN forwarding.
- Intra-DSLAM and Inter-DSLAM filters of the DSLAM are capable to be disabled partly or entirely on VLAN basis.
- DSLAM provides positive Ethertype filtering with the following Ethertype values in upstream direction:
  - 0x0800: IP
  - 0x0806: ARP

  Positive filtering means, that DSLAM transmits Ethernet frames only with the defined Intertype values.
- IVD can filter Ethernet Broadcast frames in downstream direction.
- IVD provides capabilities to prevent BRAS (Gateway) MAC spoofing.
- IVD provides capabilities to prevent end user spoofing and end user blocking.

Technical specification of Ethernet DSLAM

- DSLAM can filter any traffic originates from the DSL endpoints before a valid DHCP IP address assigning.
- After a valid DHCP IP address assigning the DSLAM transmits only traffic originates from the given source MAC/IP is stored during IP assigning.
- DSLAM supports DHCP Option 82 insertion.
- DSLAM supports DHCP relay with Option 82 insertion.

Static IP Access method

- The DSLAM supports bridged encapsulation at U interface defined by DSL Forum in WT-101 (Migration to Ethernet Based DSL Aggregation, Rev.7, May. 2005) on Figure 4 stack a.
- DSLAM supports filtering options in order to prevent L2 traffic between DSL customers connected to the same DSLAM considering Static IP environment (Intra-DSLAM filtering).
- DSLAM supports filtering options in order to prevent L2 traffic between DSL customers connected to different DSLAMs considering Static IP environment (Inter-DSLAM filtering) considering N:1 VLAN forwarding.
- Intra-DSLAM and Inter-DSLAM filters of the DSLAM are capable to be disabled partly or entirely on VLAN basis.
- DSLAM provides positive Ethertype filtering with the following Ethertype values in upstream direction
  - 0x0800: IP
  - 0x0806: ARP

  Positive filtering means, that DSLAM transmits Ethernet frames only with the defined Intertype values.
- IVD can filter Ethernet Broadcast frames in downstream direction.
- IVD provides capabilities to prevent BRAS (Gateway) MAC spoofing.
- IVD supports proxy ARP function.
- IVD transmits traffic only originates from given source IP address(es).

- **Transparent LAN Service (L2VPN)**

  The IVD solution provides additional requirements in order to support L2 VPN service (Transparent LAN).
  The system is the possibility of totally transparent L2 transport of L2 VPN service Ethernet frames, including
  - unicast, multicast and broadcast frames,
  - tagged and untagged frames and
  - frames with special content (e.g. L2 Control Protocol, Routing).

  The transparent L2 transport results in L3 independence, so customers can use whatever L3 protocols (e.g. IP, IPX, etc.).

  There are two scenarios when a L2-VPN is implemented over Ethernet transport:
  - Routers (L3 CPE) at ADSL endpoints
  - Switches (L2 CPE) at ADSL endpoints
- The IVD can support both of the L2VPN solutions.

Routers (L3 CPE) at ADSL endpoints

- The DSLAM transparent for unicast, multicast and broadcast traffic originates from subscriber.
- Dynamic routing protocol exchange routing information using MC frames which addresses are in the Local Network Control Block (224.0.0/24) and in some cases in the Internetwork Control Block (224.0.1/24). Some examples are as follows: RIPv2 (224.0.0.9), OSPF (224.0.0.5, 224.0.0.6), (E)IGRP (224.0.0.10), PIMv2 (224.0.0.13, 224.0.1.39, 224.0.1.40), etc.
- The DSLAM is transparent for dynamic routing protocols which use multicast MAC/IP addresses.
- The DSLAM supports bridged encapsulation at U interface defined by DSL Forum in WT-101 (Migration to Ethernet Based DSL Aggregation, Rev.7, May. 2005) on Figure 4 stack a.
- The DSLAM supports routed encapsulation at U interface defined by DSL Forum in WT-101 (Migration to Ethernet Based DSL Aggregation, Rev.7, May. 2005) on Figure 4 stack c.
- In case of routed encapsulation DSLAM is able to convert routed to bridged encapsulation
- DSLAM provides N:1 forwarding for VLAN allocation.

- Considering bridged encapsulation and N:1 scenario. The DSLAM provides possibility to limit the MAC addresses originates from the DSL endpoints in order to protect the MAC table of the devices.
- DSLAM is able to add 802.1ad tag in upstream direction.

- DSLAM is able to remove 802.1ad tag in downstream direction.
- At the uplink interface of the DSLAM will use a unique virtual MAC address per PVC as source address in case of routed encapsulation of RFC2684.

Switches (L2 CPE) at ADSL endpoints

- The DSLAM is transparent for both untagged and tagged user traffic.
- Ethertype field for the 802.1ad tagging, i.e. S-Tags, will be configurable (per access node) due to WT-101 of DSL Forum.
- The DSLAM is transparent for L2CP (Layer 2 Control Protocols on Multicast MAC addresses) originates from subscriber.
- The DSLAM supports bridged encapsulation at U interface defined by DSL Forum in WT-101 (Migration to Ethernet Based DSL Aggregation, Rev.7, May. 2005) on Figure 4 stack a.
- DSLAM provides N:1 forwarding for VLAN allocation.
- In N:1 scenario the DSLAM provides possibility to limit the MAC addresses originates from the DSL endpoints in order to protect the MAC table of the devices.
- DSLAM is able to add 802.1ad tag in upstream direction.
- DSLAM is able to remove 802.1ad tag in downstream direction.

Gaming Application Service
By combining gaming server, IP DSLAM can provide gaming service.

IPTV Service
IVD uses ADSL 2/+ high speed DSL technology, and supports IPTV 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, IVD also provides the video on demanded service. Users can easily access multimedia content based on IVD architecture.

Combined with VoIP Service
IVD 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
IVD provides the feasibility to connect mail or proxy server.

Outdoor Application
The IVD can be offered for indoor and outdoor use.

OAM Management System
The IVD is managed by Element Management system for O&M support purposes.

IVD 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 IVD provide one-chip solution with ADSL, ADSL2 and ADSL2+backward compatible technology. The ADSL mode for ADSL/ADSL2/ADSL2+ is configurable per subscriber ports. The system use ATM basic encapsulation method for data transmission. ATM Layer is according to ITU-T Recommendation G.992.1, G.992.3, G.992.5 and G.991.2. By the integrated POTS splitter and LT function, The IPDSLAM system is capable of delivering high speed digital information over existing unshielded twisted copper pair telephone lines without any changes. The ADSL transmission system is implemented according to ITU-T Recommendation G.992.1 Annex A. The Frequency Division Duplexing (FDD) for FDM or EC mode is used for separation of the upstream and downstream signals, as it is specified in ITU-T Recommendation G.992.1, G.992.3 and G.992.5. To provide interoperability between ATU-C (ADSL Transceiver Unit – Central) and ATU-R (ADSL Transceiver Unit – Remote), Handshake Procedures for ADSL, ADSL2 and ADSL2+ Digital Subscriber Line transceivers is supported in ADSL system according to ITU-T Recommendation G.994.1.

The rate of IVD when operating in, ADSL system supports downstream data rate from 32 kbps to 8 Mbps for ADSL mode, 32 kbps to 12 Mbps for ADSL2 mode, 32 kbps to 24 Mbps for ADSL2+ mode and upstream data rate from 32 kbps to 800 kbps for ADSL mode, 32 kbps to 1 Mbps for ADSL2 mode, 32 kbps to 1 Mbps for ADSL2+ mode. Both downstream and upstream data rate is adaptive and adjustable in 32 kbps increments.

The firewall and VPN security of VoIP security router is also provided by the architecture to meet business requirements. This application is suitable on Telecom, Hotel and MTU applications. The entire system is managed by EMS system.

Voice Features

The voice channel is 24 ports with Voice QoS guarantee. The feature of Signaling: Loop start and polarity reversal can provide for billing purpose. The system provide external Ringing Source and up to three REN. The Loop Current: 24 mA. The

Voice codec type should be G.711, G.729a, G.726, G.723.

VoIP Physical Interface

Interface: 24 FXS Ports

1.2 Hardware Architecture

1.2.1 System Architecture Overview

IVD Master has the capability to subtend up to 6 Slaves. The hardware interface of Master unit covers Alarm relay, console, management with RJ45, Gigabits optical interface with SC connector, GE subtend interface with RJ45 connector. Users can connect the IVD 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 IVD Slave units up to the number of ports available on the Ethernet switch as shown in the following page.

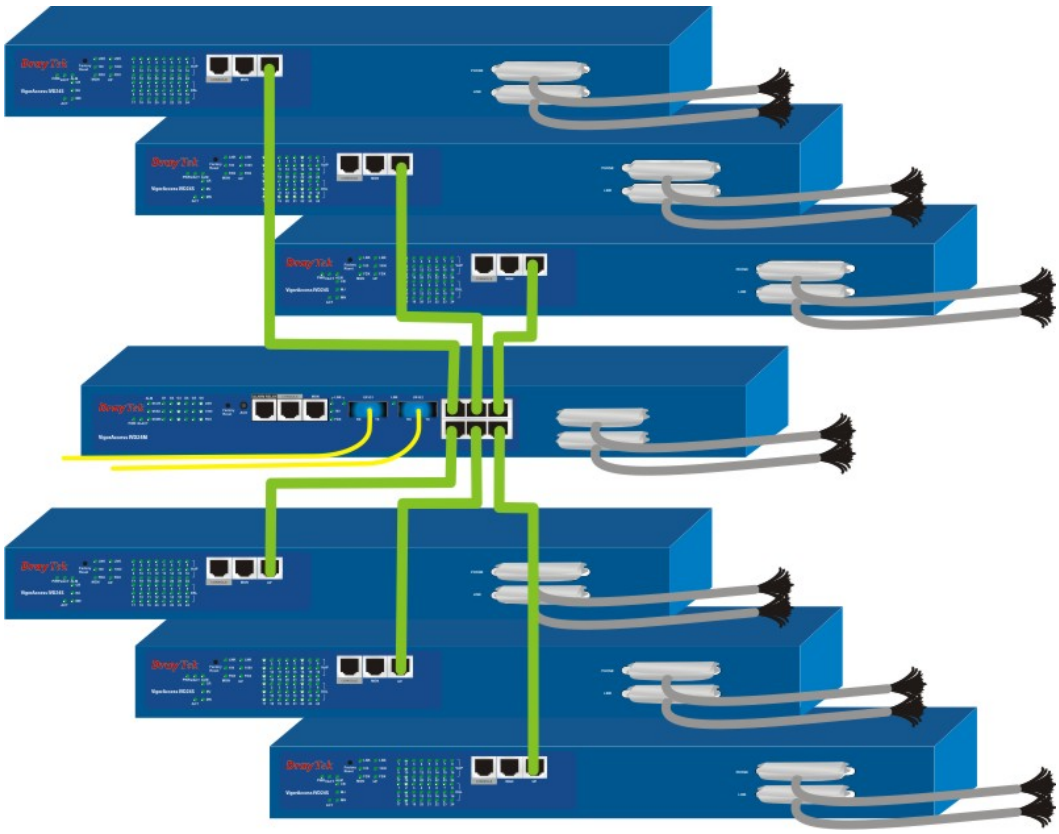


Figure 1-2. Stacking IVD architecture

1.2.2 IVD Master Overview

The purpose of 19" modularized master unit is as a central unit in stacking 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 system can operate individually covered modular built-up system.
The picture of master unit is shown in Figure 1-3.

Figure 1-3. IVD Master Device Picture

Master unit supports some features are as following –
Network Interface - The trunk should be 1000-Based LX, SX or GE Interface.

- 1000 Base T; according to IEEE 802.3-2002
- 1000 Base SX; according to IEEE 802.3-2002
- 1000 Base LX; according to IEEE 802.3-2002

Cascade Interface - GE interfaces can be cascaded up to six IVD slave units.
The Ethernet interface (full-duplex) throughput provides 100 Mbps (Fast Ethernet) or min. 500M for GE interface
Capacity – It supports subtended 6 slaves with ADSL 2/+ port range from 24 to 144 ports.
Security – It supports Packet filter, and password protection.
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.
Dimension (HxWxD)- 44.45mm (1.73 in) x 440mm (17.32 in.) x280mm (11.02 in.)
The outer cover of devices is capable to resist mechanical damaging impacts.
The outer cover of offered devices applied meets the requirements of Flammability Class V-1 according to Standard MSZ EN 60950.

1.2.3 IVD Slave Overview

The role of 19" slave unit is to provide a high-performance; good services DSL feature in Internet environment. The picture of IVD unit is shown in Figure 1-4.

Figure 1-4. IVD Slave device picture

Slave unit supports some features are shown as follows –
Network Interface – One Gigabit Copper interfaces for uplink.
Capacity – It supports ADSL 2/+ 24 ports. 24 FXS on same RJ21 subscriber line.
Failover – Provide one RJ21 for failover when device power off or Internet failure
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 Console, Telnet and EMS tool.
Q.o.S - Packet filter and classification.
Dimension (HxWxD)- 45mm (1.73 in) x 440mm (17.32 in.) x280mm (11.02 in.)

1.3 Box Connections

1.3.1 Rack-Mounting the BOX

IVD 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 1-5.

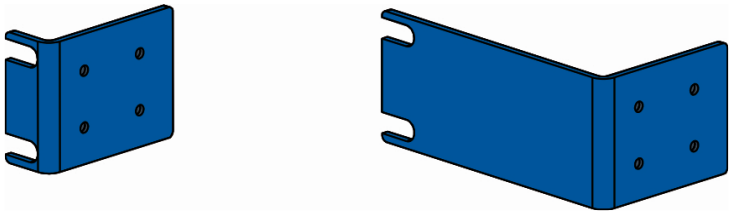


Figure 1-5. Brackets for 19-, 23-inch rack

Attach the brackets to the chassis in 19-, 23-inch rack as shown in Figure 1-6. The second bracket attaches the other side of the chassis as above procedure.

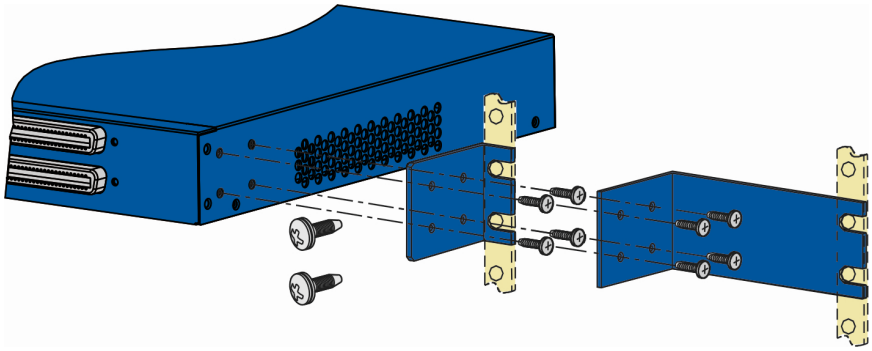


Figure 1-6. Bracket installation for front mounting on 19-, 23-inch rack

1.3.2 Installing Chassis in Rack

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

1.3.3 Desktop Type Installation

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

1.3.4 Power, Ground Connections on the Rear Panel

The AC input and ground connections are on the rear panel and shown in Figure 1-7. You can connect the rack to ground by spring screws.

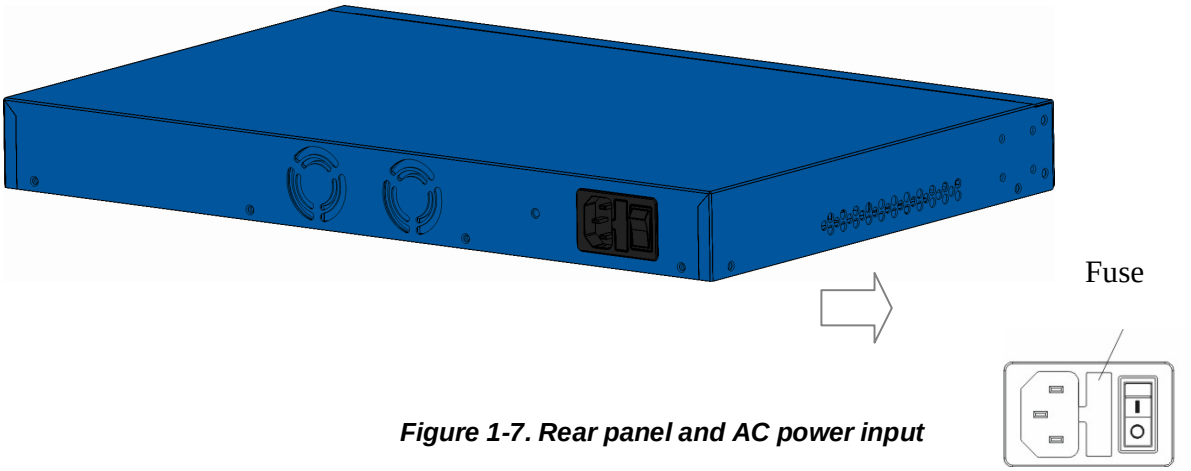


Figure 1-7. Rear panel and AC power input

The DC 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.

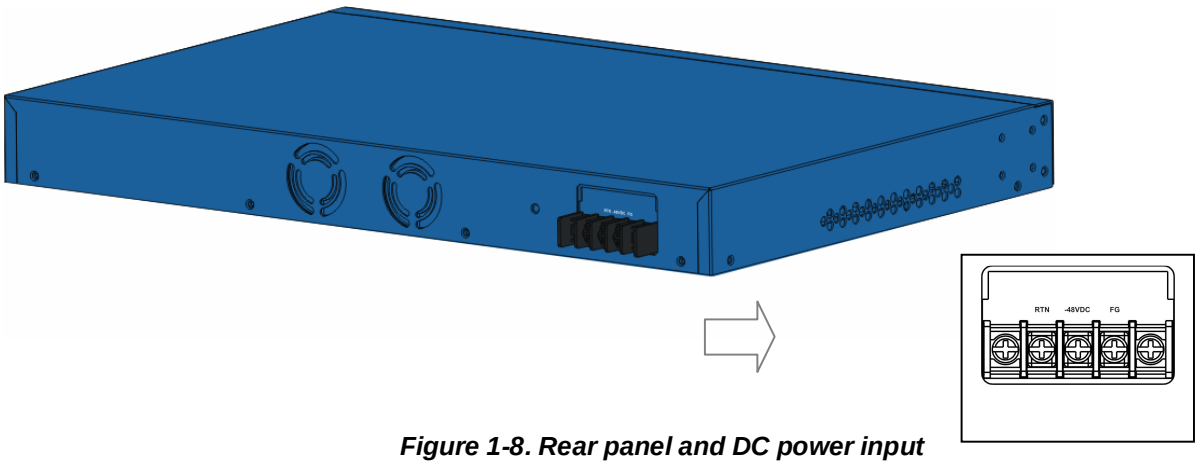


Figure 1-8. Rear panel and DC power input

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 IVD 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 1-9 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.

Step 7 Check and turn on the power from power source. If the power is properly connected, a PWR green LED on the front panel of IVD lights up.

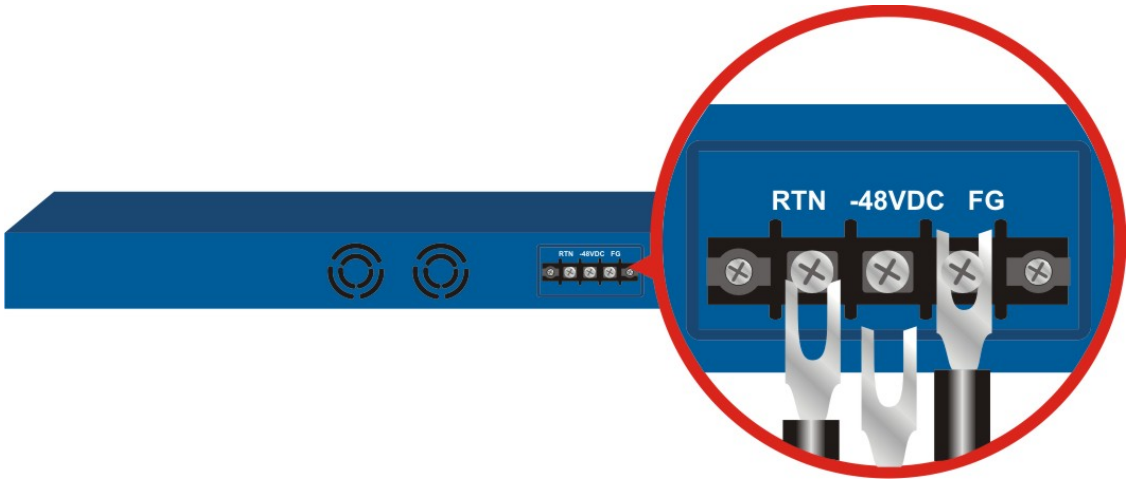


Figure 1-9. Rear panel and DC power input

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 1-10. 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.

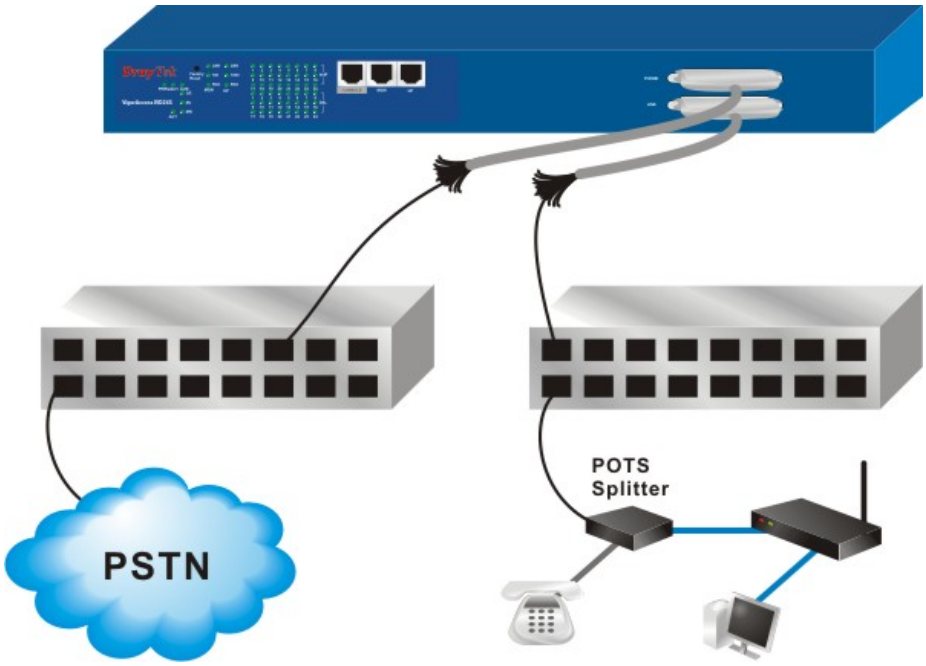


Figure 1-10. MDF connection architecture

1.5.2 Centric Patch Panel Connection

The IVD 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 IVD to RJ-11 connector. The CPP front panels are shown in Figure 1-11. It is usually installed between end-user's 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.

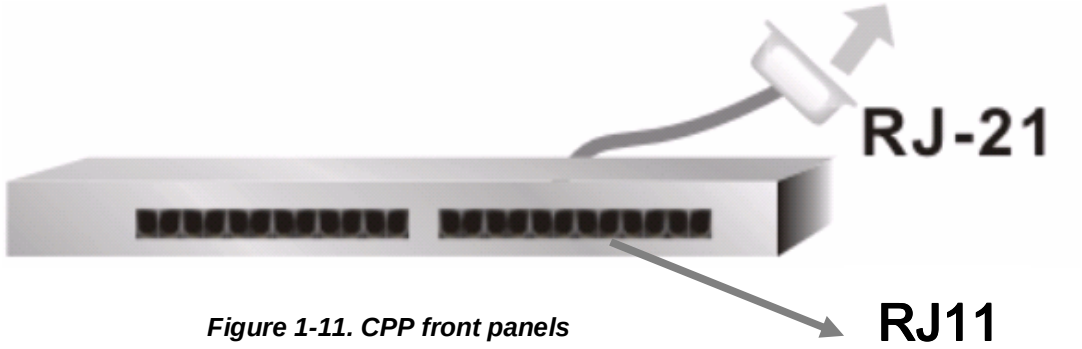


Figure 1-11. CPP front panels

The following figures give some examples of scenario for using IVD 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 IVD 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 1-12.

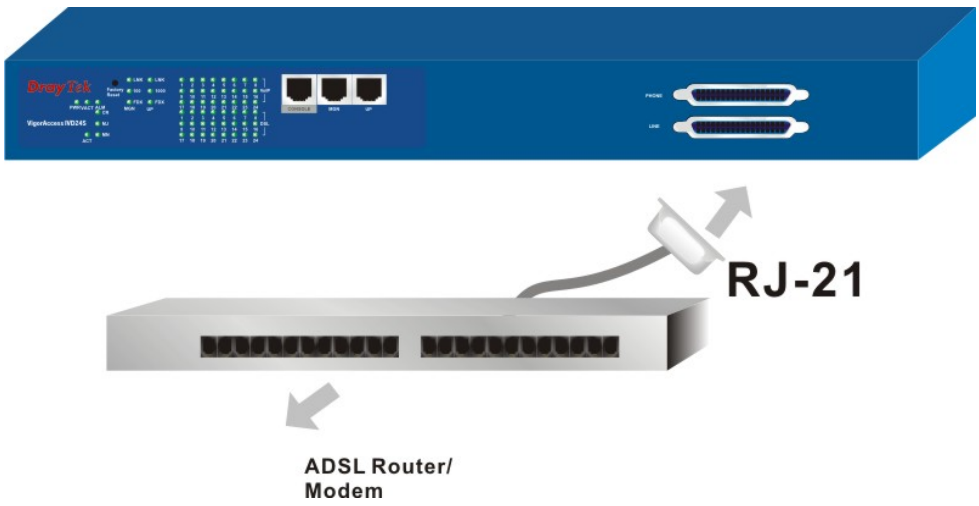


Figure 1-12. Data only CPP connection

1.5.2.2 Installation CPP Scenario B

Phone service is available in IVD. 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 1-13.

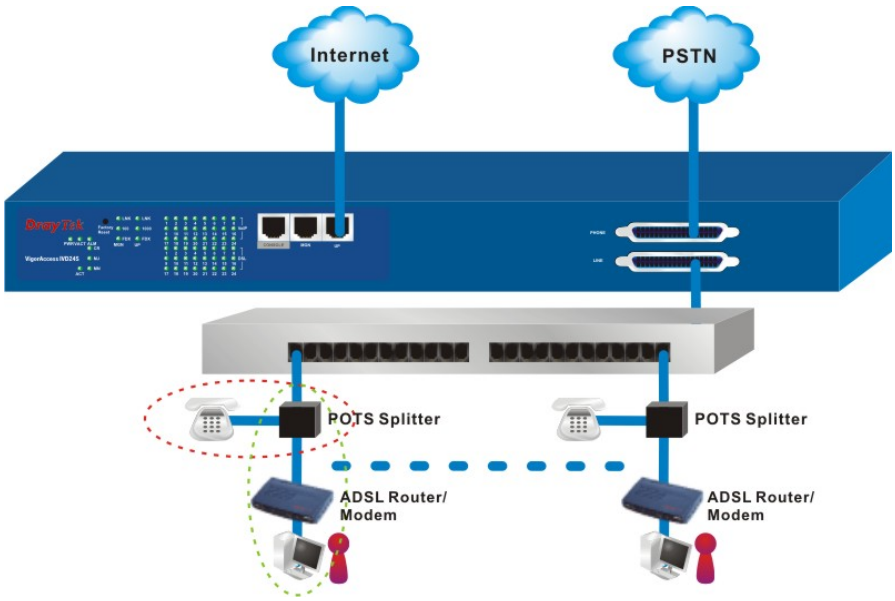


Figure 1-13. Data/Voice CPP connection

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 IVD. The jet is used for initialization of the IVD during the preliminary installation. The "management cable", as shown in Figure 1-14, converts the RJ45 to the RS232 interface. The RJ45 jet connects to a console interface in the IVD, 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 1-14. Console management cable

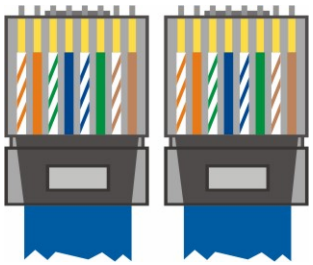
The pin-out for this connector is shown in Table 1-1 as follows.

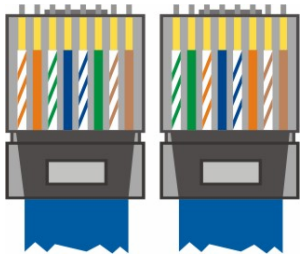
Table 1-1. The RS232 adaptor PINOUT

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.





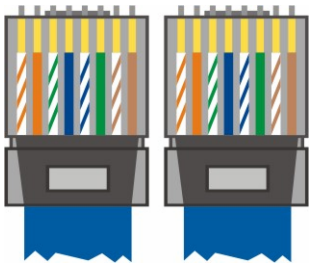
RJ-45 **Straight-through** Cable Pin-outs			
Signal	Pin	Pin	Signal
Tx+	1	1	Tx+
Tx-	2	2	Tx-
Rx+	3	3	Rx+
--	4	4	--
--	5	5	--
Rx-	6	6	Rx-
-	7	7	-
-	8	8	-

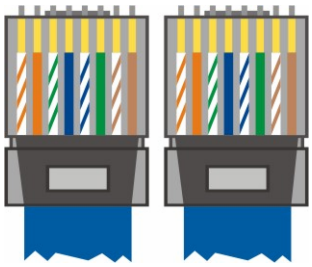
RJ-45 **Crossover** Cable Pin-outs			
Signal	Pin	Pin	Signal
Tx+	1	1	Rx+
Tx-	2	2	Rx-
Rx+	3	3	Tx+
--	4	4	--
--	5	5	--
Rx-	6	6	Tx-
-	7	7	-
-	8	8	-

Figure 1-15. 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 1-16. 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 1-17.
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.

1.6.5 RJ21 DSL and Phone Connector

Connections are made with two 50-pin champ cables (Figure 1-18) that are attached to the RJ21 interface on IVD. 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.

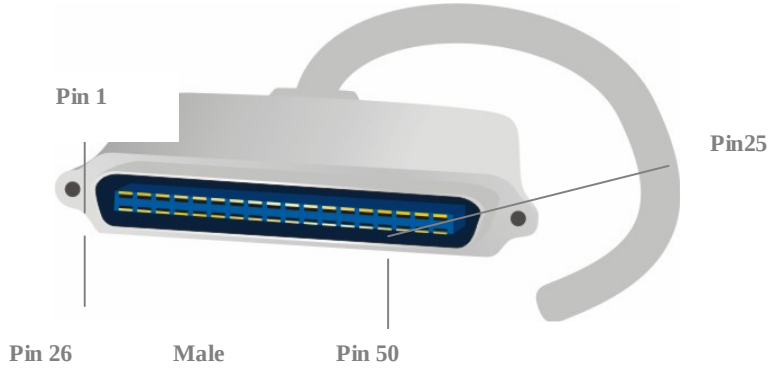


Figure 1-17. The RJ21 champ cable connection

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

2 Installation

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

This chapter is divided into the following sections,

- Section 2.1: System Connection Description
- Section 2.2: IVD Master Device Setup
- Section 2.3: IVD Slave Device Setup

2.1 System Connection Description

There are following steps to setup the IVD connection,

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

After previous steps are completed, the system architecture will be show as Figure 2-1.

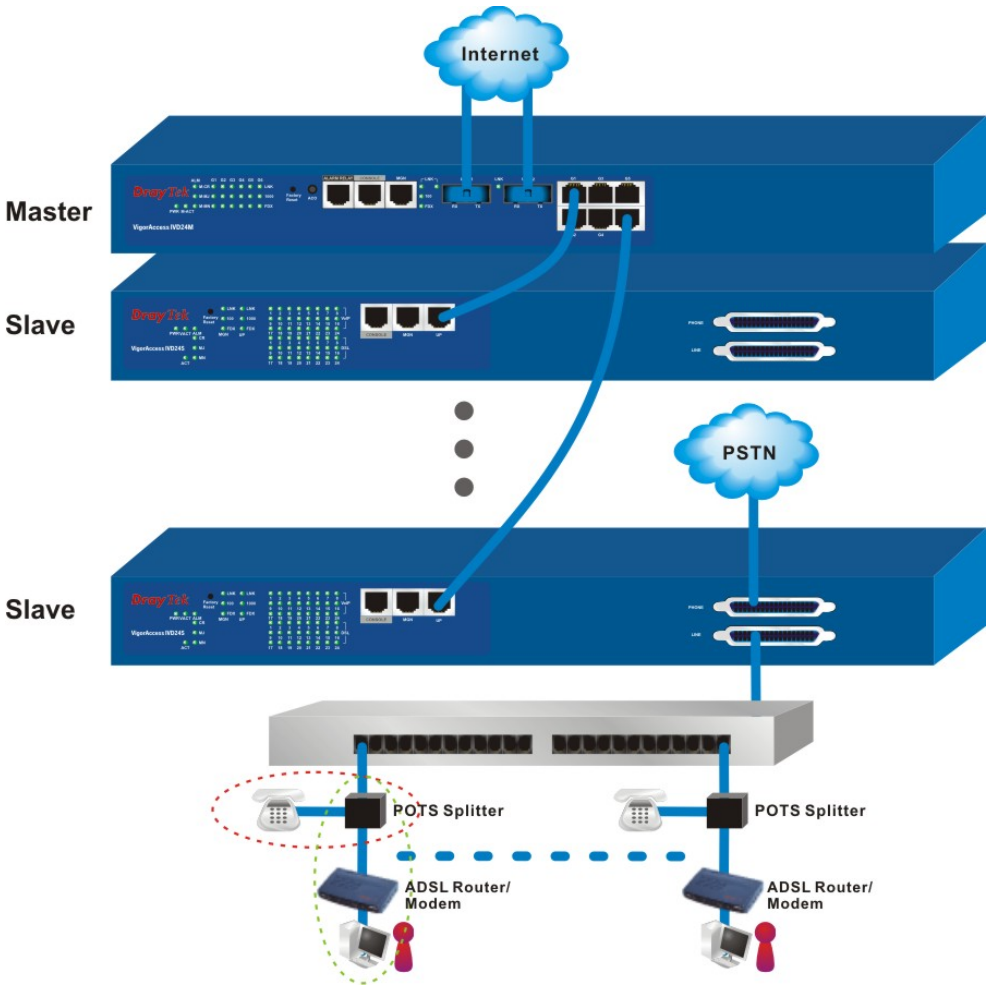


Figure 2-1. IVD network connections overview

2.2 IVD Master Device Setup

2.2.1 IVD Master Front Panel Connection

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

Factory Reset – A reset button is used to reset system, and then IVD 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 IVD and to manage IVD 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.

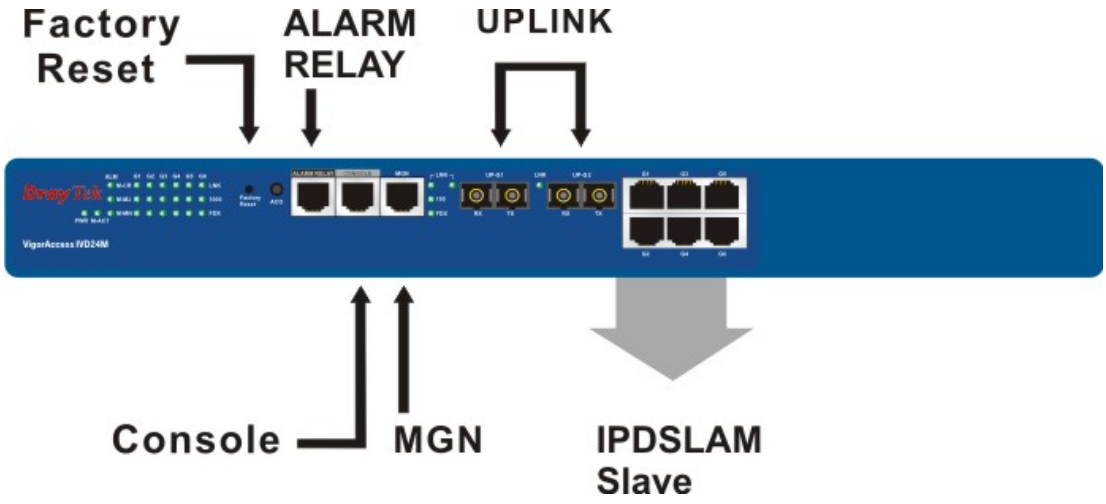


Figure 2-2. IVD master interface on front panel

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

Table 2-1. IVD 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	--
Uplink (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)*	

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**"

Example:

```
**********************************************************
*            Bootloader Version: V1.0.9                  *
**********************************************************
Press [ENTER] key within 5 sec. to download image...0
Please wait a minute...
Login:
```

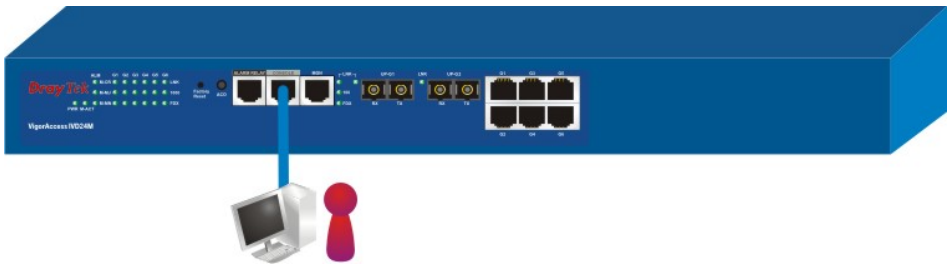


Figure 2-3. Master console port connection

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
Example:

```
-------------------------------------------------------------------------------
  OUTBAND INTF CONFIGURATION
-------------------------------------------------------------------------------
IP Address      : 172.16.1.1
NetMask         : 255.255.255.0
Vlan Id         : 0
```

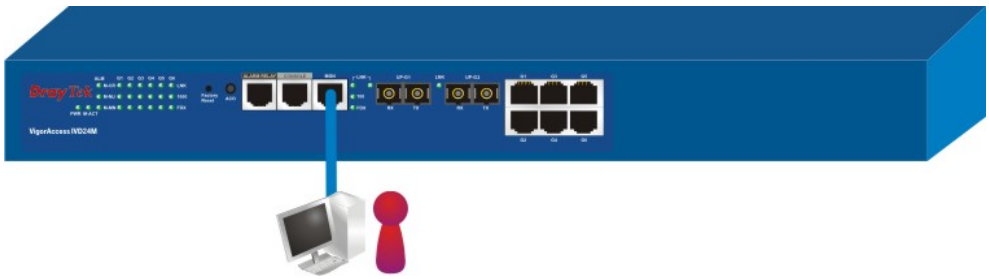


Figure 2-4. Master management port connection

2.2.4 Maser Subtend Port Connection

Users can connect the uplink of IVD Slave to subtend interface of IVD Master by plug and play. Use following command to connect from Master to Slave.

Admin> dsl -s <n>

Press 'exit' to return

Entering character mode
Escape character is '^]'.

[dsl-slave-n]#

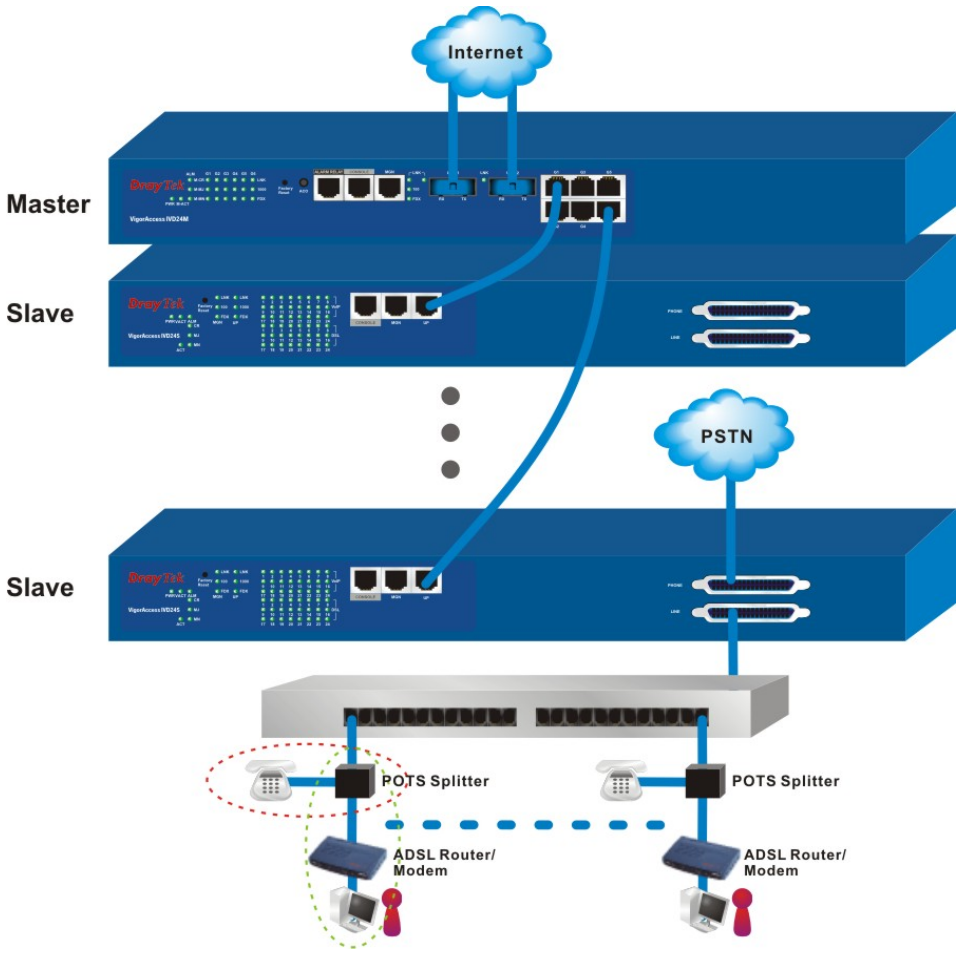


Figure 2-5. Master subtend connection

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.

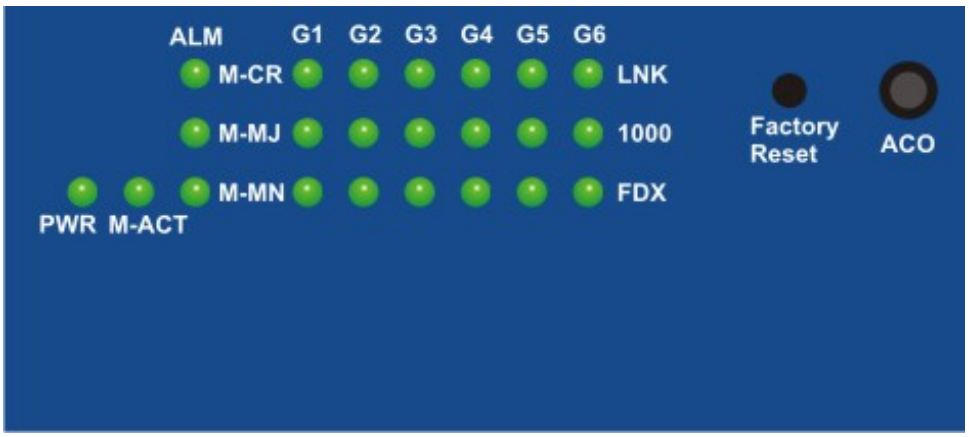


Figure 2-6. Master subtend connection

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.

2.3 IVD Slave Device Setup

2.3.1 IVD Slave Front Panel Connection

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

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

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 IVD and to manage IVD by CLI command.

UPLINK – Support one 1000M Ethernet ports to Internet. The interface can be used as for Telnet management. Users can set local PC (personal computer) as the same subnet as IVD and to manage IVD by CLI command.

PHONE – Connected to PSTN normally.
LINE – Connected to ADSL devices or telephones for users.

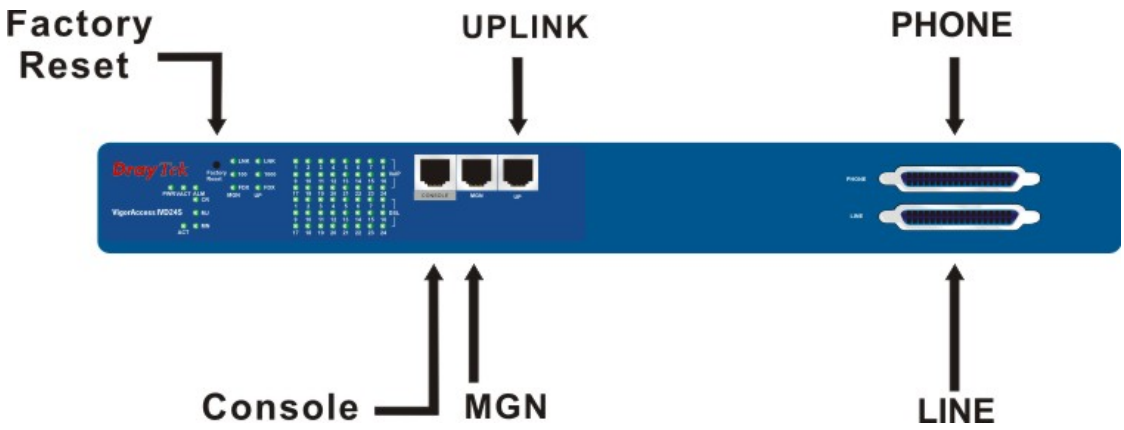


Figure 2-7. IVD front panel connections overview

Table 2-3. IVD connections

Port	Type, Color	Connected to	Remarks
Power Cord	Cord, Black Wire with lug terminal	AC Inlet DC Inlet	100-240VAC -42 ~ 56VDC
Console (Serial)	RS232, Grey	Connect to PC RS232 port for debug	--
MGN	RJ-45, Blue	To Intranet with a management host	
UPLINK	RJ-45, Blue	To Internet management	
PHONE	RJ-21,	To PSTN	
LINE	RJ-21,	To subscriber copper line	

2.3.2 IVD 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 a serial port of a computer.
The default setting is “baud rate **9600**, no parity, and 8 bit with 1 stop bit (N,8,1)”

The default login is “**admin**”, password is “**1234**”

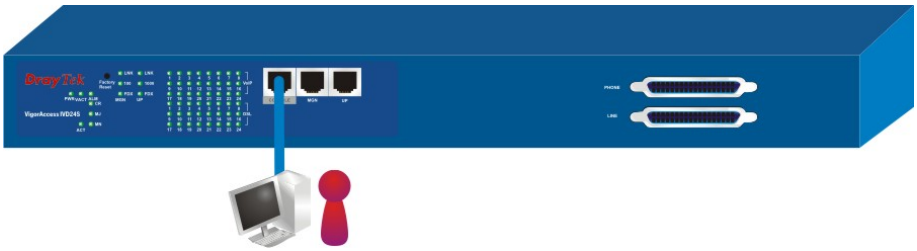


Figure 2-8. IVD slave console port connection

2.3.3 IVD Management Port Connection

Users can connect the RJ-45 cable to the Ethernet port of the computer. The IP address is **172.16.1.2** by default. The subnet of PC should be the same as default IP setting.

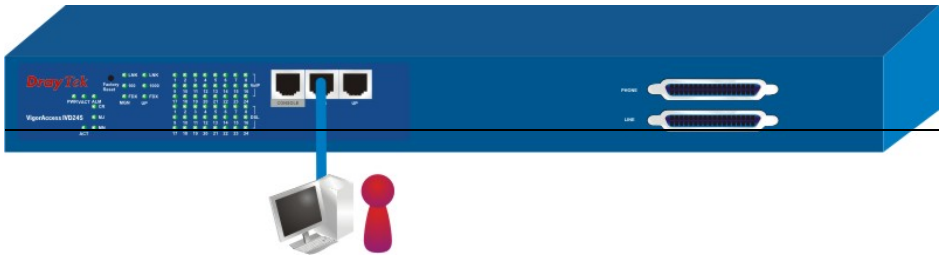


Figure 2-9. IVD management port connection

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 IVD 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 IVD 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 IVD with a blue RJ-45 cable, and the UP1 or UP2 LED will blink.

Furthermore, IVD provides signal LED for CR (Critical Alarm), 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. IVD LED indication

Table 2-4. IVD front panel LED and description

LED		Indication	Description	Remarks
PWR		Green	Power ON	100-240VAC/ -42V ~ 56VDC
		OFF	Power OFF	
VACT		Green	Blink when VoIP system is active	
		OFF	When VoIP System is inactive	
ACT		Green	Blink when DSL system is active	
		OFF	When DSL system is inactive	
ALM		Green	VoIP System alarm is active	
		OFF	VoIP System alarm is inactive	
UP/MGN	LNK	Green	Ethernet link is established	
		OFF	No Ethernet link established	
		Blinking	Packets in incoming/outgoing	
	1000 (UP) 100 (MGN)	Green	The speed for Ethernet is 1000M,when LNK LED is ON (MGN is 100M)	
		OFF	The speed for Ethernet is 100M when LNK LED is OFF	
	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 OFF	
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	
VoIP		Green	VoIP is active	1~24
		Blinking	VoIP is ringing	
		OFF	VoIP is inactive	

3 IVD Product Features

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: Multicast Modes
- Section 3.7: VoIP Features
- Section 3.8: Miscellaneous

3.1 Introduction

The IVD (Integrated Voice and Data) is an IP-based DSLAM (Internet Digital Subscriber Line Access Multiplexer) that connects to 24 ADSL subscribers to the Internet and 24 VoIP-FXS ports included. 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. IVD 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.

10/100/1000 Mbps Auto-negotiating Ethernet Port
IVD supports two 10/100/1000 Mbps auto-negotiate Ethernet ports connects to an Ethernet network. The IVD supports Ethernet interfaces towards the transport 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 802.3 ad standard.

Supports oversized Ethernet frames up to 1526 byte.
IEEE 802.1Q Tagged VLANand Double-tagged VLAN capabilities conform to IEEE 802.1ad Standard

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

VLAN Feature

- The DSLAM is able to attach VLAN tag (S-Tag) to untagged frames, received on user ports at the upstream direction.
- The DSLAM is able to attach a second VLAN tag (S-Tag) to tagged frames (C-Tag) received on user ports at the upstream direction.
- The DSLAM is able to attach two VLAN tags (S-Tag, C-Tag) to untagged frames, received on user ports at the upstream direction.
- The DSLAM is able to remove VLAN Tag identification (S-Tag) from frames received from the aggregation the DSLAM". (i.e. downstream direction) before sending them on user ports.
- The DSLAM is able to remove VLAN Tag identification from frames received from the aggregation network (i.e. downstream direction) before sending them on user ports. The options for. The options for removal are both S-Tag and C-Tag.
- The Ethertype field for the 802.1ad tagging, i.e. S-Tags, is configurable.

- The DSLAM supports two types of tagged ports:
- ・ VLAN-transparent port
  ・ Non VLAN transparent port

VLAN allocation and forwarding mechanisms

- IVD conforms to 1:1 VLAN forwarding defined in WT101 of DSL Forum.
- IVD is able to disable address learning for 1:1 VLANs.
- IVD conforms to N:1 VLAN forwarding defined in WT101 of DSL Forum.

IEEE 802.1p Priority

IVD supports IEEE 802.1p at VLAN level 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

IVD 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

IVD 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

IVD supports bridge and routed of multi-protocol encapsulation over ATM adaptation Layer 5 based on RFC2684.

Management

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

PVC Binding VLAN
DSLAM supports binding of ATM PVCs of a given DSL port to different VLANs according to WT101 of DSL Forum, IPDSLAM supports simultaneously the following
- binding multiple ATM PVCs (of same or different DSL ports) to a singe VLAN,
- binding multiple (m) ATM PVCs (of same or different DSL ports) to multiple (n)
- VLAN where m>=n and n≠1.

A given ATM PVC will not be bound to more than one VLAN.

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. This feature can be used for VoIP traffics.

3.2.1 Prioritized Bridging

IVD 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

IVD supports multiple scheduling mechanisms.
- Strict Priority Scheduling
- Probabilistic Priority Scheduling

3.2.3 Rate Limiting

IVD 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

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

3.2.5 Multiple Mechanisms

IVD 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

IVD 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

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

3.3.1 Static Mac Address

IVD 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.

3.3.2 FDB Conflicting Traps

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

3.3.3 MAC Address Tracking

IVD 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.

3.3.4 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.

3.3.5 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.

IVD 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

IVD 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, IVD 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.

- IVD supports configurable Ethertype filter for upstream direction.
- IVD supports configurable MAC filter for upstream direction.
- IVD supports configurable Broadcast (blocking/enabling) filter for downstream direction.
- IVD supports configurable Multicast (enabling, disabling, prefix specific enabling) filter for upstream direction.
- DSLAM is able to store at least N*8 MAC addresses, where "N=Maximum number of DSL ports on the DSLAM".
- In order to prevent source MAC flooding attacks the DSLAM is able to limit the number of source MAC addresses learned from a PVC.
- MAC addresses learning on the Network Side Ethernet interface is configurable (enable/disable).
- IVD supports static MAC address entries.
- IVD support Virtual MAC address and MAT (MAC Address Translation) for both PPPoE and DHCP connection methods, equivalent solution for BRAS MAC spoofing.
- Virtual MAC address and MAT is configurable (enable/disable) at least per VLAN.
- IVD supports L2 marking of the traffic coming from the ATM PVCs.
- IVD supports L3 marking of the traffic coming from the ATM PVCs.
- IVD use the Giga Ethernet Interface to cascade to extend the capacity.
- Binding management traffic to a dedicated VLAN is provided.

3.4.2 Classifier Tree

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

3.4.3 Multiple Filter Stages

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

3.5 ATM Features

IVD supports some functions about ATM issue.

3.5.1 Remote CPE Management

IVD supports RAW AAL5 interface for remote CPE management. This function can be implemented via EMS tool.

3.5.2 Diagnostic Testing

IVD supports OAM based on I.610 F5 end-to-end and segment loopback SELT and DELT diagnostic tool. The DSLAM provides OAM functionalities corresponding to WT-101 of DSL Forum.

3.5.3 Dynamic Modification

IVD 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 Multicast Modes

- IGMPv2 operation is provided and conform to RFC2236.
- IVD supports IGMP snooping function
- IVD supports configurable filtering of IGMP Membership Report messages.
- IVD supports dropping of all IGMP messages received on a subscriber port.
- IVD supports an IGMP v2 transparent snooping function. This feature is configurable on a per VLAN basis.
- IVD supports IGMP immediate leave as part of the IGMP snooping function.

- IVD provides statistics on all active groups on a per-VLAN and per-port basis.
- IVD allows the configuration of IP multicast groups or ranges of multicast groups per multicast VLAN based on:
  - Source address matching
  - Group address matching
- IVD is able to configure per DSL port the maximum number of simultaneous multicast channels allowed.
- IVD supports the Globally Scoped Multicast Addresses (224.0.1.0 – 238.255.255.255).
- IVD supports the Limited Scoped Multicast Addresses (239.0.0.0/8).
- IVD supports a mechanism to prevent a user port from becoming a multicast router port by blocking IGMP query messages.
- IVD supports mechanisms to stop user ports injecting unauthorized multicast traffic into the aggregation network.
- The DSLAM support IGMP Fast Leave.
- N:1 VLANs forwarding mode is used in order allow efficient forwarding of multicast traffic. (It is to be noted that other types of traffic (data, voice, unicast video) could be delivered via N:1 VLANs as well.)
- Dedicated Multicast VLAN model is supported. (This is a model where a dedicated N:1 VLAN is used to send some multicast groups from a multicast router / BNG to one or several access nodes, over an aggregation network. Other traffic is sent across different VLANs, where these VLANs could be 1:1 or N:1.)
  Integrated Multicast VLAN model is supported. (This is a model where multicast traffic is inserted into one of the N:1 VLANs that are terminated at a subscriber DSL port, or alternatively dot1q trunked to the RG. This effectively means multicast and unicast share a VLAN.)

3.7 VoIP Features

- VoIP Telephony
  It is based on MGCP/SGCP, SIP call signaling.
- IVD supports codec with G.711, G.729a, G.726 and G.723.
- IVD supports On-net to On-net, On-net to Off-net, Off-net to On-net and Off-net to Off-net call.
- IVD supports VAD (silience suppression).

- IVD supports echo cancellation (G.168)(16ms echo tail length)
- IVD supports 24 FXS lines.
- IVD supports VoIP features as below -

  MGCP, SIP protocols.

  Codec G.711, G.729A, G.723.1, G.726.

  VAD(Silence Suppression) & CNG.

  G.168-2000 Echo Canceller, Jitter Buffer.

  Packet Loss Concealment.

  Out of Band DTMF(RFC2833).

  Modem Support Rate Up V.92. (for G.711 only)

  QoS for Bandwidth Reservation.

  Hunt Group.

  Outbound Proxy.

  Call Forwarding.

  Call Holding.

  T.38 Fax Rely.

  NAT Traversal. (STUN)

  Incoming Call Barring.

  FXO Incoming/Outgoing Preset Number.

3.8 Miscellaneous

IVD supports some other important features as below.

- Load-sharing Redundancy
  These two Ethernet uplinks of IVD 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 IVD 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.

A Power Spectral Density

A.1 The ADSL PSD Mask

The IVD system supports the PSD masks defined in ETSI TS 101 388 v1.3.1, Chapter 4.2.2, FDD ADSL over ISDN. The PSD mask transmitted on the ATU-C is shown as below.

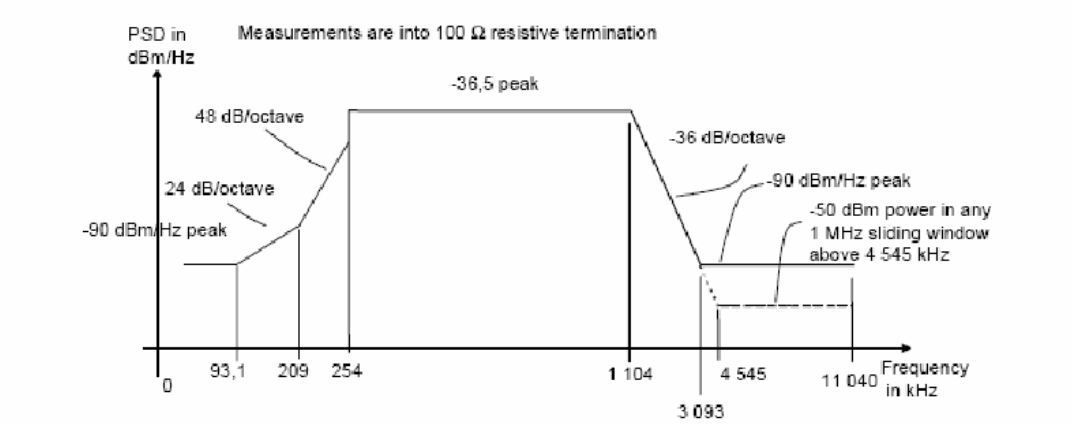


Figure A.1 The IVD ADSL PSD mask

The IVD transceiver will not be reset by a micro interruption event of duration t = 10ms, which occur at an event frequency of 0,2 Hz is according to ETSI TS 101 388 v1.3.1, The Longitudinal Conversion Loss (LCL) at the U-R interface is greater than 40 dB over the 120 kHz up to 1104 kHz frequency range, according to the DSL Forum Technical Report TR-067.

A.2 The ADSL2 PSD Mask

The ADSL2 mode of IVD system supports the PSD masks defined in defined in ITU-T Recommendation G.992.3, Annex B.1.3 and Annex B.2.2, FDD ADSL over ISDN

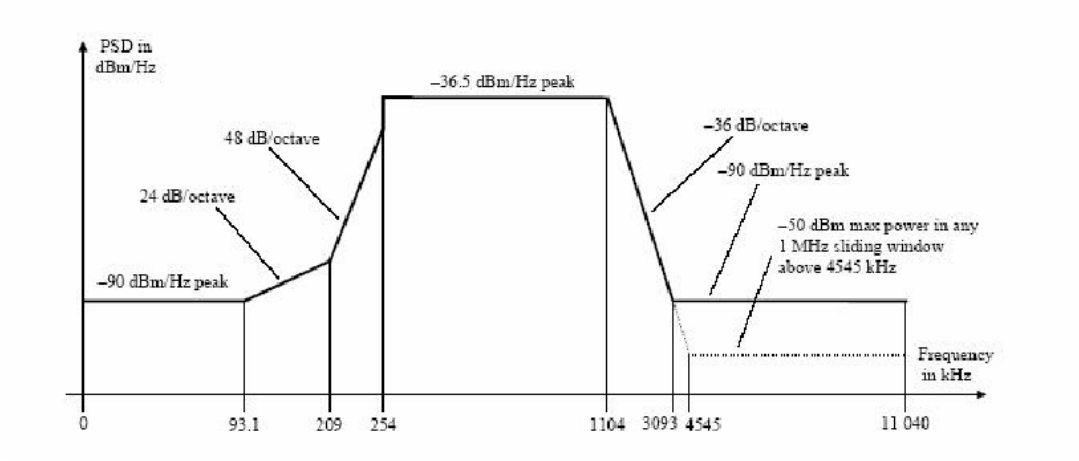


Figure A.1 The IVD ADSL2 PSD mask

The ADSL2 transceiver will not be reset by a micro interruption event of duration t = 10ms, which occur at an event frequency of 0,2 Hz. according to ETSI TS 101 388 v1.3.1. Operating in ADSL2 mode the Longitudinal Conversion Loss LCL at the U-R interface is greater than 40 dB over the 120 kHz up to 1104 kHz frequency range, according to the DSL Forum Technical Report TR-067.

A.3 The ADSL2+ PSD Mask

The ADSL2+ mode of IVD system supports the PSD masks defined in defined in ITU-T Recommendation G.992.5, Annex B.1.3 and Annex B.2.2, FDD ADSL over ISDN.

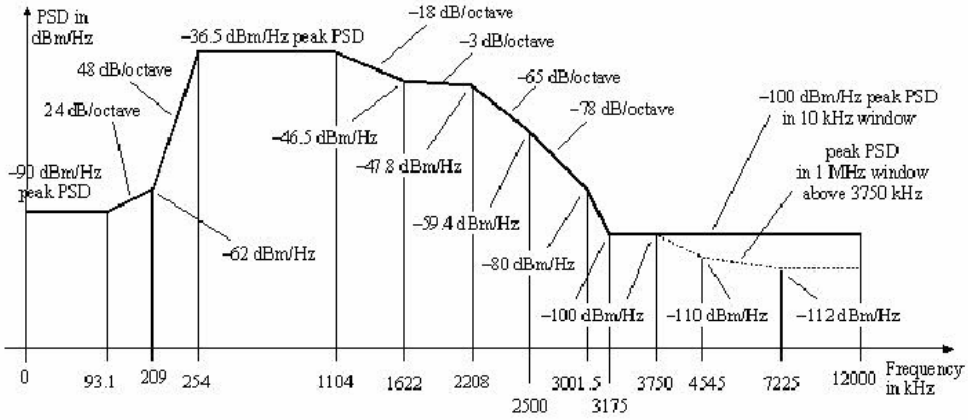


Figure A.1 The IVD ADSL2+ PSD mask

The ADSL2+ transceiver of the system will not be reset by a micro interruption event of duration t = 10ms, which occur at an event frequency of 0,2 Hz according to ETSI TS 101 388 v1.3.1 [2.1.3.2.1]. Operating in ADSL2+ mode the Longitudinal Conversion Loss (LCL) at the U-R interface is greater than 40 dB over the 120 kHz up to 2208 kHz frequency range, according to the ITU-T Recommendation G.992.5, Annex B.4.

B Performance

IVD of ADSL and ADSL2 system can work on that loop range and provide immunity to noise as it is specified in ETSI TS 101 388 V1.3.1.

Performance of line transmission system (BER) is not higher than 10^{-7}.

C Splitter Specification

Splitter requirement

The splitter is responsible for separating base-band POTS or ISDN signals from high-pass ADSL signals. Splitter terminates the copper telephone lines and distributes POTS/ISDN and ADSL signals. At exchange side of the ADSL transmission system passive ISDN splitter is used.

The ISDN splitter can separate ISDN BRA signal, which is conform with ETR 080 ANNEX A (2B1Q line code) from ADSL signals. The ISDN splitter characteristics conform that parameters, which are defined in ETSI TS 101 952-1-3 (2002-05) and TS 101 952-1-4 (2002-11). Electrical parameter of ports of splitter conforms with the parameters are defined in Table.