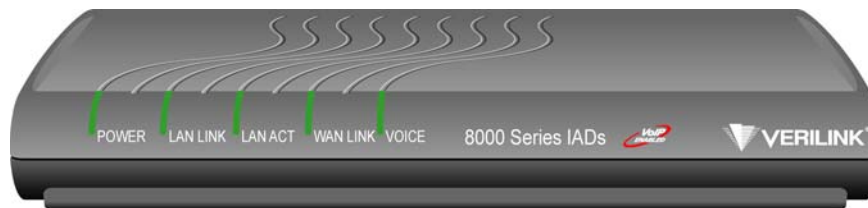
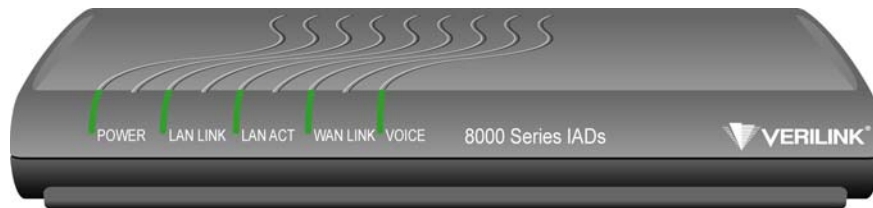


# Verilink<sup>®</sup> 8000 Series 81xx/82xx/83xx/85xx Reference Manual

December 2004  
34-00339.B



**8104, 8108 8104s,  
8108s, 8504, 8508,  
8504s, 8508s**

## **Copyright Notice**

Copyright © 2004 Verilink Corporation. All rights reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form by any means without the written permission of Verilink.

Manual Reorder # 34-00333.B

December 2004

## **Trademarks**

Verilink® is a registered trademark of the Verilink Corporation.

All other brand and product names used herein are trademarks or registered trademarks of their respective manufacturers.

## **Documentation Disclaimer**

This document does not create any express or implied warranty about Verilink or about its products or services. Verilink's sole warranty is contained in its product warranty. The end-user documentation is shipped with Verilink's products and constitutes the sole specifications referred to in the product warranty. Verilink has made reasonable efforts to verify that the information contained herein is accurate, but Verilink assumes no responsibility for its use or for any infringement of patents or other rights of third parties that may result. The customer is solely responsible for verifying the suitability of Verilink's products for its use. Specifications are subject to change without notice.

## **Warranty**

Verilink's product warranty is included at the back of this document.

## **FCC Requirements**

This equipment has been tested and found to comply with the limits for a Class A digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user is required to correct the interference at the user's own expense.

This equipment generates, uses, and can radiate radio frequency energy, and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception (which can be determined by turning the equipment off and on), the user is encouraged to try to correct the interference by taking one or more of the following measures:

- Reorient or relocate the receiving antenna
- Increase the separation between the equipment and receiver
- Plug the equipment into an outlet on a circuit different from that to which the receiver is currently connected
- Consult the dealer or an experienced radio/TV technician for help

This device must also accept any interference received, including interference that may cause undesired operation.



---

**WARNING:** *The 8108 and 8508 are to be used only with a certified Class 2 power supply. See Appendix C, "Specifications."*

---



---

**WARNING:** *Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.*

---

The 8x08 complies with Part 68 of the FCC Rules and the requirements adopted by the ACTA. On the bottom of the 8x08 unit is a label that contains, among other information, a product identifier in the format of US:GICDDNANNE8x08. If requested, this number must be provided to the telephone company.

- 1 All direct connections to network lines must be made using standard plugs and jacks (compliant with Part 68 and the requirements adopted by the ACTA). A compliant telephone cord with a modular plug is provided with this product. It is designed to be connected to a compatible modular jack that is also compliant. See installation instructions for details. The table below presents a list of applicable registration jack USOCs and facility interface codes (FIC). These are required when ordering service from the telco.

IAD	Port ID	REN/SOC	FIC	USOC
8108	ADSL	0.0B		RJ-11C
8508	SHDSL	0.0B		RJ-11C

- 2 If the unit appears to be malfunctioning, it should be disconnected from the network lines until the source of trouble is determined to be your equipment or the telephone line. If your equipment needs repair, it should not be reconnected until it is repaired.
- 3 If your telephone equipment causes harm to the telephone network, the telephone company may discontinue your service temporarily. If possible, they will notify you in advance. However, if advance notice is not practical, you will be notified as soon as possible. You will be informed of your right to file a complaint with the FCC.
- 4 Your telephone company may make changes to its facilities, equipment, operations, or procedures that could affect the proper functioning of your equipment. If they do, you will be notified in advance so you can have the opportunity to maintain uninterrupted telephone service.
- 5 If you experience trouble with the 8108/8508 units, please contact Verilink for information on obtaining service or repairs (refer to “Support from Verilink” on page xxv). The telephone company may ask that you disconnect this equipment from the network until the problem has been corrected or until you are sure the equipment is not malfunctioning. No user serviceable parts are contained in this equipment. This equipment may not be used for coin service provided by the telephone company. Connection to party lines is subject to state tariffs. Contact the state Public Utilities Commission or Corporation for information. Do not attempt to repair this equipment yourself.

### Canadian Emissions Requirements

This digital apparatus does not exceed the Class A limits for radio noise emissions from digital apparatus set out in the Radio Interference Regulations of the Canadian Department of Communications.

Le présent appareil numérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques (de la class A) prescrites dans le Règlement sur le brouillage radioélectrique édicté par le ministère des Communications du Canada.

### Safety Precautions

When handling this equipment, follow these basic safety precautions to reduce the risk of electric shock and injury:

- Follow all warnings and instructions marked on the product and in the manual.
- Unplug the hardware from the wall outlet before cleaning. Do not use liquid cleaners or aerosol cleaners. Use a slightly damp cloth for cleaning.
- Do not place this product on an unstable cart, stand, or table. It may fall, causing serious damage to the product.
- Slots in the unit are provided for ventilation to protect it from overheating. These openings must not be blocked or covered. Never place this product near a radiator or heat register.
- This product should be operated only from the type of power source indicated on the marking label and manual. If you are unsure of the type of power supply you are using, consult your dealer or local power company.
- Do not allow anything to rest on the power cord. Do not locate this product where the cord interferes with the free movement of people.

- Do not overload wall outlets and extension cords, as this can result in fire or electric shock.
- Never push objects of any kind into the unit. They may touch dangerous voltage points or short out parts that could result in fire or electric shock. Never spill liquid of any kind on this equipment.
- Unplug the equipment from the wall outlet and refer servicing to qualified service personnel under the following conditions:
  - When the power supply cord or plug is damaged or frayed
  - If liquid has been spilled into the product
  - If the product has been exposed to rain or water
  - If the product has been dropped or if the housing has been damaged
- To reduce the risk of electrical shock, do not remove the cover from the unit or external power supply. There are no user-serviceable parts inside this unit. Contact qualified Verilink service personnel.

8208, 8208s, 8304,  
8308, 8304s, 8308s

## Copyright Notice

Copyright © 2004 Verilink Corporation. All rights reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form by any means without the written permission of Verilink.

Manual Reorder # 34-00333.B

September 2004

## Trademarks

Verilink® is a registered trademark of the Verilink Corporation.

All other brand and product names used herein are trademarks or registered trademarks of their respective manufacturers.

## Documentation Disclaimer

This document does not create any express or implied warranty about Verilink or about its products or services. Verilink's sole warranty is contained in its product warranty. The end-user documentation is shipped with Verilink's products and constitutes the sole specifications referred to in the product warranty. Verilink has made reasonable efforts to verify that the information contained herein is accurate, but Verilink assumes no responsibility for its use or for any infringement of patents or other rights of third parties that may result. The customer is solely responsible for verifying the suitability of Verilink's products for its use. Specifications are subject to change without notice.

## Warranty

Verilink's product warranty is included at the back of this document.

## FCC Requirements

This equipment has been tested and found to comply with the limits for a Class A digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user is required to correct the interference at the user's own expense.

This equipment generates, uses, and can radiate radio frequency energy, and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception (which can be determined by turning the equipment off and on), the user is encouraged to try to correct the interference by taking one or more of the following measures:

- Reorient or relocate the receiving antenna
- Increase the separation between the equipment and receiver
- Plug the equipment into an outlet on a circuit different from that to which the receiver is currently connected
- Consult the dealer or an experienced radio/TV technician for help

This device must also accept any interference received, including interference that may cause undesired operation.



---

**WARNING:** *The 8208 is for use only with a certified Class 2 power supply. See Appendix B, "Specifications."*

---



---

**WARNING:** *Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.*

---

The 8208 complies with Part 68 of the FCC Rules and the requirements adopted by the ACTA. On the bottom of the 8208 unit is a label that contains, among other information, a product identifier in the format of US:GICDDNANNE8208. If requested, this number must be provided to the telephone company.

- 1 All direct connections to network lines must be made using standard plugs and jacks (compliant with Part 68 and the requirements adopted by the ACTA). A compliant telephone cord with a modular plug is provided with this product. It is designed to be connected to a compatible modular jack that is also compliant. See installation instructions for details. The table below presents a list of applicable registration jack USOCs and facility interface codes (FIC). These are required when ordering service from the telco.

IAD	Port ID	REN/SOC	FIC	USOC
8208	1.544 Mbps SF	6.0N	04DU9-BN	RJ-48C jack
	1.544 Mbps SF, B8ZS		04DU9-DN	
	1.544 Mbps ANSI ESF		04DU9-1KN	
	1.544 Mbps ANSI ESF, B8ZS		04DU9-1SN	
8308	SDSL	0.0B		RJ-11C

- 2 If the unit appears to be malfunctioning, it should be disconnected from the network lines until the source of trouble is determined to be your equipment or the telephone line. If your equipment needs repair, it should not be reconnected until it is repaired.
- 3 If your telephone equipment causes harm to the telephone network, the telephone company may discontinue your service temporarily. If possible, they will notify you in advance. However, if advance notice is not practical, you will be notified as soon as possible. You will be informed of your right to file a complaint with the FCC.
- 4 Your telephone company may make changes to its facilities, equipment, operations, or procedures that could affect the proper functioning of your equipment. If they do, you will be notified in advance so you can have the opportunity to maintain uninterrupted telephone service.
- 5 If you experience trouble with the 8208/8308 units, please contact Verilink for information on obtaining service or repairs (refer to “Support from Verilink” on page xxv). The telephone company may ask that you disconnect this equipment from the network until the problem has been corrected or until you are sure the equipment is not malfunctioning. No user serviceable parts are contained in this equipment. This equipment may not be used for coin service provided by the telephone company. Connection to party lines is subject to state tariffs. Contact the state Public Utilities Commission or Corporation for information. Do not attempt to repair this equipment yourself.

### Canadian Emissions Requirements

This digital apparatus does not exceed the Class A limits for radio noise emissions from digital apparatus set out in the Radio Interference Regulations of the Canadian Department of Communications.

Le présent appareil numérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques (de la class A) prescrites dans le Règlement sur le brouillage radioélectrique édicté par le ministère des Communications du Canada.

### Safety Precautions

When handling this equipment, follow these basic safety precautions to reduce the risk of electric shock and injury:

- Follow all warnings and instructions marked on the product and in the manual.
- Unplug the hardware from the wall outlet before cleaning. Do not use liquid cleaners or aerosol cleaners. Use a slightly damp cloth for cleaning.
- Do not place this product on an unstable cart, stand, or table. It may fall, causing serious damage to the product.
- Slots in the unit are provided for ventilation to protect it from overheating. These openings must not be blocked or covered. Never place this product near a radiator or heat register.

- This product should be operated only from the type of power source indicated on the marking label and manual. If you are unsure of the type of power supply you are using, consult your dealer or local power company.
- Do not allow anything to rest on the power cord. Do not locate this product where the cord interferes with the free movement of people.
- Do not overload wall outlets and extension cords, as this can result in fire or electric shock.
- Never push objects of any kind into the unit. They may touch dangerous voltage points or short out parts that could result in fire or electric shock. Never spill liquid of any kind on this equipment.
- Unplug the equipment from the wall outlet and refer servicing to qualified service personnel under the following conditions:
  - When the power supply cord or plug is damaged or frayed
  - If liquid has been spilled into the product
  - If the product has been exposed to rain or water
  - If the product has been dropped or if the housing has been damaged
- To reduce the risk of electrical shock, do not remove the cover from the unit or external power supply. There are no user-serviceable parts inside this unit. Contact qualified Verilink service personnel.

8216, 8224s, 8316s,  
8324s, 8512s, 8516s,  
8524s

## Copyright Notice

Copyright © 2004 Verilink Corporation. All rights reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form by any means without the written permission of Verilink.

Manual Reorder # 34-00333.B

September 2004

## Trademarks

Verilink® is a registered trademark of the Verilink Corporation.

All other brand and product names used herein are trademarks or registered trademarks of their respective manufacturers.

## Documentation Disclaimer

This document does not create any express or implied warranty about Verilink or about its products or services. Verilink's sole warranty is contained in its product warranty. The end-user documentation is shipped with Verilink's products and constitutes the sole specifications referred to in the product warranty. Verilink has made reasonable efforts to verify that the information contained herein is accurate, but Verilink assumes no responsibility for its use or for any infringement of patents or other rights of third parties that may result. The customer is solely responsible for verifying the suitability of Verilink's products for its use. Specifications are subject to change without notice.

## Warranty

Verilink's product warranty is included at the back of this document.

## FCC Requirements

This equipment has been tested and found to comply with the limits for a Class A digital device, except for the 8512, which complies with Class B limits, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user is required to correct the interference at the user's own expense.

This equipment generates, uses, and can radiate radio frequency energy, and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception (which can be determined by turning the equipment off and on), the user is encouraged to try to correct the interference by taking one or more of the following measures:

- Reorient or relocate the receiving antenna
- Increase the separation between the equipment and receiver
- Plug the equipment into an outlet on a circuit different from that to which the receiver is currently connected
- Consult the dealer or an experienced radio/TV technician for help

This device must also accept any interference received, including interference that may cause undesired operation.



---

**WARNING:** *The 8224/8324 and 8524 are for use only with a certified Class 2 power supply. See Appendix B, "Specifications."*

---



---

**WARNING:** *Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.*

---

The NetEngine 8224/8524 complies with Part 68 of the FCC Rules and the requirements adopted by the ACTA. On the bottom of the 8000 Series units is a label that contains, among other information, a product identifier in the format of US:GICDDNAN85xx or US:GICDDNAN82xx. If requested, this number must be provided to the telephone company.



- 1 All direct connections to network lines must be made using standard plugs and jacks (compliant with Part 68 and the requirements adopted by the ACTA). A compliant telephone cord with a modular plug is provided with this product. It is designed to be connected to a compatible modular jack that is also compliant. See installation instructions for details. The table below presents a list of applicable registration jack USOCs and facility interface codes (FIC). These are required when ordering service from the telco.

IAD	Port ID	REN/SOC	FIC	USOC
8224s	1.544 Mbps SF	6.0N	04DU9-BN	RJ-48C jack
	1.544 Mbps SF, B8ZS		04DU9-DN	
	1.544 Mbps ANSI ESF		04DU9-1KN	
	1.544 Mbps ANSI ESF, B8ZS		04DU9-1SN	
8324s	SDSL	0.0B		RJ-11C
8524s	SHDSL	0.0B		RJ-11C

- 2 If the unit appears to be malfunctioning, it should be disconnected from the network lines until the source of trouble is determined to be your equipment or the telephone line. If your equipment needs repair, it should not be reconnected until it is repaired.
- 3 If your telephone equipment causes harm to the telephone network, the telephone company may discontinue your service temporarily. If possible, they will notify you in advance. However, if advance notice is not practical, you will be notified as soon as possible. You will be informed of your right to file a complaint with the FCC.
- 4 Your telephone company may make changes to its facilities, equipment, operations, or procedures that could affect the proper functioning of your equipment. If they do, you will be notified in advance so you can have the opportunity to maintain uninterrupted telephone service.
- 5 If you experience trouble with the 8000 Series units, please contact Verilink for information on obtaining service or repairs (refer to “Support from Verilink” on page xxv). The telephone company may ask that you disconnect this equipment from the network until the problem has been corrected or until you are sure the equipment is not malfunctioning. No user serviceable parts are contained in this equipment. This equipment may not be used for coin service provided by the telephone company. Connection to party lines is subject to state tariffs. Contact the state Public Utilities Commission or Corporation for information. Do not attempt to repair this equipment yourself.

### Canadian Emissions Requirements

This digital apparatus does not exceed the Class A limits for radio noise emissions from digital apparatus set out in the Radio Interference Regulations of the Canadian Department of Communications.

Le présent appareil numérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques (de la class A) prescrites dans le Règlement sur le brouillage radioélectrique édicté par le ministère des Communications du Canada.

### Safety Precautions

When handling this equipment, follow these basic safety precautions to reduce the risk of electric shock and injury:

- Follow all warnings and instructions marked on the product and in the manual.
- Unplug the hardware from the wall outlet before cleaning. Do not use liquid cleaners or aerosol cleaners. Use a slightly damp cloth for cleaning.
- Do not place this product on an unstable cart, stand, or table. It may fall, causing serious damage to the product.
- Slots in the unit are provided for ventilation to protect it from overheating. These openings must not be blocked or covered. Never place this product near a radiator or heat register.
- This product should be operated only from the type of power source indicated on the marking label and manual. If you are unsure of the type of power supply you are using, consult your dealer or local power company.
- Do not allow anything to rest on the power cord. Do not locate this product where the cord interferes with the free movement of people.

- Do not overload wall outlets and extension cords, as this can result in fire or electric shock.
- Never push objects of any kind into the unit. They may touch dangerous voltage points or short out parts that could result in fire or electric shock. Never spill liquid of any kind on this equipment.
- Unplug the equipment from the wall outlet and refer servicing to qualified service personnel under the following conditions:
  - When the power supply cord or plug is damaged or frayed
  - If liquid has been spilled into the product
  - If the product has been exposed to rain or water
  - If the product has been dropped or if the housing has been damaged
- To reduce the risk of electrical shock, do not remove the cover from the unit or external power supply. There are no user-serviceable parts inside this unit. Contact qualified Verilink service personnel.

# Table of Contents

## *Preface*

About this Manual .....	xxiii
Products Covered by this Manual .....	xxiii
Manual Organization .....	xxiii
Typographic Conventions .....	xxiv
Customer Service and Technical Support .....	xxiv
Support from Your Network Supplier .....	xxiv
Support from Verilink .....	xxv
Telephone .....	xxv
E-mail .....	xxv
Internet .....	xxv
Returning a Unit to Verilink .....	xxvi

## *Chapter 1 Introduction*

Interfaces and Features of the	
Low POTS Port Platform Architecture .....	1-2
Low POTS Port Platform Architecture .....	1-2
Low POTS Port Features .....	1-2
Low POTS Port Front Panel LED Status Indicators .....	1-3
Low POTS Port Rear Panel Connectors .....	1-4
Interfaces and Features of the	
High POTS Port Platform Architecture .....	1-6
High POTS Port Platform Architecture .....	1-6
High POTS Port Features .....	1-6
High POTS Port Front Panel LED Status Indicators .....	1-7
High POTS Port Rear Panel Connectors .....	1-8

## *Chapter 2 Quick Start Guide*

Unpacking the IAD .....	2-1
Installing the IAD .....	2-2
AC Power and Uninterruptible Power Supply .....	2-2
Clearance Requirements .....	2-2
Wiring Requirements .....	2-2
Connecting the IAD Via a Terminal Emulator .....	2-2
Connecting the IAD to a PC .....	2-3
Logging in via a Terminal Emulation Program .....	2-4
Setting the Ethernet Port IP Address .....	2-6
Setting the WAN Port IP Address .....	2-8
Resetting the IAD .....	2-8
Connecting via Telnet .....	2-9

Running Telnet .....	2-9
Basic IAD Configuration .....	2-11
Connecting LAN, WAN, and Telephones .....	2-11
Ethernet LAN Connection .....	2-11
WAN Connections .....	2-12
Telephone Connections .....	2-12
Life Line Connection .....	2-12
USI Connection .....	2-12
Confirming Proper Setup .....	2-13

## ***Chapter 3 Administration***

IAD Security .....	3-1
Password Configuration Menu .....	3-2
Change User ID .....	3-3
Change User Password .....	3-4
RADIUS Server Settings .....	3-4
Setting Up SNMP .....	3-5
SNMP Configuration Menu .....	3-6
Enable/Disable SNMP via IP .....	3-7
Enable/Disable SNMP via EOC .....	3-7
Enable SNMP via Both IP and EOC .....	3-7
Disable SNMP via Both IP and EOC .....	3-7
Configure System Contact .....	3-7
Configure System Name .....	3-8
Configure System Location .....	3-8
Configure SNMP Community .....	3-8
Configure SNMP Trap Host IP Address .....	3-9
Enable/Disable SNMP Traps via EOC .....	3-9
Configure Restart Trap Maximum Delay .....	3-9
Defining Different SNMP Version 3 Categories .....	3-9
LAN Configuration Menu .....	3-11
Establishing LAN Speed and Duplex Mode .....	3-11
Upgrading the System .....	3-11
Using TFTP Servers via LAN or WAN .....	3-12
Copying the Source Files .....	3-12
Upgrading via TFTP .....	3-12
Verifying the Upgrade .....	3-13
Utilities Menu .....	3-13
Ping Utility .....	3-14
Trace Route .....	3-15
Configure Console Baud Rate .....	3-15
Configure Console Timeout .....	3-15
Reset or Reload ACOS from FLASH .....	3-16
Set System Defaults .....	3-16
Save System Settings as Defaults .....	3-16
Display Event Log .....	3-17
Clear “Last Reset Reason” .....	3-17

Time Zone Menu .....	3-18
Display Configuration File .....	3-18
File System Menu .....	3-18
Directory of all Files .....	3-19
Copy File .....	3-19
Rename File .....	3-19
Delete File .....	3-19
Format File System Drive .....	3-20
Space Left in File System .....	3-20
File Transfer Menu .....	3-20
Load Boot ROM .....	3-20
Update ACOS [acos.bin] .....	3-21
Update Entire System .....	3-21
File Transfer Utilities .....	3-21
TFTP Server Menu .....	3-22

## ***Chapter 4 Configuration***

Introduction .....	4-1
Managing Configuration Files .....	4-1
WAN Configuration .....	4-2
Basic WAN Setup Tasks .....	4-2
Setting the WAN Port IP Address .....	4-3
Identifying the WAN Interface and Datalink Protocol .....	4-3
WAN Configuration Menu .....	4-4
Configure Physical Interface - SDSL .....	4-6
Quick Configuration for SDSL WAN .....	4-9
Configure Physical Interface - T1/E1 .....	4-10
Configure Physical Interface - ADSL .....	4-18
Configure Physical Interface - SHDSL .....	4-19
Configure Physical Interface - USI .....	4-21
Configure Datalink Protocol .....	4-21
Configure ATM PVCs .....	4-24
Configure ATM Options .....	4-30
Configure DLCIs .....	4-32
Configure Frame Relay Options .....	4-35
Router Configuration .....	4-38
Basic Router Setup Tasks .....	4-39
Router Configuration Menu .....	4-39
Configure Port IP Address .....	4-40
Unconfigure Port IP Address .....	4-41
Configure Port Maximum Transmission Unit (MTU) .....	4-42
Add/Remove a Static or Source Route .....	4-42
Enable/Disable RIP .....	4-44
Configure RIP Version by Port .....	4-44
Configure RIP Poisoned Reverse by Port .....	4-45
Configure DNS Client .....	4-45
Configure DHCP Client .....	4-46

Configure DHCP Relay .....	4-47
Configure Telnet Server Port .....	4-48
Configure IP QoS .....	4-48
Configure IP Filtering .....	4-49
Configure IP Header Compression (IPHC) .....	4-50
Configure LAN IP Broadcast Destination .....	4-51
Configure Domain Name .....	4-51
Configure Host Name .....	4-51
Remove Host and Domain Names .....	4-52
Display Route Table .....	4-52
Bridge Configuration .....	4-52
Basic Bridge Setup Tasks .....	4-53
Bridge Configuration Menu .....	4-54
Enabling and Disabling Bridging .....	4-55
IP Over Bridging .....	4-55
Enable/Disable Bridging Globally .....	4-56
Enable/Disable Bridging by Port .....	4-56
Bridge Aging Timer .....	4-57
Enabling and Disabling Spanning Tree .....	4-57
Enable/Disable Spanning Tree Globally .....	4-57
Enable/Disable Spanning Tree by Port .....	4-58
Configure Spanning Tree Bridge Priority .....	4-58
Configure Spanning Tree Port Priority .....	4-58
Configure Spanning Tree Hello Time .....	4-59
Configure Spanning Tree Maximum Age .....	4-59
Configure Spanning Tree Forward Delay .....	4-59
Configure Spanning Tree Path Cost .....	4-60
Delete Bridge Forwarding Database Entry .....	4-60
Voice Path Configuration .....	4-60
Basic Voice Path Setup Tasks .....	4-61
Voice Configuration Menu .....	4-61
Set Voice Gateway .....	4-61
Set Jitter Delay .....	4-77
Voice Port Settings .....	4-78
Display Comander Mode ( $\mu$ -law, A-law) .....	4-82
Set Country Mode .....	4-83
Set DuSLIC Mode .....	4-83
Enable/Disable G726 Annex A .....	4-83
Interworking Connections .....	4-83
FRF.5 .....	4-85
FRF.8 .....	4-86
Firewall Configuration .....	4-87
Creating a Firewall via IP Filtering and NAT .....	4-87
DHCP Server Configuration .....	4-88
Basic DHCP Server Setup Tasks .....	4-88
DHCP Server Configuration Menu .....	4-88
Enable/Disable DHCP Server .....	4-89
Enable/Disable Checking Additional DHCP Servers .....	4-89

Configure DHCP Server Parameters .....	4-89
Configure DHCP Address Range Pool .....	4-90
Configure DHCP Client Entry .....	4-90
Display DHCP Configuration .....	4-91
Display DHCP Server Statistics .....	4-92
Display DHCP Server Assigned and Unassigned Addresses .....	4-92
Display DHCP Entry Details .....	4-93
Delete a DHCP Client Entry .....	4-93
Delete a DHCP Assignment Entry .....	4-93
Multicast Configuration .....	4-94
Multicast Configuration Menu .....	4-94
Enable/Disable Global IP Multicasting .....	4-94
Configure PIM - Dense Mode by Port .....	4-95
Add/Change Multicast Route Source .....	4-95
Show IGMP Group .....	4-96
Show IGMP Querier .....	4-96
Show Multicast Routing Table .....	4-97
Show PIM Neighbor .....	4-98
NAT Configuration .....	4-98
NAT Configuration Menu .....	4-99
Enable/Disable NAT Translation by Port .....	4-100
Configure NAT TCP and UDP Timeouts .....	4-100
Configure NAT Port Range .....	4-100
Configure NAT Local Server Entry .....	4-101
Configure NAT Alias Entry .....	4-102
Display NAT Statistics .....	4-103
Display NAT Connection Table .....	4-104
Display NAT Connection Details .....	4-104
Display NAT Local Server Table .....	4-105
Display NAT Alias Table .....	4-105
Delete IP Address from NAT Tables .....	4-105
Delete NAT Local Server Entry .....	4-106
Delete NAT Alias Entry .....	4-106
Setting PPP Options .....	4-106
Setting Derived Timing Options .....	4-107
Derived Timing Menu .....	4-107
Enable/Disable Derived Timing .....	4-107

## ***Chapter 5 Reports***

Reports Menu .....	5-1
Current Configuration Report .....	5-2
Network Statistics Reports .....	5-4
ICMP Statistics Report .....	5-5
IGMP Statistics Report .....	5-6
IP Statistics Report .....	5-8
PIM Statistics Report .....	5-9
TCP Statistics Report .....	5-10

UDP Statistics Report .....	5-12
Clear Network Statistics .....	5-12
Interface Statistics Reports .....	5-13
Display Interface Statistics .....	5-14
Display DLCI Statistics .....	5-15
Display ATM PVC Statistics .....	5-16
Display Bridge Statistics .....	5-21
Clear Interface Statistics .....	5-22
Media Statistics Reports .....	5-22
Display Frame Relay Statistics .....	5-23
Display ATM Statistics .....	5-24
Display G7070 ADSL Statistics (81xx) .....	5-25
Display G2237 xDSL Statistics (85xx) .....	5-26
Display Serial (USI) Statistics (8216s/8224s/8316s/8324s/8512s/8516s/8524s) .....	5-27
Display Ethernet Statistics .....	5-28
Display POTS Statistics .....	5-30
Clear Media Statistics .....	5-30
Route Table Report .....	5-30
ARP Table Report .....	5-31
Bridge Forwarding Database Report .....	5-31
Bridge Status Report .....	5-32
PPP Authorization Entries Report .....	5-32
System Uptime Report .....	5-33
Memory Statistics Reports .....	5-33
Display System Memory Statistics .....	5-33
Display Kernel Tasks Memory Statistics .....	5-33
Tasks Run Time .....	5-34
Zero All Statistics .....	5-34

## ***Chapter 6 Command Line Interface***

Introduction .....	6-1
CLI Help .....	6-1

## ***Chapter 7 Troubleshooting and Diagnostics***

Using the Diagnostics Menu .....	7-1
POTS Diagnostics .....	7-2
Dialup Test .....	7-2
Hotline Test .....	7-3
Ring Test .....	7-3
Ring Test .....	7-3
On/Off Hook Test .....	7-4
SDSL Diagnostics .....	7-5
Troubleshooting the IAD .....	7-5



## **Chapter 8 Verification**

Power-up Test .....	8-1
Operational Test .....	8-1
Testing the IAD .....	8-2
Maintenance .....	8-2
Displaying the Current Configuration .....	8-2

## **Appendix A Menu Map**

## **Appendix B Specifications**

T1/E1 (8208/8208s) .....	B-1
Voice Features .....	B-1
Analog Voice .....	B-1
Digital Voice .....	B-1
Data Features .....	B-2
WAN Features .....	B-2
Network Interfaces .....	B-2
T1 .....	B-2
E1 .....	B-3
T1/E1 Provisioning (8208s Only) .....	B-3
ATM .....	B-3
Frame Relay .....	B-3
Configuration and Management .....	B-4
10/100 Ethernet (Management or IP Gateway) .....	B-4
Supervisory Port .....	B-4
Upgrades .....	B-4
Management .....	B-4
Security Features .....	B-4
Integrated Firewall .....	B-4
Management Interfaces .....	B-4
Alarms .....	B-4
Diagnostics .....	B-4
Environmental .....	B-5
Connector Pin Assignments .....	B-6
Console Port Pin Assignments (DB-9) .....	B-6
POTS Port Pin Assignments (RJ-11) .....	B-6
10/100Base-T Connector Pin Assignments (RJ-45) .....	B-6
T1/E1 Connector Pin Assignments (RJ-48) .....	B-6
T1/E1 (8216s and 8224s) .....	B-7
Voice Features .....	B-7
Analog Voice .....	B-7
Digital Voice .....	B-7
Data Features .....	B-7
WAN Features .....	B-8
Network Interfaces .....	B-8

T1 .....	B-8
E1 .....	B-8
T1/E1 Provisioning .....	B-9
ATM .....	B-9
Frame Relay .....	B-9
Universal Serial Interface (DB-25) .....	B-9
Configuration and Management .....	B-9
10/100 Ethernet (Management or IP Gateway) .....	B-9
Supervisory Port .....	B-10
Upgrades .....	B-10
Management .....	B-10
Security Features .....	B-10
Integrated Firewall .....	B-10
Management Interfaces .....	B-10
Alarms .....	B-10
Diagnostics .....	B-10
Environmental .....	B-10
Connector Pin Assignments .....	B-12
Console Port Pin Assignments (DB-9) .....	B-12
POTS Port Pin Assignments (RJ-21) .....	B-12
10/100Base-T Connector Pin Assignments (RJ-45) .....	B-12
T1/E1 Connector Pin Assignments (RJ-48) .....	B-12
USI Connector Pin Assignments (RS-530, V.35) .....	B-13
SDSL (8304/8304s and 8308/8308s) .....	B-14
Voice Features .....	B-14
Analog Voice .....	B-14
Digital Voice .....	B-14
Data Features .....	B-14
WAN Features .....	B-15
Interface .....	B-15
ATM .....	B-15
Frame Relay .....	B-15
Configuration and Management .....	B-16
10/100 Ethernet (Management or IP Gateway) .....	B-16
Supervisory Port .....	B-16
Upgrades .....	B-16
Management .....	B-16
Security Features .....	B-16
Integrated Firewall .....	B-16
Management Interfaces .....	B-16
Alarms .....	B-16
Environmental .....	B-16
Connector Pin Assignments .....	B-18
Console Port Pin Assignments (DB-9) .....	B-18
POTS Port Pin Assignments (RJ-11) .....	B-18
10/100Base-T Connector Pin Assignments (RJ-45) .....	B-18
SDSL Connector Pin Assignments (RJ-11) .....	B-18
SDSL (8316s and 8324s) .....	B-19
Voice Features .....	B-19
Analog Voice .....	B-19

Digital Voice .....	B-19
Data Features .....	B-19
WAN Features .....	B-20
Interface .....	B-20
ATM .....	B-20
Frame Relay .....	B-20
Universal Serial Interface (DB25) .....	B-21
Configuration and Management .....	B-21
10/100 Ethernet (Management or IP Gateway) .....	B-21
Supervisory Port .....	B-21
Upgrades .....	B-21
Management .....	B-21
Security Features .....	B-21
Integrated Firewall .....	B-21
Management Interfaces .....	B-21
Alarms .....	B-21
Environmental .....	B-22
Connector Pin Assignments .....	B-23
Console Port Pin Assignments (DB-9) .....	B-23
POTS Port Pin Assignments (RJ-21) .....	B-23
10/100Base-T Connector Pin Assignments (RJ-45) .....	B-23
SDSL Connector Pin Assignments (RJ-11) .....	B-23
USI Connector Pin Assignments (RS-530, V.35) .....	B-23
ADSL (8104/8104s and 8108/8108s) .....	B-25
Voice Features .....	B-25
Analog Voice .....	B-25
Digital Voice .....	B-25
Data Features .....	B-25
WAN Features .....	B-26
Interface .....	B-26
ATM .....	B-26
Configuration and Management .....	B-26
10/100 Ethernet (Management or IP Gateway) .....	B-26
Supervisory Port .....	B-27
Upgrades .....	B-27
Management .....	B-27
Security Features .....	B-27
Integrated Firewall .....	B-27
Management Interfaces .....	B-27
Alarms .....	B-27
Environmental .....	B-27
Connector Pin Assignments .....	B-28
Console Port Pin Assignments (DB-9) .....	B-28
SHDSL Connector Pin Assignments (RJ-45) .....	B-28
10/100Base-T Connector Pin Assignments (RJ-48) .....	B-28
ADSL Pin Assignments (RJ-11) .....	B-28
SHDSL (8504/8504s and 8508/8508s) .....	B-29
Voice Features .....	B-29
Analog Voice .....	B-29
Digital Voice .....	B-29

Data Features .....	B-29
WAN Features .....	B-30
Interface .....	B-30
ATM .....	B-30
Configuration and Management .....	B-30
10/100 Ethernet (Management or IP Gateway) .....	B-30
Supervisory Port .....	B-31
Upgrades .....	B-31
Management .....	B-31
Security Features .....	B-31
Integrated Firewall .....	B-31
Management Interfaces .....	B-31
Alarms .....	B-31
Environmental .....	B-31
Connector Pin Assignments .....	B-32
Console Port Pin Assignments (DB-9) .....	B-32
POTS Port Pin Assignments (RJ-11) .....	B-32
10/100Base-T Connector Pin Assignments (RJ-45) .....	B-32
SHDSL Connector Pin Assignments (RJ-11) .....	B-32
SHDSL (8512s, 8516s, and 8524s) .....	B-33
Voice Features .....	B-33
Analog Voice .....	B-33
Digital Voice .....	B-33
Data Features .....	B-33
WAN Features .....	B-34
Interface .....	B-34
ATM .....	B-34
Universal Serial Interface (DB25) .....	B-34
Frame Relay (USI Interface Only) .....	B-34
Configuration and Management .....	B-35
10/100 Ethernet (Management or IP Gateway) .....	B-35
Supervisory Port .....	B-35
Upgrades .....	B-35
Management .....	B-35
Security Features .....	B-35
Integrated Firewall .....	B-35
Management Interfaces .....	B-35
Alarms .....	B-35
Environmental .....	B-35
Connector Pin Assignments .....	B-37
Console Port Pin Assignments (DB-9) .....	B-37
POTS Port Pin Assignments (RJ-21) .....	B-37
10/100Base-T Connector Pin Assignments (RJ-45) .....	B-37
SHDSL Connector Pin Assignments (RJ-11) .....	B-37
USI Connector Pin Assignments (RS-530, V.35) .....	B-38

## ***Appendix C Applications Notes***

Frame Relay .....	C-1
Setting the Fragment (Maximum Frame) Size .....	C-1
Peak Cell Rate (PCR) Considerations and Recommendations .....	C-2
Voice-only Applications .....	C-2
Voice and Data Applications .....	C-2
Network Address Translation (NAT) .....	C-2
Accessing the Internet from the LAN .....	C-3
Configuring NAT Port Range .....	C-3
Configuring NAT TCP Timeout .....	C-3
Configuring NAT UDP Timeout .....	C-3
Accessing LAN Devices from the Internet .....	C-3
NAT Local Server Configuration .....	C-4
NAT Alias Configuration .....	C-4
IP Filtering .....	C-4
Information Policy .....	C-5
Filtering Interface .....	C-5
IP Packet Filtering Syntax and Grammar .....	C-7
Grammar .....	C-7
Filter Rules .....	C-8
Actions .....	C-8
Options .....	C-9
Matching Parameters .....	C-9
Keep History .....	C-11
Examples .....	C-12
Dial Plan .....	C-12

## ***Appendix D Glossary***



# PREFACE

## About this Manual

---

This reference guide for the 8000 Series describes IAD features and specifications, configuration, and cabling. It is *not* a users guide containing step-by-step procedures. This manual is designed to be used as a reference regarding commands, interface ports, configuration parameters, and other information specific to your IAD.

## Products Covered by this Manual

**ADSL:** 8104, 8104s, 8108, 8108s

**T1/E1:** 8208, 8208s, 8216s, 8224s

**SDSL:** 8304, 8304s, 8308, 8308s, 8316s, 8324s

**SHDSL:** 8504, 8504s, 8508, 8508s, 8512s, 8516s, 8524s

## Manual Organization

The chapters and appendices in this manual are arranged for quick reference when you need it. We recommend that you first read the Quick Start Guide and then refer to the remaining chapters for more detailed information. Appendices are designed to complement the main chapters.




- *Chapter 1, "Introduction"* – introduces the features of the 8000 Series IADs, including the hardware, indicators, and ports.
- *Chapter 2, "Quick Start Guide"* – describes the process of getting an IAD up and running in a typical customer premises. This chapter is helpful if you're new to Verilink 8000 Series products, because it lists each step, beginning with unpacking the IAD. It also provides information about logging on, using the menu interface, setting the IP address, basic configuration tasks, and restarting the IAD. The subsequent chapters provide more detailed information.
- *Chapter 3, "Administration"* – provides information about security, configuring Simple Network Management Protocol (SNMP), upgrading ACOS, system utilities, and other topics.
- *Chapter 4, "Configuration"* – details how to configure the 8000 Series for physical connection to the network (T1/E1 and SDSL, frame relay and ATM,

and TDM voice for channelized T1/E1 circuits) as well as router, bridge, voice path, firewall, DHCP, Multicast, and NAT configuration.

- *Chapter 5, "Reports"* – describes the reports you can run.
- *Chapter 6, "Command Line Interface"* – describes how to enter and exit CLI mode, and how to use each command in the command line interface. You may use these commands instead of using the corresponding commands in the menu interface.
- *Chapter 7, "Troubleshooting and Diagnostics"* – shows you how to troubleshoot and diagnose your configuration when abnormal symptoms occur in the voice or computer network.
- *Chapter 8, "Verification"* – describes the steps you take to verify normal operation once you've installed, connected, and configured your IAD. It also covers maintenance and how to display the current configuration.
- *Appendix A, "Menu Map"* – provides a graphic view of your IAD's menu interface, illustrating its navigation and organization.
- *Appendix B, "Specifications"* – defines the specifications for the 8000 Series IADs. In addition, this section provides ordering information and all the connector pin assignments for the interfaces on the back of the 8000 Series IADs.
- *Appendix C, "Applications Notes"* – provides various applications details.
- *Appendix D, "Glossary"* – provides a glossary of terms used in this manual.

## Typographic Conventions

The following table lists the conventions used throughout this guide.

Convention	Description
	A <i>Notice</i> calls attentions to important features or instructions.
	A <i>Caution</i> alerts you to serious risk of data loss or other results that may cause you or the IAD trouble if the warning is not heeded.
	A <i>Warning</i> alerts you to the risk of serious damage to the IAD or injury and possible death to the end user.

## Customer Service and Technical Support

---

Verilink provides easy access to customer support information through a variety of services. This section describes these services.

### Support from Your Network Supplier

If assistance is required, contact your network supplier. Many suppliers are authorized Verilink service partners who are qualified to provide a variety of



services, including network planning, installation, hardware maintenance, application training, and support services. When you contact your network supplier for assistance, have the following information ready:

- Diagnostic error messages
- A list of system hardware and software, including revision levels
- Details about recent configuration changes, if applicable

## Support from Verilink

If you are unable to receive support from your network supplier or want to contact us directly, Verilink offers worldwide customer support by telephone, e-mail, and through Verilink's Internet Web site.

### Telephone

Customer support is available 8–5 CST, Monday–Friday. To speak directly with a Verilink customer service representative, you may dial one of the following numbers:

- Sales and Marketing: 800-VERILINK (837-4546)
- Technical Support: 800-285-2755 (toll-free)  
256-327-2255 (local)
- Customer Service: 800-926-0085 ext. 3002 (toll-free)
- Out-of-Warranty Repair FAX Number for Purchase Order:  
256-772-3388

### E-mail

You can request sales and marketing information or pose a technical support question about your Verilink product by contacting us at the e-mail addresses provided below. Verilink will respond to e-mailed requests for support during regular business hours (8–5 CST, Monday–Friday).

- Sales and Marketing: [info@verilink.com](mailto:info@verilink.com)
- Technical Support: [support@verilink.com](mailto:support@verilink.com)

### Internet

Visit Verilink's Web site to access the latest Verilink product information, technical publications, news releases, contact information, and more:

<http://www.verilink.com>

If this reference manual is revised to reflect code changes or other updates, the most recent version will be posted to the Verilink Web site.

## Returning a Unit to Verilink

---

If for any reason you must return your Verilink product, it must be returned with the shipping prepaid, and packaged to the best commercial standard for electronic equipment. For in-warranty repair, Verilink will pay shipping charges for delivery on return. You are responsible for mode and cost of shipment to Verilink.

You must have a Return Material Authorization (RMA) number marked on the shipping package. To obtain an RMA number, call Customer Service at 800-926-0085, extension 3002. Products sent to Verilink without RMA numbers will be returned to the sender unopened, at the sender's expense.

When calling Verilink for an RMA, please have the following information available:

- Model number and serial number for each unit
- Reason for return and symptoms of problem
- Purchase order number to cover charges for out-of-warranty items (Faxed purchase order required)
- Name and phone number of person we can contact if we have questions about the unit(s)

The address for you to use when returning a unit to Verilink will be provided when the RMA is issued. The standard delivery method for return shipments is Standard Ground for domestic returns and International Economy for international returns (unless otherwise specified).

## INTRODUCTION

This chapter introduces the Verilink 8000 Series integrated access devices (IADs) and describes their hardware and software.

As competition in the telecommunications market intensifies, carriers find themselves under growing pressure to reduce network costs and deliver differentiated, highly competitive services. In response to this challenge, Verilink provides a family of IADs that incorporates the capabilities of multiple networking devices capable of supporting multiple networking protocols such as TDM, Frame Relay, and ATM, and multiple applications such as the integration of voice/data and high-speed internet access. By consolidating multiple network devices, converging multiple services, and moving intelligence to the network's edge, Verilink's 8000 Series IADs lower requirements for capital equipment, minimize operational expenditures, and maximize carriers' profits. Using the Verilink Series 8000 IADs to integrate legacy networks into evolving infrastructures, service providers can now also enable budget-constrained customers to leverage the power of wide-area communications for competitive advantage. In particular, these new services allow SMBs, often lacking the resources to install and manage multiple communications devices, to compete effectively with their larger counterparts in the global marketplace.

The 8000 IADs are access devices that terminate a network WAN, and provide the end user with the ability to send and receive both voice calls and data transmissions via a single connection. The network WAN connection may be either T1, E1, SDSL, ADSL, or SHDSL. The High POTS Port models have from 12 to 24 POTS ports that have metal housing and a Universal Serial Interface (USI). The Low POTS Port models have from 4 to 8 POTS ports that provide service via individual RJ-11 ports. Low POTS Port models are encased in a plastic housing. All models are equipped with a 10/100Base-T Ethernet interface with integrated routing protocols and functionality.

The built-in flexibility of the 8000 Series, supporting emerging protocols such as MGCP and SIP, enables the IAD to evolve with the network, and provides an easily managed, cost-effective migration to VoIP. The "s" version of the 8000 Series IADs provides a single unit solution that can support VoATM and VoIP applications in a single unit. The 8208s, 8216s, and 8224s also

support TDM. This provides the user with CPE investment protection, reduced inventory and training requirements, as well as a built-in migration path from TDM or VoATM to VoIP by a simple reconfiguration of the unit. No costly truck rolls or forklift upgrades are required.

The Verilink IADs are ideal for service providers, offering small businesses or home offices high-quality voice and data service over broadband circuits. The 8000 Series supports any POTS device via a voice subsystem, and any IP-based computer system (Ethernet printers; personal computers, including Windows, Macintosh, Unix, Linux, etc.; network file servers, and other network devices via a LAN subsystem.

## Interfaces and Features of the Low POTS Port Platform Architecture

---

### Low POTS Port Platform Architecture

The Low POTS Port IADs are based on a single-board, fixed-configuration architecture. Each unit supports one WAN interface (T1/E1, SDSL, ADSL, SHDSL), one LAN interface, and four or eight POTS interfaces. The units are housed in a plastic enclosure with an external power supply.

All units are based on a common core design consisting of a Motorola Power QUICC CPU, 16 or 8 Mbytes of dynamic memory, and 2 Mbytes of FLASH memory. Voice packetization and processing are handled by Texas Instruments Digital Signal Processors (DSP).

### Low POTS Port Features

The Verilink Low POTS Port IADs provide a highly interoperable, cost-effective voice and high-speed data integration solution that is compatible with industry-leading DSLAM and Voice Gateway manufacturers. These IADs prioritize voice packets and dynamically allocate bandwidth between voice and data services. Features include the following:

- For SDSL, supports the following DSLAMs:
  - ATM: Lucent, Nortel, and Nokia
  - Frame Relay: AccessLan, CopperMountain, and Paradyne.
- Supports the following Voice Gateways: CopperCom, JetStream, TdSoft, Broadsoft, MetaSwitch, Cirpack, NuERA Tollbridge, Nortel, General Bandwidth, Accelerated
- Provides seamless voice and high-speed data integration over SDSL, T1/E1, ADSL, or SHDSL
- Supports data from POTS and 10/100Base-T customer premise interfaces
- Compatible with standards-based IP, ATM, and Frame Relay WAN protocols
- Provides RJ-11 POTS interface with Loop Start or Ground Start

- Provides dynamic and static IP routing and bridging capabilities
- Provides firewall support via IP filtering
- Offers DHCP and NAT to support IP address management
- The “s” versions provide support for MGCP and SIP with the flexibility to support TDM/VoATM/VoIP applications all in one unit
- Provides management capabilities including Telnet, SNMP, and TFTP

The Low POTS Port IADs are characterized by their different WAN interfaces:

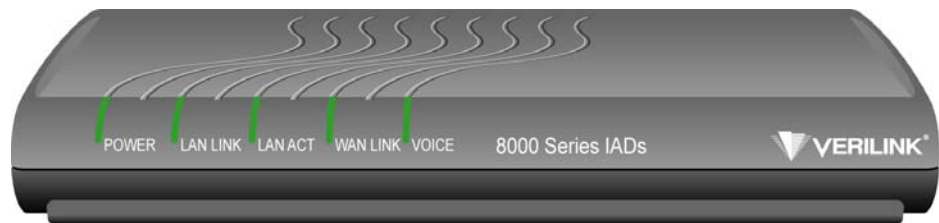
- **8208** – provides voice services and WAN access via T1 or E1.
- **8308/8304** – provides voice services and WAN access via SDSL.
- **8108/8104** – provides voice services and WAN access via ADSL.
- **8508/8504** – provides voice services and WAN access via SHDSL.

Physical and electrical specifications for the 8208, 8308/8304, 8108/8104, and 8508/8504 IADs are listed in Appendix B, *Specifications*.

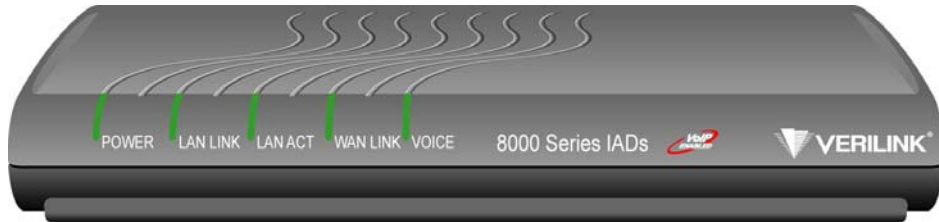
## Low POTS Port Front Panel LED Status Indicators

The Low POTS Port front panels contain five LED status indicators. Each is described in the table below.

**Figure 1.1** *Low POTS Port Non-“s” Version Front Panel*



**Figure 1.2** *Low POTS Port “s” Version Front Panel*



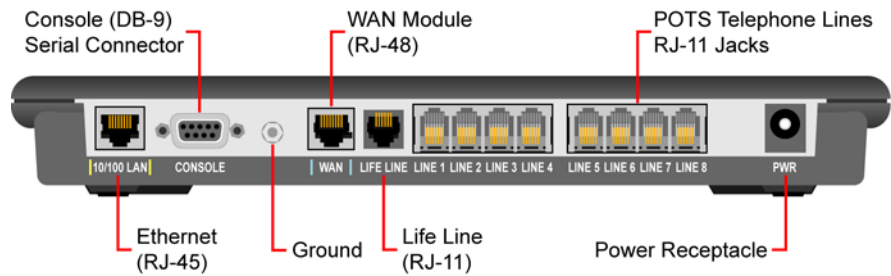
LED	Description
<b>POWER</b>	Illuminates when the IAD is powered on.
<b>LAN LINK</b>	Illuminates when there is an operational LAN connection on the Ethernet port.
<b>LAN ACT</b>	Flashes when there is activity on the Ethernet port.

LED	Description
<b>WAN LINK</b>	Flashes as the IAD is establishing a link, and illuminates solid when there is a proper connection on the WAN port and synchronization has been achieved.
<b>VOICE</b>	Illuminates when there is activity on the voice ports. When connected to a CopperCom and Jetstream Voice Gateway, it remains lit, and blinks when there is activity. (This LED does not remain lit when other types of voice gateways are connected, but will illuminate when a call is active.)

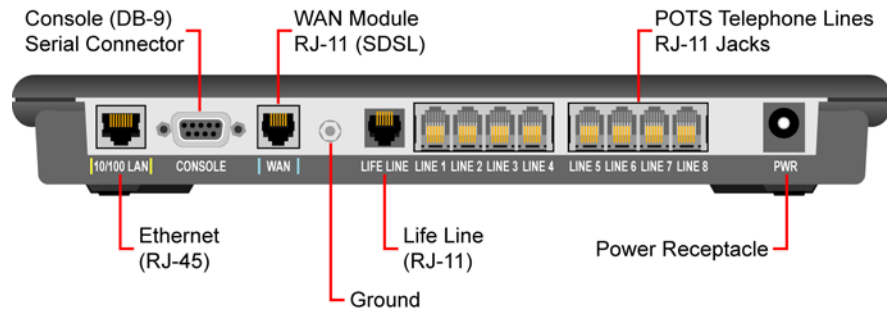
## Low POTS Port Rear Panel Connectors

The Low POTS Port rear panels have the following connectors: **10/100 LAN**, **CONSOLE**, **WAN**, **LIFE LINE**, **LINE 1-8 telephone connectors**, and **PWR**. Each of these connectors is described below. Each unit has a **Ground**, the use of which is illustrated in Figure 2.1.

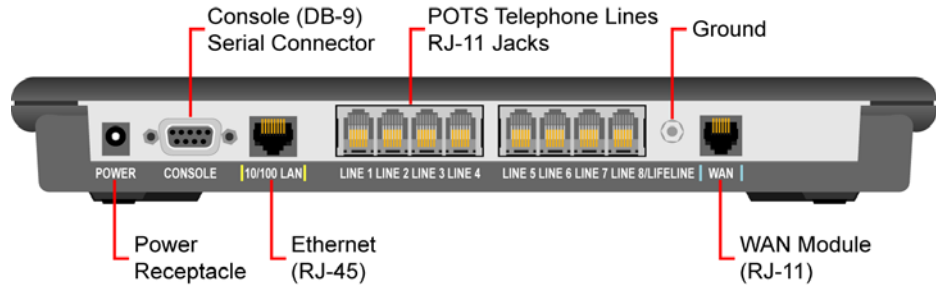
**Figure 1.3** *T1/E1 Low POTS Port Rear Panel Connectors*



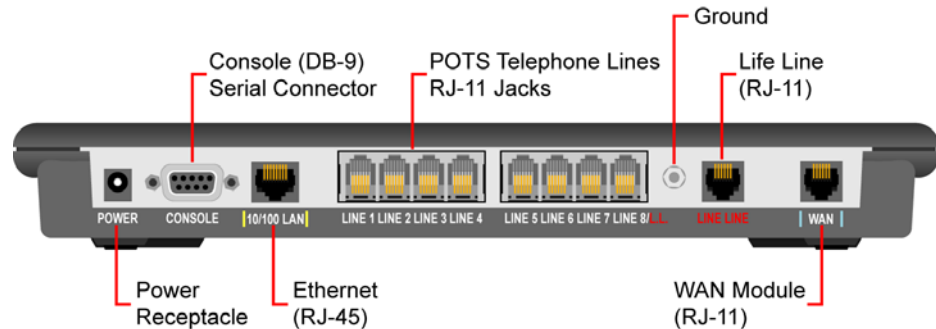
**Figure 1.4** *SDSL Low POTS Port Rear Panel Connectors*



**Figure 1.5** ADSL Low POTS Port Rear Panel Connectors



**Figure 1.6** SHDSL Low POTS Port Rear Panel Connectors



**POWER (DC Power Adapter)**

Connects the IAD to any AC 100-240 V outlet (adapter included).

**Console (RS-232 Serial Port)**

Connects the IAD to a PC using a straight-through nine-pin serial (DB-9) cable, for the purpose of using a terminal emulator for IAD configuration and management.

**10/100LAN (10/100Base-T Ethernet Port)**

Connects the IAD to the local area network using a CAT-5 straight-through Ethernet cable, or directly to a PC for accessing via Telnet (using a cross-over, customer-supplied cable).

**LINE 1-8 (Telephone Interfaces)**

Supports eight analog telephones via RJ-11 POTS ports.

**LIFE LINE**

Provides access to a telephone line when there is no power or voice gateway to the IAD. Refer to *Life Line Connection* on page 2-12 for a description of which unit uses which port for the Life Line connection.



**NOTICE:** *The 8108 also uses the WAN connection for the Life Line connection.*

**WAN**

Connects through WAN interface as follows:

- 8208 – T1/E1 (uses an RJ-48 connector)
- 8308/8304 – SDSL (uses an RJ-11 connector)
- 8108/8104 – ADSL (uses an RJ-11 connector).

- 8508/8504 – SHDSL (uses an RJ-11 connector).

**Data Interfaces** The data connection through the IAD supports IEEE 802.1-compliant bridging and routing. When the IAD is configured for routing, it supports Routing Information Protocol (RIP) version 1, version 2, or static IP routing. The IAD complies with RFC-1812 when interfacing with IPV4 routers. The IAD can terminate the following data interfaces:

- ATM data transport via SDSL, SHDSL, and T1/E1 per RFC 1483 or RFC 2364
- Frame Relay data transport via SDSL and T1/E1 per RFC 1490
- Frame Relay data transport per RFC 1483 with Q.922 frames

## Interfaces and Features of the High POTS Port Platform Architecture

---

### High POTS Port Platform Architecture

The High POTS Port IADs are based on a single-board, fixed-configuration architecture. Each unit supports 1 WAN interface (T1/E1, SDSL, SHDSL), 1 LAN interface, and 12, 16, or 24 POTS interfaces via an RJ-21 connector. These units are housed in a metal enclosure with an internal power supply. All units are based on a common core design consisting of a Motorola Power QUICC CPU, 16 Mbytes of dynamic memory, and 4 Mbytes of FLASH memory. Voice packetization and processing are handled by Texas Instruments Digital Signal Processors (DSP).

### High POTS Port Features

The Verilink High POTS Port IADs provide a highly interoperable, cost-effective voice and high-speed data integration solution that is compatible with industry-leading DSLAM and Voice Gateway manufacturers. These IADs prioritize voice packets and dynamically allocate bandwidth between voice and data services. Features include the following:

- For SDSL, supports the following DSLAMs:
  - ATM: Lucent, Nortel, and Nokia
  - Frame Relay: AccessLan, CopperMountain, and Paradyne.
- For SHDSL, supports the following DSLAMS for ATM: Lucent, Nortel, and Nokia
- Supports the following Voice Gateways: CopperCom, JetStream, TdSoft, Broadsoft, MetaSwitch, Cirpack, NuERA Tollbridge, Nortel, General Bandwidth, Accelerated
- Provides seamless voice and high-speed data integration over SDSL, T1/E1, or SHDSL
- Supports data from POTS and 10/100Base-T customer premise interfaces



- Compatible with standards-based IP, ATM, and Frame Relay WAN protocols
- Interworking feature allows Frame Relay and ATM networks to exchange data using either FRF.5 or FRF.8 protocol
- Provides RJ-21 POTS interface with Loop Start or Ground Start
- USI supports V.35 and EIA-530
- Provides dynamic and static IP routing and bridging capabilities
- Provides firewall support via IP filtering
- Offers DHCP and NAT to support IP address management
- Supports MGCP and SIP with the flexibility to support TDM/VoATM/VoIP applications all in one unit
- Provides management capabilities including Telnet, SNMP, and TFTP

The High POTS Ports are characterized by their different WAN interfaces:

- **8216s/8224s** – provides voice services and high-speed Internet or corporate connectivity over T1 or E1.
- **8316s/8324s** – provides voice services and high-speed Internet or corporate connectivity over SDSL.
- **8512s/8516s/8524s** – provides voice services and high-speed Internet or corporate connectivity over SHDSL.

## High POTS Port Front Panel LED Status Indicators

The High POTS Port front panels contain seven LED status indicators. Each is described in the table below.

**Figure 1.7** High POTS Port Front Panel



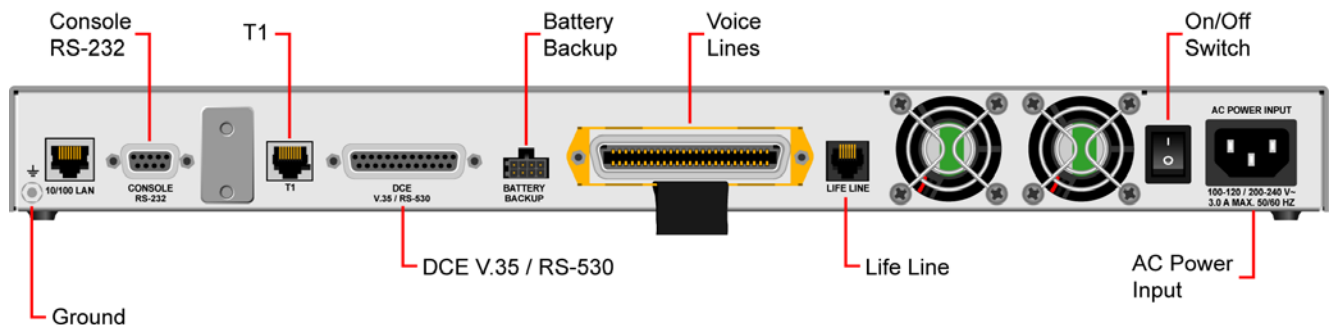
LED	Description
<b>POWER</b>	Illuminates when the IAD is powered on.
<b>LAN LINK</b>	Illuminates when there is an operational LAN connection on the Ethernet port.
<b>LAN Activity</b>	Flashes when there is activity on the Ethernet port.
<b>WAN Link</b>	Flashes as the IAD is establishing a link, and illuminates solid when there is a proper connection on the WAN port and synchronization has been achieved.
<b>VOICE</b>	Illuminates when there is activity on the voice ports. Remains lit when connected to a Jetstream Voice Gateway, and blinks when there is activity.

LED	Description
DCE LINK	Illuminates when there is a link between the IAD and data communications equipment (DCE).
DCE ACT	Illuminates or blinks when there is activity on the DCE link.

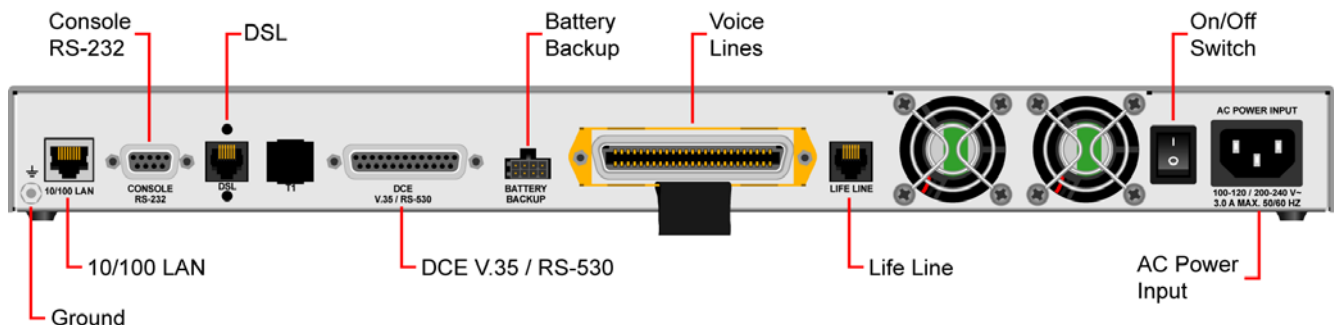
## High POTS Port Rear Panel Connectors

The High POTS Port rear panels have the following connectors: **10/100 LAN**, **CONSOLE**, **T1 (or DSL, depending on model)**, **DCE V.35/RS-530 (USI)**, **BATTERY BACKUP**, **Voice Lines**, **LIFE LINE**, **On/Off Switch**, and **AC POWER INPUT**. Each of these is described below. Each unit also has a **Ground**, a typical diagram of which is shown in Figure 2.1.

**Figure 1.8** T1/E1 High POTS Port Rear Panel Connectors



**Figure 1.9** SDSL and SHDSL High POTS Port Rear Panel Connectors



### 10/100 LAN (10/100Base-T Ethernet Port)

Connects the IAD to the local area network using a CAT-5 straight-through Ethernet cable, or directly to a PC for accessing via Telnet (using a cross-over, customer-supplied cable). The data interfaces connect through the IAD supporting IEEE 802.1-compliant bridging and routing. When configured for routing, supports Routing Information Protocol (RIP) version 1, version 2, or static IP routing. The IAD complies with RFC-1812 when interfacing with IPV4 routers. The IAD can terminate the following data interfaces:

- ATM data transport via SHDSL, SDSL, and T1/E1 per RFC 1483 or RFC 2364
- Frame Relay data transport via SDSL and T1/E1 per RFC 1490

- Frame Relay data transport per RFC 1483 with Q.922 frames
- Console (RS-232 Serial Port)** Connects the IAD to a PC using a straight-through nine-pin serial (DB-9) cable, for the purpose of using a terminal emulator for IAD configuration and management.
- WAN (T1 or DSL, Depending on IAD Model Number)** Connects through WAN interface as follows:
- 8216s/8224s – T1/E1 (uses an RJ-48 connector)
  - 8316s/8324 – SDSL (uses an RJ-11 connector)
  - 8512s/8616s/8524s – SHDSL (uses an RJ-48 connector).
- DCE V.35/RS-530 (USI)** When configured as an RS-530 port with a straight-through DB-25 serial cable, connects to your leased-line DSU/CSU equipment. When configured for use as V.35, Black Box Corporation provides a cable (FA058) for conversion. To convert from RS-530 to RS-449, Black Box provides a cable EDN57J. Contact Black Box for availability of and support for these cables.
- Battery Backup** Connects a battery backup accessory (future feature).
- Voice Lines** Supports 12, 16, or 24 analog telephones via RJ-21 connectors.
- LIFE LINE** Provides access to a telephone line when there is no power or voice gateway to the IAD. Refer to *Life Line Connection* on page 2-12 for a description of which unit uses which port for the Life Line connection.
- AC Power Input** Connects the IAD to any AC 100-240 V outlet.
- Data Interfaces** The data connection through the IAD supports IEEE 802.1-compliant bridging and routing. When the IAD is configured for routing, it supports RIP version 1, version 2, or static IP routing. The IAD complies with RFC-1812 when interfacing with IPV4 routers. The IAD can terminate the following data interfaces:
- ATM data transport via SDSL, SHDSL, and T1/E1 per RFC 1483 or RFC 2364
  - Frame Relay data transport via SDSL and T1/E1 per RFC 1490
  - Frame Relay data transport per RFC 1483 with Q.922 frames



## QUICK START GUIDE

This chapter describes the steps to install, connect, and set the IP address of the 8000 Series IAD. It introduces the menu interface and describes how to perform basic configuration for common LAN and WAN environments. It also describes basic operations such as resetting the IAD and logging off.

In many cases, all the information you need to get an IAD up and running is included in this single chapter. In most installations, you will proceed through these topics in order. If your situation varies, you will find more detailed information on installation, connection, configuration, and troubleshooting in the chapters that follow this Quick Start Guide.

### Unpacking the IAD

---

Each IAD is packed and shipped in a durable container. Unpack and carefully remove the IAD from the package and packing material.

**IAD Package Components** Each IAD is shipped with the components listed below. As you unpack them, note their condition and identity and compare the list with the packing list in the package.

- AC power adapter and cord (6 feet long), or AC power cord
- Agency Compliance information sheet
- Ethernet cable (straight through), 7 feet long
- WAN cable, 7 feet long

If you note any visible damage or missing components, notify the shipping company immediately to make a damage claim. Contact the company from which the IAD was purchased (Verilink, or an authorized distributor) to obtain a Return Material Authorization (RMA) for return of damaged equipment or to order missing components. (Refer to *Support from Verilink* on page xxv.)



---

**NOTICE:** *Verilink suggests you keep the shipping container and packing material for future storage or shipping of the unit.*

---

# Installing the IAD

---

After you unpack the IAD, find a suitable location to install the unit. Ideal locations include a computer equipment room or a telephone or wiring closet. You can locate the IAD on a table or shelf, or it may be wall-mounted. Install the IAD in a location that is generally protected and where it will be undisturbed.

## AC Power and Uninterruptible Power Supply

The IAD requires access to AC power (NEMA 15-3R). Make sure the IAD is located within 6 ft of an AC power outlet. Locate the nearest power outlet and plug in the supplied AC power adapter or AC power cord. If there is an uninterruptible power supply on premises, plug the AC power adapter or cord into that power source.

Ensure the power cord conveniently and safely reaches the rear panel of the IAD where the power plug or adapter jack is located.



---

**NOTICE:** *Do not attach the AC power adapter or power up the unit at this time.*

---

## Clearance Requirements

When you install the IAD horizontally, make sure you maintain at least 2 inches of horizontal distance from other IADs or other electronic equipment to ensure adequate ventilation and heat dissipation.



---

**NOTICE:** *Due to generated heat, 8000 Series IADs should not be stacked on top of each other.*

---

## Wiring Requirements

Make sure the telephone wiring, LAN, and WAN cables reach the IAD and can be dressed in a manner that is safe for the wiring, does not pull or create lateral stress on the connectors or ports on the rear of the IAD, and does not present a trip hazard to personnel working in the vicinity of the equipment. Do *not* connect any cables or wiring at this time.

## Connecting the IAD Via a Terminal Emulator

The IAD is configured and managed from either the console or Ethernet port. A Telnet session is usually used to access the IAD via Ethernet. After you use a terminal emulator program via the console port (refer to *Console Port Pin Assignments (DB-9)* on page B-6 for console port specifications) to set the IP address, you may continue to use a terminal emulator via the console port. The factory-set default IP address is **192.168.1.254** for the Ethernet port.



---

**NOTICE:** *After a period of inactivity (3 min by default), the IAD automatically terminates console-based and Telnet sessions to maintain security. To change this value, see Configure Console Timeout on page 3-15.*

---

Before you can connect to the IAD via Telnet, make sure the IP address is set correctly for this network by following these steps:

- Connect the IAD to a PC
- Log in to the IAD
- Set the IP address

Each of these steps is described in detail below.



---

**NOTICE:** *Ensure the IAD and PC are both powered OFF before connecting the console cable. If both devices are not turned off when you connect the cables, you may place the IAD in an unstable state, and you may need to reset one or both devices before you can perform configuration tasks.*

---

## Connecting the IAD to a PC

To connect the IAD to a PC via the console port, follow the steps below.

- 1** Turn off both devices and insert the male connector of a DB9 serial cable into the console port on the IAD.
- 2** Insert the female connector of the cable into a serial (COM) port on your PC.

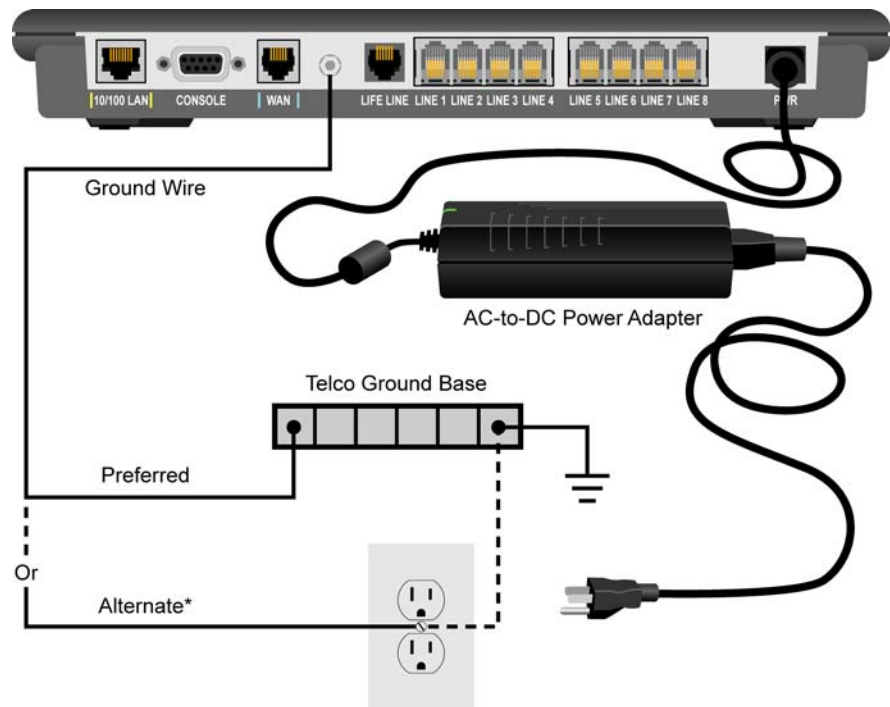


---

**WARNING:** *For Ground Start applications, ensure the IAD is properly grounded. Refer to Figure 2.1.*

---

**Figure 2.1** Typical Grounding Diagram



- 3 With the console cable connected, plug the AC power adapter into the IAD. This starts the IAD, and it executes the boot process to begin normal operation. Verify that the **Power** indicator on the front panel illuminates.



---

**NOTICE:** For “cold start” access, the IAD default (factory-set) IP address is 192.168.1.254 on the Ethernet side.

---



---

**NOTICE:** For “Ground Start” applications, all elements in the voice path must be set to “Ground Start.”

---



---

**NOTICE:** As the IAD boots, it sends status messages to the console port. If you are connected, you will see the boot sequence progress.

---



---

**NOTICE:** This unit should be installed by qualified service personnel only, and must be connected to a socket outlet with protective earthing connection.

---

## Logging in via a Terminal Emulation Program

With a serial cable connected, follow the steps below to log in to the IAD:

- 1 Open a terminal emulation program (Hyperterminal, for example).



- 2 Select the COM port to which the IAD is connected.
- 3 Type or select the settings described in the table below and save your changes.

Setting	Value		Setting	Value
Bits per second	19,200		Stop bits	1
Data bits	8		Flow control	None
Parity	None		Emulation	ANSI or VT100

- 4 Press Enter. The IAD displays the login message:

**Enter Login ID >**




---

**NOTICE:** *If the IAD does not respond, make sure the IAD is powered up, check the cable and connections, and review the settings.*

---

- 5 Type the default supervisor level user ID (`Supervisor`) (or your user ID, if changed) and press Enter. Note that both the user ID and password are case-sensitive. The table below lists the default user IDs and passwords.




---

**NOTICE:** *Refer to Chapter 3, “Administration”, for detailed procedures regarding all IAD administrative tasks. Follow these procedures after performing the basic set-up functions described in this “Quick-Start Guide”.*

---

Security Level	User ID	Password
User	<Enter>	<Enter>
Network Administrator	NetMan	<Enter>
Supervisor	Supervisor	supervisor

- 6 The IAD displays the password message:

**Enter Password >**

- 7 Type the default password (`supervisor`, or your password if different) and press Enter. If login is not successful, the IAD displays the following message:

**Invalid UserID or Password - Try again  
Press any key to continue...**

- 8 Press any key, and repeat the login sequence. If you cannot log in, call your support provider for assistance.

When you first log in, the IAD displays the Main menu (*Figure 2.2*). The menu may vary, depending on the IAD.




---

**NOTICE:** *If you are entering the menu to change a previously established configuration, refer to Managing Configuration Files on page 4-1 to save the current configuration for fast restoration in case the new configuration does not work.*

---

**Figure 2.2** *Main Menu*

```

*****
*                               *
*                               *
*****
1. Reports Menu
2. Configure IP Router
3. Configure Bridge
5. Configure WAN
6. Configure LAN
7. Configure SNMP
8. Configure Login
9. System Utilities
I. Interworking Connections
D. Configure DHCP Server
M. Configure Multicast
N. Configure NAT
T. Telephony Clock Recovery
Z. Diagnostics Menu
C. Command Line Interface
Q. PPP Options Menu
P. VoicePath Configure
R. Reset System

```




---

**NOTICE:** *Options vary depending on the voice gateway selected in the Voice Path Configure command. Refer to Voice Path Configuration on page 4-60.*

---




---

**NOTICE:** *When the IAD prompts you for input, the current value is displayed in parentheses. To conveniently accept the current value, just press Enter.*

---

## Setting the Ethernet Port IP Address

Before you configure the Ethernet IP address, you should know the IP address and subnet mask that are to be assigned to this port. They may be displayed on the work order, or you may obtain or determine the appropriate IP address by consulting with the network administrator.

The IAD is shipped with the IP address set to **192.168.1.254** and the subnet mask set to **255.255.255.0**. To configure a port IP address, follow the steps below.

- 1** On the Main menu, type "2 ." The IAD displays the Router Configuration menu (*Figure 2.3*).

**Figure 2.3 Router Configuration Menu**

```
*****
*      Router Configuration Menu      *
*****
C. Configure Port IP Address
U. Unconfigure Port IP Address
M. Configure Port Max Transmission Unit
S. Add/Remove a Static Route
R. Enable/Disable RIP
V. Configure RIP Version by Port
P. Configure RIP Poisoned Reverse by Port
N. Configure DNS Client
H. Configure DHCP Client
L. Configure DHCP Relay
T. Configure Telnet Server Port
A. Configure IP QoS
F. Configure IP Filtering
Q. Configure IP Header Compression
B. Configure LAN IP Broadcast Destination
G. Configure Domain Name
I. Configure Host Name
```

- 2 Type "C" to select Configure Port IP. The IAD displays the available interfaces. The available interfaces that display depend on the specific IAD as shown in *Figure 2.4* and *Figure 2.5* below.

**Figure 2.4 8308 Available Interfaces**

```
Available Interfaces :
  1. SDSL
  2. 10/100BaseT Ethernet
  0. (Abort)
Selection :
```

**Figure 2.5 8208 Available Interfaces**

```
Available Interfaces :
  1. T1/E1
  2. 10/100BaseT Ethernet
  0. (Abort)
Selection :
```

- 3 Type "2" to set the IP address for the Ethernet port. If the IP address is configured for the port, the IAD displays information about the interface and a prompt such as that shown in the example below:

```
IP interfaces on port 1:
ID          IPAddr          IPMask          Priority
--          -
  0          192.168.xxx.xxx  255.255.255.128  NORMAL
```

Enter connection to configure:

- 4 Type the ID number of the connection you want to configure (in this case, "0") and press Enter.
- 5 Type the new IP address, and press Enter (or press Enter to retain the current IP address). The IAD displays the Current Subnet Mask and prompts you for a new one.
- 6 Type the new Subnet Mask (usually 255 . 255 . 255 . 0) and press Enter. The IAD prompts you to select High or Normal priority.
- 7 To give the interface normal priority, type "N" or press Enter.
- 8 Type "Y" or Enter to save the new IP address and subnet mask.
- 9 To exit, press Escape, and then type "Y" to terminate the session.
- 10 Quit the terminal emulator program.
- 11 Reset the IAD as described below ("*Resetting the IAD*") for the new IP address to be in effect.



---

**NOTICE:** *When you configure the IAD, you must restart the IAD each time you change the settings for those changes to take effect. You may make several configuration changes before resetting.*

---

If you plan to use Telnet for configuration tasks (*Connecting via Telnet* on page 2-9), this is a good time to disconnect the serial cable from the PC and IAD.

## Setting the WAN Port IP Address

To set the WAN port IP address, follow the same procedures as those listed in *Setting the Ethernet Port IP Address* on page 2-6.

## Resetting the IAD

Many configuration tasks require that you reset (or restart) the IAD before the new settings or configuration will take effect. When you use the menu interface (or the Command Line Interface - Chapter 6, "*Command Line Interface*") to make changes, or change the physical characteristics of the IAD (such as the Ethernet port MAC address), you must reset the IAD.

The IAD stores all configuration settings in memory. When it restarts, it loads the last configuration saved before it was powered down or restarted. When restarting is required, it will be included as a step in the configuration process.

You can reset the IAD in one of the two following ways:

To reset the IAD from the menu:

- 1 On the Main menu, type "R" to select Reset System.
- 2 Type "R" again at the prompt. This resets and starts the IAD with your new settings.
- 3 To log in again, enter your user ID and password.

To reset the IAD manually, unplug the power adapter from the IAD and then plug it back in.



---

**CAUTION:** *Be sure to complete your task and return to the Main menu before restarting the IAD manually. Resetting the IAD terminates all telephone calls and computer sessions in progress. You should ensure there are no services being rendered before resetting the IAD.*

---

## Connecting via Telnet

To manage the IAD via the LAN (or Intranet), you must set an IP address for the Ethernet port before you can use Telnet to access the IAD.

Although you can also access the IAD using Telnet via the WAN (provided a management DLCI or PVC is configured along with a WAN IP address), this section describes connecting via the LAN. For information about setting the IP address of the WAN port (Refer to *Managing Configuration Files* on page 4-1.)

If you configure a RADIUS Client, you must use a RADIUS-authenticated User ID/password for Telnet access. If the RADIUS server or the connection to the RADIUS Client goes down, Telnet access will not be permitted. For information about configuring a RADIUS client (Refer to *RADIUS Server Settings* on page 3-4.)

## Running Telnet

Before you use Telnet to log into the IAD, ensure the IAD and your PC are connected to the same network via straight-through Ethernet cables (or directly connected via a cross-over cable), and you know the IP address of the IAD. Both devices must be on the same subnet.

To log in, follow the steps below.

- 1 Run Telnet on your PC.
- 2 Type the IP address of the Ethernet port (refer to *Setting the Ethernet Port IP Address* on page 2-6), click Connect and then press Enter to gain the attention of the IAD. The IAD responds by prompting you to enter your Login ID.
- 3 Type your user ID and press Enter. The IAD will then prompt you to enter your Password.



---

**NOTICE:** *After a period of inactivity (three minutes by default), the IAD automatically terminates console-based and Telnet sessions to maintain security. To change this value, refer to *Configure Console Timeout* on page 3-15.*

---



---

**NOTICE:** *Default user IDs and passwords are listed in the table on page 2-5. For information on security levels, and user ID and password management see *IAD Security* on page 3-1.*

---

4 Type your password and press Enter to display the Main menu (*Figure 2.2*).



---

**NOTICE:** *The user ID and password transmit as clear text, which may be captured by unauthorized individuals. If you are concerned with network security, you may not want to use Telnet to configure the IAD.*

---

### **Navigating the IAD Menu Interface**

Menus in the IAD configuration system are arranged hierarchically. That is, you select single-key options to navigate *down* to display specialized menus and specific tasks, and press the Escape key successively to return back to menus higher in the interface.

The specific menus, submenus, and commands that display depend on the interfaces for the specific IAD, the options configured, and the security level you use to log in.

To select a menu item, type the option displayed to the left of the item. Although character options are displayed in upper case, the IAD accepts both upper- and lower-case options. It is not necessary to press Enter after typing the selection – the IAD immediately responds with a request for input or another menu for more options.

For a hierarchical map of the Main menu, its menus and commands, see Appendix A.

### **Entering Settings and Values**

When the IAD requests input for a setting or configuration value, type it at the prompt. Press the Enter key to terminate the input and proceed to the next step. The IAD responds with error messages if a value is incorrect, or it displays the current menu so you can continue with related tasks.

### **Using Default or Current Values**

The IAD displays a default or current value in parentheses immediately to the right of each message, just to the left of the command prompt. To accept this value, press the Enter key.

For example, when the prompt asking you to enter a new Subnet mask displays, you may press Enter to cause the IAD to set **255.255.255.0** as the Subnet Mask value. Using the Enter key to skip through default or current values often speeds the process of proceeding through a family of input steps to more quickly reach the input step where you wish to change a value.

### **Exiting the Menu Interface**

To exit the menu interface, return to the Main menu using the Escape key, and press Escape one more time. When the IAD asks you to confirm, press "Y" to exit or press Return to accept the default value "N" to cancel the exit.



---

**NOTICE:** *After exiting, you can quit the terminal emulator or Telnet session. If you made changes to the configuration that require resetting the IAD, be sure to do so before exiting.*

---

## Basic IAD Configuration

Each IAD is shipped with a default configuration set in the file *default.st*. Once you make any changes to your IAD, a new file is created to store the new configuration—*config.st*—to preserve the default settings.

After you have configured the IAD for correct operation in a customer's premises, the current system settings in the *config.st* file may be saved as the default configuration file (*custdef.st*), and you may choose to set the IAD to boot from this file each time it is reset. You may also copy this file to a PC or TFTP server for downloading to other identically configured IADs. Once you have replaced the original *custdef.st* file, you cannot retrieve it. Consider copying the *custdef.st* file to a safe location before replacing it.

To perform basic IAD configuration, follow the steps below.

- Configure the LAN IP address, if not already completed (page 2-6).
- Configure each of the WAN options and the DSLAM profile (page 4-2 and the pages following 4-1).
- Create and configure at least one DLCI (page 4-32) or PVC (page 4-24) for data traffic and set the WAN IP address (page 2-6).
- Configure static or default route (page 4-42) or enable bridging (page 4-53) for all data traffic.
- Create and configure a DCLI (page 4-32) or PVC (page 4-24) for voice where required, and select appropriate voice gateway settings (page 4-61).
- Reset the IAD (page 2-8) to enable all configuration changes.



---

**NOTICE:** *You must reset the IAD after configuring IP addresses before you may add routes.*

---

## Connecting LAN, WAN, and Telephones

This section details how to connect the IAD to the computer and telephone systems the IAD is intended to support.

Before proceeding, make sure you have an appropriate serial cable for your PC, identify the LAN switching equipment where you'll connect the IAD, identify the telephone cables, and verify that WAN service is installed and configured by the service provider.

When you've completed this section, reset the IAD so it can synchronize these physical connections.

### Ethernet LAN Connection

The Ethernet LAN port on the rear of the IAD is an RJ-45 jack for 10/100Base-T Ethernet cables. If the IAD is intended to act as an Internet gateway for the LAN in the customer's premises, connect the IAD to the switch, hub, or router using an Ethernet straight-through cable.




---

**NOTICE:** *You may temporarily connect the IAD directly to a PC for Telnet configuration (without going through a hub or router). The Ethernet receiver automatically detects the type of Ethernet cable (customer-supplied).*

---

## WAN Connections

WAN connections vary, based on the WAN interface on your IAD. The 8308 is an SDSL-equipped IAD and uses an RJ-11 connector to connect to the rear panel WAN connection. To make the connection, plug the SDSL cable into the RJ-11 WAN connector. (Refer to page B-6.) The 8208 is a T1/E1-equipped IAD and uses an RJ-48 connector on the IAD rear panel for WAN connection. To make the connection, plug the cable from the ATM network into the RJ-45 WAN connector. Refer to page B-6 to see the pinouts for the T1/E1 connection.

## Telephone Connections

The 8000 Series IADs provide eight RJ-11 ports for POTS devices. These devices may be POTS telephones, modems, FAX machines, or other POTS-compatible devices.

## Life Line Connection

The IADs have an RJ-11 Life Line associated with the POTS line. (Refer to the table below.) The Life Line is an analog line that can be directly connected to the PSTN. In case of power loss or loss of voice gateway connection, the designated POTS line automatically switches to the Life Line connection.

Product	Life Line Port
8208/8208s, 8308/8308s/8304/8304s, 8216s/8224s/8316s/8324s/8512s/8516s/8524s	POTS Line 1
8104/8104s, 8504/8504s	POTS Line 4
8108/8108s, 8508/8508s	POTS Line 8




---

**NOTICE:** *The 8104/8108 uses the WAN connection for the Life Line connection.*

---

## USI Connection

If your IAD is equipped with a USI port, you may connect it now. Located on the rear panel, the port uses a shielded, DB25 connector. The connector is DCE – data is transmitted on the receive pin and received on the transmit pin. The V.35 and EIA-530 interfaces use different voltage levels. You must supply the appropriate cable for each interface. Refer to Appendix B for pinout connections.



## Confirming Proper Setup

When you have completed the tasks in this chapter, reset the IAD and test your configuration for proper data and voice operation. Reset the IAD (page 2-8) to synchronize the physical connections using the verification procedure described in *Chapter 8*.



## ADMINISTRATION

This chapter describes how to control security to your IAD, validate users using a RADIUS Server, configure SNMP via IP or AAL2 Embedded Operations Channel (EOC), upgrade IAD software, and perform other general and utility-oriented tasks.



---

**NOTICE:** *When the IAD prompts you for input, the current value is displayed in parentheses. To conveniently accept the current value, just press Enter.*

---

### IAD Security

---



---

**NOTICE:** *After setting IAD Security parameters, you must reset the IAD (page 2-8) for the new settings to take effect.*

---

To maintain IAD security, the IAD provides multi-level login access using a single user ID and password, which you can set at the following levels:

- User
- Network Administrator
- Supervisor

The user ID at the User security level may be modified, but the user ID at the Network Administrator and Supervisor levels may not.

The password for each security level may be changed. Although you may use the same password for all security levels, Verilink recommends that you use a different one for each level. The table below lists the privileges available at each security level.

Security level	Privileges
Supervisor	This user level is the highest level. Users who log in as Supervisor have full access to all IAD features (menu and command line interface, including changing User security level, user ID, and any level passwords, plus complete IAD configuration capability.
Network Administrator	At this level, users may perform tasks that alter the network settings of the IAD, plus are able to access to all data networking configuration menus, and can update routing and bridging information and status. This user can change the password at this level, and also can change the User-level User ID and password, and can access all display-only menus. At this level, users user cannot modify WAN or LAN settings, alter derived timing, use the Command Line Interface, or modify voicepath settings.
User	At this level, the user has access to display-only menus, and can view the current configuration, interface, and media statistics, routing and bridging information, and status. The user may change this level User ID and password, but cannot make or save any changes to the configuration of the IAD.

To maintain IAD security, a user with Supervisor privileges should modify the User security level user ID and passwords for both User level and Network Administrator level prior to placing the IAD into production.

The table below lists the default values for the user IDs and passwords:

Security Level	User ID	Password
User	<Enter>	<Enter>
Network Administrator	NetMan	<Enter>
Supervisor	Supervisor	supervisor

The user ID and password may contain up to 17 alphanumeric characters. These values are case sensitive; spaces and punctuation characters are not allowed.

The IAD can store only one user ID and password at each security level.

## Password Configuration Menu

To access the Password Configuration menu, type "8" (Configure Login) on the Main menu.

Figure 3.1 Password Configuration Menu

```
*****
*           Password Configuration Menu           *
*****
 1. Change User ID
 2. Change User Password
 3. Change NetMan Password
 4. Change Supervisor Password
 5. Change Primary RADIUS Server Address
 6. Change Primary RADIUS Encryption Secret
 7. Change Secondary RADIUS Server Address
 8. Change Secondary RADIUS Encryption Secret
 9. Display RADIUS Configuration
 X. Disable RADIUS Configuration
```

## Change User ID

To change the user ID for the User security level (the only security level that allows the user ID to be changed), follow the steps below.

- 1 Type "1" to change the user ID for the User security level.
- 2 Type the new User ID (up to 17 characters) and press Enter. The IAD informs you that the user ID has been updated.
- 3 Reset the IAD.

### *Including User IDs and Passwords in Config Files for Multiple Site Distribution*

If you create master configuration files for distribution to multiple IADs, you may include the user ID and passwords directly in the configuration file to reduce configuration tasks.



---

**NOTICE:** *When the user ID and passwords are stored in a configuration file, the IAD saves the configuration file immediately upon rebooting, without requiring the log-in process. The user ID and passwords are stripped from the configuration file before saving to prevent a security risk.*

---

Using a text editor, update the config file by adding the following attributes in the [user] category:

```
userid={string}
password={string}
netman-password={string}
support-password={string}
```

The password parameter is for User-level access, the "netman" password is for Network-Administrator-level access, and the "supervisor" password is for Supervisor-level access.

## Change User Password

To change a password at any security level, you must sign on at or above the security level you're changing and follow the steps below.

- 1 Type "2", "3", or "4" on the Password Configuration menu to change the password for the selected level.
- 2 Enter the password for the current level.
- 3 Enter the new password after the prompt, or press Enter to enter a null password.
- 4 Enter the new password (or Enter) again, to confirm the change.

The IAD immediately updates the password. The next time you log in at that level, the new password will be in effect.



---

**NOTICE:** *You cannot use the Escape key to exit the password update command. To exit, deliberately enter an incorrect password at the confirmation step, or reset the IAD.*

---

## RADIUS Server Settings

You can use a RADIUS Server to determine the validity of unknown user ID/password pairs in your IAD. Verilink does not provide a RADIUS Server; the user must provide a RADIUS Server to use this feature. For more information on RADIUS Server, see RFC 2865.

If you configure a RADIUS Server, the IAD must be able to successfully connect to the RADIUS Server. This requires WAN configuration, IP configuration, static or default routes, and other configurations for your network. Additionally, you must use a RADIUS-authenticated user ID/password for Telnet access. If the RADIUS Server becomes inoperative, Telnet access will not work.

To use a RADIUS Server, set the following options:

- Change the primary or secondary RADIUS Server Address
- Change the primary or secondary RADIUS Server Encryption Secret
- Display RADIUS Server Configuration

Each of these settings is described below.

### ***Change Primary (or Secondary) RADIUS Server Address***

To change the primary or secondary RADIUS Server address, follow the steps below.

- 1 Type "5" on the Password Configuration menu to select Change Primary RADIUS Server Address or Type "7" to select Change Secondary RADIUS Server Address. The IAD displays the current Radius Server and prompts you to enter a new one by IP Address or name.
- 2 Type the IP address in one of the following formats and press Enter.

IP address  
Fully-qualified host and domain names  
(for example: radius.Verilink.com—maximum 42 bytes)



---

**NOTICE:** *If you enter host and domain names, you must configure the IAD as a DNS client (see page 4-45).*

---

**3** Reset the IAD.

### ***Change Primary (or Secondary) RADIUS Encryption Secret***

To change the primary or secondary RADIUS encryption key, follow the steps below.

- 1** Type "6" on the Password Configuration menu to select Change Primary RADIUS Encryption Secret or type "8" to change Secondary RADIUS Encryption Secret. The IAD displays the current Radius Encryption Secret and prompts you to enter a new one.
- 2** Type the new encryption key and press Enter.
- 3** Reset the IAD.

### ***Display RADIUS Configuration***

To display the current RADIUS Server configuration, follow the steps below.

- 1** Type "9" on the Password Configuration menu to select Display RADIUS Configuration. The IAD displays the following information:

```
Primary RADIUS Server:  
Primary RADIUS Secret:  
Secondary RADIUS Server:  
Secondary RADIUS Secret:
```

### ***Disable RADIUS Configuration***

To disable the RADIUS Server configuration, type "X" on the Password Configuration Menu (Figure 3.1). The IAD disables both the Primary and Secondary RADIUS Server configurations.

## **Setting Up SNMP**

---



---

**NOTICE:** *After updating SNMP settings, you must reset the IAD (refer to page 2-8) for the new settings to take effect.*

---

SNMP is supported via Internet Protocol (IP) and the Loop Emulation System Embedded Operation Channel (LESEOC). The LESEOC interface is only available with either the AAL2/LES CAS or ELCP voice gateway. This interface allows the voice gateway to monitor and control specific IAD operational parameters.




---

**NOTICE:** *Some voice gateways with this feature require a read-write community name of LESEOC to be configured in the IAD.*

---

The SNMP Configuration menu is accessible from the Main menu. You may enable SNMP via IP, EOC, or both. Traps may be sent to a configurable IP address, the EOC, or both. The System Contact, System Name, and System Location may also be configured. These values are accessible via the RFC 1213 MIB. The IAD supports the following SNMP settings:

- System Contact
- System Name
- System Location
- SNMP Community
- SNMP Trap Host IP Address

The following SNMP traps are supported:

- System reset
- Attempts to access SNMP with an invalid community name
- Starting and stopping TFTP within SNMP

The IAD supports MIBs for RFCs 1213, 1317, 1406, 1493, and 1463 as well as af-vmoa-0174 (AAL2/LES MIB).

## SNMP Configuration Menu

To display the SNMP Configuration menu, type “7” on the Main menu. Each of the menu’s configuration options is described below.

**Figure 3.2** *SNMP Configuration Menu*

```

*****
*           SNMP Configuration Menu           *
*****
E. Enable/Disable SNMP via IP
F. Enable/Disable SNMP via EOC
A. Enable SNMP via both IP and EOC
B. Disable SNMP via both IP and EOC
P. Configure System Contact
N. Configure System Name
L. Configure System Location
T. Configure SNMP Trap Host IP Address
U. Enable/Disable SNMP Traps via EOC
D. Configure Restart Trap Max Delay
3. SNMP Version 3 Menu

```




---

**NOTICE:** *The strings you enter in SNMP are not case sensitive.*

---



## **Enable/Disable SNMP via IP**

To Enable or Disable SNMP via IP, follow the steps below.

- 1** Type "E" on the SNMP Configuration menu to enable or disable SNMP via IP. The IAD displays the current status of SNMP.
- 2** To enable SNMP, type "E" or "D" to disable. The IAD saves the configuration (if changed).
- 3** Continue with other SNMP settings, or press Escape to return to the Main menu.
- 4** Reset the IAD.

## **Enable/Disable SNMP via EOC**

To Enable or Disable SNMP via EOC, follow the steps below.

- 1** Type "F" on the SNMP Configuration menu to enable or disable SNMP via EOC. The IAD displays the current status of SNMP.
- 2** To enable SNMP, type "E" or type "D" to disable. The IAD saves the configuration (if changed).
- 3** Continue with other SNMP settings, or press Escape to return to the Main menu.
- 4** Reset the IAD.

## **Enable SNMP via Both IP and EOC**

To Enable SNMP via Both IP and EOC, follow the steps below.

- 1** Type "A" on the SNMP Configuration menu to enable SNMP via IP and EOC. The IAD saves the configuration.
- 2** Continue with other SNMP settings, or press Escape to return to the Main menu.
- 3** Reset the IAD.

## **Disable SNMP via Both IP and EOC**

To Disable SNMP via both IP and EOC, follow the steps below.

- 1** Type "B" on the SNMP configuration menu to disable SNMP via IP and EOC. The IAD saves the configuration.
- 2** Continue with other SNMP settings, or press Escape to return to the Main menu.
- 3** Reset the IAD.

## **Configure System Contact**

To configure the System Contact, follow the steps below.

- 1 Type "P" on the SNMP Configuration menu to configure system contact (up to 39 alphanumeric characters). The IAD displays the current system contact and prompts you to enter a new one.
- 2 Type the name of the new contact person or department and press Enter. The IAD save the configuration.
- 3 Continue with other SNMP settings, or press Escape to return to the Main menu.
- 4 Reset the IAD.

## Configure System Name

To configure the System Name, follow the steps below.

- 1 Type "N" on the SNMP Configuration menu to configure the system name (up to 39 alphanumeric characters). The IAD displays the current system name and prompts you to enter a new one.
- 2 Type the new system name and press Enter. The IAD saves the configuration.
- 3 Continue with other SNMP settings, or press Escape to return to the Main menu.
- 4 Reset the IAD.

## Configure System Location

To configure the System Location, follow the steps below.

- 1 Type "L" on the SNMP Configuration menu to configure the system location (up to 39 alphanumeric characters). The IAD displays the current system location and prompts you to enter a new one.
- 2 Type the name of the new server location and press Enter. The IAD saves the configuration.
- 3 Continue with other SNMP settings, or press Escape to return to the Main menu.
- 4 Reset the IAD.

## Configure SNMP Community

The value you set must match the write community name of the SNMP host to enable the SNMP Set operation. If you enable SNMP and the read-write Community Name is null, SNMP enters read-only mode with a community name of "public."

- 1 Type "L" on the SNMP Configuration menu to select Configure System Location. The IAD displays the current community name and prompts you to enter a new one.
- 2 Type the name of the SNMP community to which your system belongs and press Enter. The IAD saves the configuration.

- 3 Continue with other SNMP settings, or press Escape to return to the Main menu.
- 4 Reset the IAD.

### **Configure SNMP Trap Host IP Address**

To configure the SNMP Trap Host IP Address, follow the steps below.

- 1 Type "T" on the SNMP Configuration menu to select Select Configure SNMP Trap Host IP Address of the system setup for trap operations. The IAD displays the current IP address and prompts you to enter a new one.
- 2 Type the IP address and press Enter. The IAD saves the configuration.
- 3 Continue with other SNMP settings, or press Escape to return to the Main menu.
- 4 Reset the IAD.

### **Enable/Disable SNMP Traps via EOC**

To Enable or Disable SNMP Traps via EOC, follow the steps below.

- 1 Type "U" on the SNMP Configuration menu to enable or disable SNMP traps via EOC. The IAD displays the current status.
- 2 To enable traps via EOC, type E. To disable them, type D. The IAD saves the configuration.
- 3 Continue with other SNMP settings, or press Escape to return to the Main menu.
- 4 Reset the IAD.

### **Configure Restart Trap Maximum Delay**

To configure Restart Trap Maximum Delay, follow the steps below.

- 1 Type "D" on the SNMP Configuration menu to configure the restart trap maximum delay time. The IAD prompts you to input a new value.
- 2 Type the new value in seconds and press Enter. The IAD saves the configuration.
- 3 Continue with other SNMP settings, or press Escape to return to the Main menu.
- 4 Reset the IAD.

### **Defining Different SNMP Version 3 Categories**

SNMP 3.0 requires the configuration of six data structures on the SNMP 3.0 menu (Figure 3.3), which is accessible from the SNMP Configuration menu. Menu options are available to configure a default set of structures, which will allow SNMP 1.0 or SNMP 3.0. Choose Option 3 on the SNMP 3.0 Configuration menu to set a simple default configuration.

**Figure 3.3** *SNMP V3 Configuration Menu*

```
*          SNMP V3 Configuration Menu          *
*****
A. Configure SNMP Community Entry
B. Configure SNMP Target Entry
C. Configure SNMP Group Entry
D. Configure SNMP Access Entry
E. Configure SNMP View Entry
F. Configure SNMP User Entry
G. Delete SNMP Community Entry
H. Delete SNMP Target Entry
I. Delete SNMP Group Entry
J. Delete SNMP Access Entry
K. Delete SNMP View Entry
L. Delete SNMP User Entry
M. Display SNMP Community Entries
N. Display SNMP Target Entries
O. Display SNMP Group Entries
P. Display SNMP Access Entries
Q. Display SNMP View Entries
R. Display SNMP User Entries
1. Set Default Version 1 Configuration
3. Set Default Version 3 Configuration
```

Two SNMP “community entries” are generated: public (read-only community), and a read-write community. Since a read-only community of public is the default for all SNMP implementations, you are encouraged to reconfigure the first community entry to a more secure value.

The “target entries” specify who may access the IAD via SNMP. The first entry, named “everyone,” allows access from the entire Internet. Entries are added if an IP trap host is configured, or if EOC access is configured. For example, if you want only IP addresses 1.2.3.0 through 1.2.3.255 to have SNMP access to the IAD, you will reconfigure the target entry with the address of 1.2.3.0, and the mask 255.255.255.0. Note EOC access is specified by the reserved IP address 255.255.255.255.

The “group entries” specify which version of SNMP to allow: 1.0 or 3.0 (user security model).

The “access entry” specifies which version of SNMP to allow, the security level (MD5 authorization encryption), and which views are accessible.

The “view entry” specifies which portion of the MIB is accessible or not accessible. For example, it is possible to create a view to allow access to the ATM Forum LES MIB from the EOC, and allow the entire MIB to be accessible from an IP location.

The “user entry” applies to SNMP 3.0 only. This is where you configure the MD5 authorization encryption password.

## LAN Configuration Menu

---

The IAD LAN port may be set for full duplex Ethernet operation if your IAD is set up as a router (page 4-38). Full duplex mode allows simultaneous transmission and receipt of Ethernet packets.

On the Main menu, type "6" (Configure LAN) to display the LAN Configuration menu.

Figure 3.4 LAN Configuration Menu

```
*****
*           LAN Configuration Menu           *
*****

Current Duplex Mode   : - Line is detected as Half Duplex
                      - Transceiver is manually set to Half Duplex
Current Ethernet Speed : - AUTO NEGOTIATED - 10 mbit/s

  1. 10 Mbps Full Duplex
  2. 10 Mbps Half Duplex
  3. 100 Mbps Full Duplex
  4. 100 Mbps Half Duplex
  5. Auto Negotiate the Speed, Full Duplex
  6. Auto Negotiate the Speed, Half Duplex
  7. Auto Negotiate the Speed and Full/Half Duplex Mode

  8. Display MII & FEC Registers
```

### Establishing LAN Speed and Duplex Mode

- 1 Type the option number of the speed and duplex mode. The IAD saves the configuration.
- 2 Press Escape to return to the Main menu.
- 3 Reset the IAD.



---

**NOTICE:** *Full duplex Ethernet operation is controlled by the switch. If the switch is set to full duplex, you may enable it in the IAD. If you enable full-duplex Ethernet in the IAD when the switch is operating in normal half-duplex mode, your IAD will not communicate on the LAN.*

---

You can display the current LAN settings using the Display Current Configuration command in the Reports menu (page 5-1).

## Upgrading the System

---

Periodically, Verilink may provide new software that you will download to the IAD to upgrade the system. You must use TFTP to perform the file transfer when upgrading the entire system.



---

**NOTICE:** *Some gateways directly support file transfer as a means of upgrading IADs. For information, refer to the Voice Gateway manufacturer's operating manual.*

---

To use TFTP, you must configure both the IAD and the computer that contains the TFTP Server program, a program for the computer that you license separately.

## Using TFTP Servers via LAN or WAN

Before the IAD can access a LAN or Intranet-based TFTP server, you must configure the IP address of the Ethernet port (page 2-6) on the same subnet as your TFTP server, and the IAD must be connected to the LAN.

To access a WAN-based server, you must configure the T/E1 or SDSL Interface with a management DLCI or PVC and a WAN IP address. For information about setting the IP address of the WAN port, see *Setting the WAN Port IP Address* on page 2-8 or *WAN Configuration Menu* on page 4-4.

## Copying the Source Files

Typically, you will receive two ZIP files (a core ZIP file and an application ZIP file) for each upgrade.

First, extract each file into a single directory on your PC. Then, set the directory as the path that the TFTP Server will use to send files to the IAD (often identified as upload/download or outbound directory).

## Upgrading via TFTP

If your TFTP Server is not running, start it now and note the IP address of the computer it is running on. To upgrade the IAD software, follow the steps below.

- 1 On the Main menu, type "9" to display the Utilities menu (see ).
- 2 Type "X" to display the File Transfer menu.

**Figure 3.5** *File Transfer Menu*

```
*****
*                               *
*                   File Transfer Menu                   *
*                               *
*****
  B. Load Boot ROM
  O. Update ACOS [acos.bin]
  X. Update Entire System
  A. File Transfer Utilities
  T. TFTP Server Menu
```

- 3 Type "X" to update the entire system (you must use TFTP).
- 4 Respond by typing "Y" to continue.

- 5 The IAD prompts you to enter the IP address of the TFTP Server.
- 6 Type the IP address of the TFTP Server and press Enter.

As file transfer progresses, the IAD reports the status of each file being copied. Two files – `acos.bin` and `boot.bin` – will only be copied if they match the platform to guard against loading incorrect system files onto an IAD.



---

**NOTICE:** *If the IAD cannot locate the first file to download (typically `release.dat`), the update will fail. Make sure you have assigned a valid IP address and subnet mask, and you're on the same subnet as the TFTP Server. Use the Ping command to ping the IAD and try again.*

---

Upon completion, the IAD reports the success or failure of each file transfer, and then reports the completion of file transfer and resets.

## Verifying the Upgrade

To verify that the files downloaded successfully after being transferred, observe the boot sequence. The IAD displays the software version in the Verilink banner.

You may also display the current configuration (page 8-2) to validate the firmware version.

## Utilities Menu

---

The Utilities menu contains utility commands, including several menus to upgrade IAD software and support ACOS application development.

To display the Utilities menu, type `"9"` on the Main menu. Option `"U"` (high-port count IADs only) will display the USI port menus.

## Utilities Menu

```
*****
*                               Utilities Menu                               *
*****
P. Ping Utility
T. Trace Route
Z. Configure Console Baud Rate
U. Configure Console Timeout
R. Hard Reset or Reload ACOS from FLASH
D. Set System Defaults
W. Save System Settings as Defaults
E. Display Event Log
L. Clear Event Log
A. Clear "Last Reset Reason"
M. Time Zone Menu
N. Display Configuration File

F. File System Menu
G. Debug Menu
X. File Transfer Menu
```

Each option on this menu is described in detail below.

## Ping Utility

To check for a device on a network, follow the steps below:

- 1 Type "P" on the Utilities menu.
- 2 Type the IP address or complete host name. If you enter a host name, you must enter the domain name also (i.e., **mycomputer.mydomain.com**).
- 3 Type the ping packet size.
- 4 Type the number of times to ping (0 causes Ping to run until you press Escape).

The IAD displays the following report:

```
Pinging: 192.168.xxx.xxx
Size: 32 bytes...

Ping Number 1 of 1 (Esc to quit)
Reply from: 192.168.xxx.xxx
Size: 32 bytes
Time: < 5 mS

**** Ping Summary ****
Packets Sent      : 1
Packets Received  : 1
Packets Lost      : 0
Average Ping Time : < 5 ms
```



## Trace Route

- 1 Type "T" on the Utilities menu and press Enter.
- 2 Type the IP address or complete host name. If you enter a host name, you must also enter the domain name (i.e., *mycomputer.mydomain.com*). The IAD displays each hop, as shown in the following sample report:

```
Trace Route Results 192.168.xxx.xxx|
1      <5ms      192.168.xxx.xxx
```

## Configure Console Baud Rate

To set the console port baud rate (for connecting to Hyperterminal via a serial cable), follow these steps:

- 1 Type "Z" on the Utilities menu to display the following menu:

```
Current Console Baud Rate is: 19200
```

```
Enter New Console Baud Rate
```

```
0. Unset (use Default)
1. 9600
2. 19200
3. 38400
4. 57600
5. 115200
```

- 2 Type "0" to reset the baud rate to the default (19200 bps), or select a specific baud rate and press Enter.
- 3 Reset the IAD to use the new console port settings. Be sure the terminal settings are the same as the console port settings.



---

**NOTICE:** *The new baud rate table will take effect only after you either recycle the power or reset the IAD.*

---

## Configure Console Timeout

To maintain security, you can set the amount of time a console or Telnet session remains alive before termination due to inactivity. To set the timeout period, follow these steps:

- 1 Type "V" on the Utilities menu to display the Console Timeout Status and a prompt for you to enter a new Timeout value or disable the Timeout.
- 2 Type a value between 0-60 minutes (default 3) and press Enter or type "0" (zero) to disable the Timeout feature.



---

**CAUTION:** *When the Timeout value is set to zero, sessions will stay alive indefinitely, and may pose a security risk. Quitting a terminal emulator session does not terminate the console port session. You must log off before quitting to avoid creating a security risk.*

---

## Reset or Reload ACOS from FLASH

When you perform a hard reset, the IAD resets, using all values set during the active session and reloads ACOS from flash memory. To perform a hard reset, follow these steps:

- 1 Type "R" on the Utilities menu. The IAD displays the following:  

```
Sure you want to do a Hard Reset? (Y/N) ->
```
- 2 Enter "Y" to immediately perform a hard reset and reload ACOS, replacing it.

## Set System Defaults

You may set the IAD to boot from the previously saved custom configuration, or boot from the factory-supplied configuration file as described below.

- 1 Type "D" on the Utilities menu. The IAD displays the following menu:

**Figure 3.6** *System Default Menu*

```
*****  
*           Select Default           *  
*****  
  1. Custom Defaults  
  2. Factory Defaults
```

- 2 Type "1" to set the previously saved custom configuration file as the boot file  
—or—  
Type "2" to set the default.st config file as the boot file.
- 3 The IAD displays a warning and asks you to confirm your decision.
- 4 Type "Y" to confirm the process. The IAD updates the setting and displays the Utility menu.
- 5 Reset the IAD to reboot with the new config file.

## Save System Settings as Defaults

To save the current configuration as the custom default or backup configuration, follow the steps below.

- 1 Type "W" on the Utilities menu. The IAD displays a warning and asks you to confirm your decision.

- 2 Type "Y" to delete the *default.st* file and save the current configuration (stored in *config.st*) as *custdef.st*, a custom default configuration file.

The IAD saves the custom configuration file and displays the Utility menu.

## Display Event Log

To display the event log, type "E". The IAD displays the event log (sample shown):

**Figure 3.7** *Event Log*

```
0:0:0:22.220 System reset
0:0:4:27.140 System soft reset from menu command
0:0:0:21.325 System reset
0:0:1:50.770 System soft reset from menu command
0:0:0:22.285 System reset
0:0:4:44.735 System soft reset from menu command
0:0:0:21.350 System reset
0:0:1:14.600 System soft reset from menu command
0:0:0:22.300 System reset
0:0:0:45.585 TELNET session started from 192.168.xxx.xxx
0:0:0:57.070 TELNET session ended from 192.168.xxx.xxx
0:0:8:11.500 TELNET session started from 192.168.xxx.xxx
0:0:8:51.955 TELNET session ended from 192.168.xxx.xxx
0:12:54:30.345 TELNET session started from 192.168.xxx.xxx
0:12:57:43.900 TELNET session ended from 192.168.xxx.xxx
1:21:7:13.110 TELNET session started from 192.168.xxx.xxx
1:21:10:29.675 TELNET session ended from 192.168.xxx.xxx
1:21:11:26.345 TELNET session started from 192.168.xxx.xxx
1:21:28:0.010 TELNET session started from 192.168.xxx.xxx
1:21:28:36.380 TELNET session started from 192.168.xxx.xxx
1:21:30:52.775 TELNET session ended from 192.168.xxx.xxx
```

Press any key to page through the log.

## Clear "Last Reset Reason"

Under certain circumstances, the IAD is able to determine the reason the IAD was reset. This information is stored and displayed when the IAD reboots, and is also displayed on the Current Configuration screen (*Displaying the Current Configuration* on page 8-2), when known.

After the reset reason is noted, you can delete the currently stored reset reason from the IAD. To do so, type "A" on the Utilities menu. The IAD deletes any existing reset reason, and displays the Utility menu.

## Time Zone Menu

The Time Zone menu () is used to help set the current time. When the IAD is reset or the power is cycled, the IAD will use Network Timing Protocol (NTP) to obtain the current time. Time Zone Menu

```
*****  
*                               Time Zone Menu                               *  
*****
```

```
Current time zone offset is -8 hours 0 minutes.  
Time zone is currently: Pacific Zone  
  O. Configure Time Zone Offset  
  N. Configure Time Zone Name  
  C. Clear Time Zone Name
```

In the Time Zone menu, you may specify your time zone so the time displayed on statistics screens will be your local time. To set, type "O" and then type in your time zone offset from Greenwich Mean Time (GMT). For example, for Pacific Standard Time (PST), you would type in an offset of "-8." Type "N" to enter a text label for your time zone.

## Display Configuration File

Select this option to view the IAD's current configuration. You may also capture the configuration for documentation or debug purposes.

## File System Menu

The File System menu contains commands to manage files on the IAD. To display the File System menu, type "F" on the Utilities menu.

Figure 3.8 *File System Menu*

```
*****  
*                               File System Menu                               *  
*****  
  D. Directory of all files  
  C. Copy file  
  R. Rename File  
  X. Remove File by name  
  F. Format File System drive  
  S. Space left in File System
```

To perform a task, type the option and read how to proceed by referring to the appropriate section below.

## Directory of all Files

To display the files stored in flash memory, type "D" on the File System menu. The IAD displays the files and size. Page down the list by pressing any key. The IAD displays the amount of free memory at the end of the list.

## Copy File

To duplicate a file with a new name, follow the steps below.

- 1 Type "C" on the File System menu. The IAD prompts you for the name of the source file.
- 2 Type the name of the existing file (including the suffix) and press Enter. The IAD prompts you for the name of the new file.

The IAD copies and saves the file with the new name. When the operation is complete, the IAD displays the File System menu.

## Rename File

To rename a file, follow the steps below.

- 1 Type "R" on the File System menu. The IAD prompts you for the name of the file to rename.
- 2 Type the new name of the file (including the suffix) and press Enter. The IAD prompts you for the name of the new file.

The IAD renames the file with the new file name. When the operation is complete, press any key to display the File System menu.



---

**CAUTION:** *Renaming files is permanent, and may render the IAD inoperative or unable to boot.*

---

## Delete File

To permanently remove a file, follow the steps below.

- 1 Type "X" on the File System menu. The IAD prompts you for the name of the file to delete.
- 2 Type the name of the file (including the suffix) and press Enter.

The IAD deletes the file. When the operation is complete, the IAD displays the File System menu.



---

**CAUTION:** *Deleting files is permanent, and may render the IAD inoperative or unable to boot.*

---

## Format File System Drive

Reformatting the file system permanently removes all files in the IAD. This command is reserved for use by Verilink network engineers.



---

**WARNING:** *The Format File System command is reserved for use by Verilink engineers. Use of this command permanently erases every file in the IAD, rendering it inoperative.*

---

## Space Left in File System

To display the amount of free space in the file system (flash memory), type "S" on the File System menu. The IAD displays the free space.

## File Transfer Menu

The File Transfer menu allows you to transfer groups of files to or from the IAD. To display the File Transfer menu (see Figure 3.5 on page 3-12), type "X" on the Utilities menu. To perform a specific task, type the option and proceed to the corresponding section below.

### Load Boot ROM

- 1 Type "B" on the File Transfer menu to download the Boot ROM to the file system on the IAD.

**Figure 3.9** *File Transfer Method Menu*

```
*****  
*           File Transfer Method           *  
*****  
  1. Receive via TFTP  
  2. Receive via XMODEM
```

- 2 Type "1" to use TFTP, or "2" to use XMODEM to transfer the file to the IAD.
- 3 The IAD displays the prompts you for the IP address of the TFTP server.
- 4 Type the IP address of the TFTP server and press Enter.
- 5 The IAD displays the following prompt for the file name to transfer:
- 6 Type the name of the file and press Enter. To exit without transferring the file, press Escape or Enter without typing the file name.
- 7 When XMODEM is selected, if the file is not located, the IAD prompts you for the file transfer speed.
- 8 The IAD transfers the file via TFTP or XMODEM.

Perform a hard reset to reset the IAD (page 3-16) whenever you load a new version of boot ROM. Performing a normal reset is not recommended.

## Update ACOS [acos.bin]

- 1 Type "0" on the File Transfer menu to display the File Transfer Method menu and download Verilink's Atlas Communications Operating System (ACOS) to the file system in Flash memory on the IAD. The file is stored on the IAD as *acos.bin*. The IAD displays the File Transfer Method menu.
- 2 Type "1" to use TFTP, or "2" to use XMODEM to transfer the new version of ACOS to the IAD. If you select XMODEM, proceed to step 5 below.
- 3 The IAD prompts you to enter the IP address of the TFTP server.
- 4 Type the IP address of the TFTP server and press Enter. The IAD displays the following prompt for the file name to transfer:
- 5 Type the name of the file and press Enter. To exit without transferring the file, press Escape or Enter without typing the file name. When XMODEM is selected, if the file is not located, the IAD prompts you for the file transfer speed. The IAD transfers the file via TFTP or XMODEM.

Perform a hard reset (page 3-16) to reset the IAD whenever you load a new version of ACOS. Performing a normal reset is not recommended.

## Update Entire System

- 1 Type "X" on the File Transfer menu to update the IAD by transferring the upgrade package of files provided by Verilink. The number and type of files varies by IAD. The IAD uses TFTP to download files sequentially to the IAD. The IAD displays a confirmation prompt.
- 2 Type "Y" to continue, or any other character to escape. The IAD prompts you for the IP address of the TFTP Server.
- 3 Type the IP address of the TFTP server and press Enter. The IAD transfers each of the system files.

When the file transfers are complete, perform a hard reset (page 3-16) to restart the IAD. Performing a normal reset after updating the system is not recommended.

## File Transfer Utilities

To perform file transfers for any files, type "A" on the File Transfer menu to display the File Transfer Method menu to download a file to the file system in the IAD. The IAD displays the File Method menu.

- 1 Type "1" to use TFTP, or "2" to use XMODEM to transfer the file to the IAD. If you select XMODEM, proceed to step 3. The IAD prompts you to enter the IP address of the TFTP server.
- 2 Type the IP address of the TFTP server and press Enter. The IAD displays a prompt for the file name to transfer.
- 3 Type the name of the file to transfer and press Enter. To exit without transferring the file, press Escape or Enter without typing the file name.

When XMODEM is selected, if the file is not located, the IAD prompts you for the file transfer speed.

After the IAD transfers the file via TFTP or XMODEM, reset the IAD (page 2-8) to use the new file. If you transfer acos.bin using this option, perform a hard reset (page 3-16).

## TFTP Server Menu

Type "T" on the File Transfer menu to display the TFTP Server menu (Figure 3.10) where you can enable and disable read access, write access, and console output.

**Figure 3.10** *TFTP Server Menu*

```
*****
*                               TFTP Server Menu                               *
*****
  IP Read access   = enabled
  IP Write access  = disabled
  EOC Read access  = enabled
  EOC Write access = disabled
  Console output   = disabled

  R. Toggle Read Access via IP
  W. Toggle Write Access via IP
  S. Toggle Read Access via EOC
  X. Toggle Write Access via EOC
  Q. Toggle Console Output
  E. Enable All TFTP Transfers
  D. Disable All TFTP Transfers
```

The IAD displays the current settings directly below the menu heading. To successively enable or disable access or output, execute the option again. The IAD saves the configuration and displays the menu. When the options are set correctly, reset the IAD for the changes to take effect.



# CONFIGURATION

## Introduction

---

This chapter describes WAN, Router, Bridge, Voice Path, Firewall, DHCP Server, and NAT Configuration.



---

**NOTICE:** *When the IAD prompts you for input, it displays the default or current value in parentheses. To conveniently accept this value, just press Enter.*

---



---

**NOTICE:** *You must reset the IAD (refer to page 2-8) for configuration changes to take effect.*

---

## Managing Configuration Files

---

Each IAD is shipped with a factory default configuration set in the file *default.st*. Once you make any changes to your IAD, a new file (*config.st*) is created to store the new configuration.

After you have configured the IAD for correct operation in a customer's premises, the current system settings in the *config.st* file may be saved as the custom default configuration file (refer to *Set System Defaults* on page 3-16). You may also copy this file to a PC or TFTP server for downloading to other identically configured IADs. Once you have copied over the custom default file (*custdef.st*), you cannot retrieve it. You should consider copying the *custdef.st* file to a safe location before replacing it.

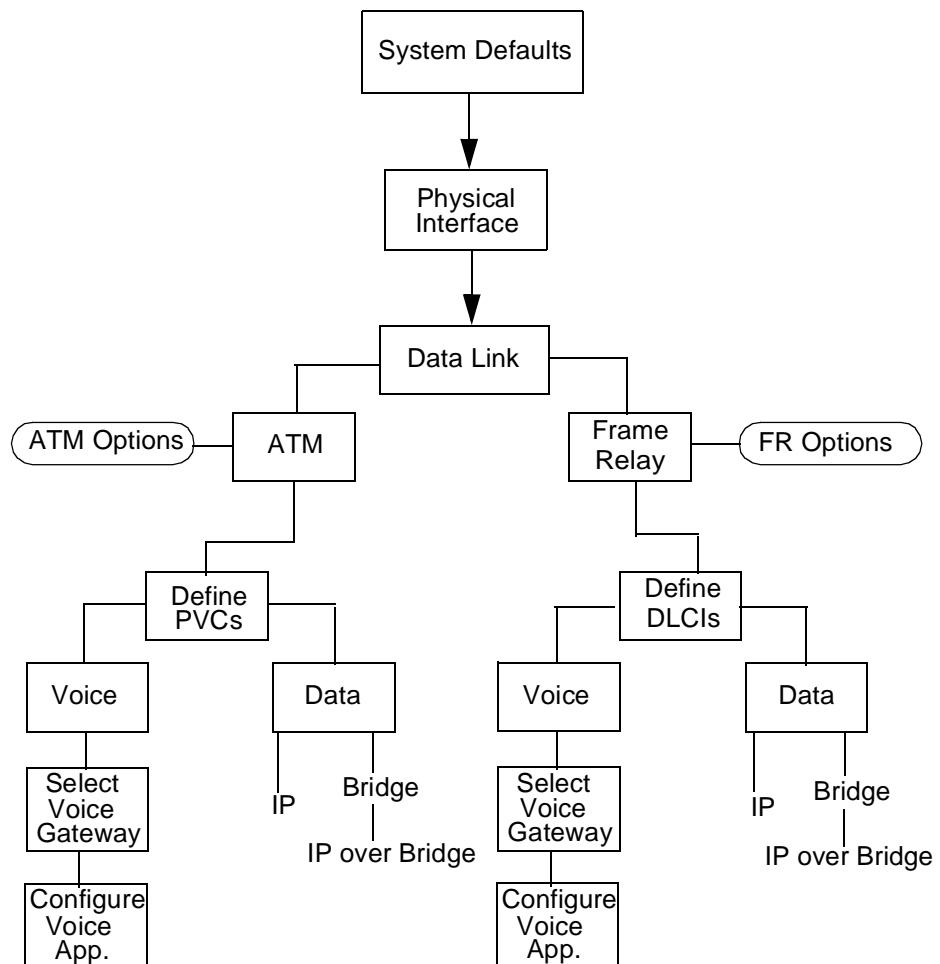
# WAN Configuration

## Basic WAN Setup Tasks

The IAD WAN can be configured for ATM, Frame Relay, or HDLC protocols, depending on the interface. (Refer to the flowchart in Figure 4.1.) The T1/E1 and SDSL interfaces support ATM, Frame Relay, and HDLC. The ADSL and SHDSL interfaces support ATM only. The US1 interface supports Frame Relay and HDLC. To set up the IAD for voice and data operation, you must first perform these basic tasks listed below:

- :Configure the WAN interface for your IAD (page 4-4)
- Select ATM or Frame Relay as the datalink protocol (page 4-3)
- For ATM protocol, configure ATM PVCs (page 4-24) and ATM options (page 4-30)
- For Frame Relay protocol, configure Frame Relay DLCIs (page 4-32) and Frame Relay options (page 4-35)
- Configure the voice path (page 4-61).

**Figure 4.1** WAN Configuration Flowchart



## Setting the WAN Port IP Address

Before you configure the WAN port IP address, you must get the proper IP address and subnet mask address identified for Internet access by your network administrator.

- 1 Type "2" on the Main menu (Figure 2.2). The IAD displays the Router Configuration menu (Figure 2.3).
- 2 Type "C" to select Configure Port IP Address. The IAD displays the available interfaces, which depend on the specific IAD as shown in Figure 2.4 and Figure 2.5.
- 3 Select the option for the interface you wish to configure with the IP address. IP addresses already configured will be listed with an ID such as is shown in the example below.

```
IP interfaces on port 1:
ID          IPAddr          IPMask          Priority
-----
0          192.168.xxx.xxx  255.255.255.128  NORMAL
```

**Enter connection to configure:**

- 4 Type the ID number of the connection you want to configure and press Enter. To overwrite a listed IP address, select the corresponding ID number (in this case "0"). To add IP addresses on the interface, select a different ID number (in this case "1-7").
- 5 Type the new IP Address, and press Enter (or press Enter to retain the current IP address). The IAD displays the Current Subnet Mask and prompts you for a new one.
- 6 Type the new Subnet Mask and press Enter. The IAD prompts you to select High or Normal priority.
- 7 To give the interface normal priority, type "N" or press Enter. Select "H" for high.
- 8 Type "Y" or Enter to save the new IP Address and Subnet Mask.
- 9 Reset the IAD as described below (also refer to *Resetting the IAD* on page 2-8) for the new IP address to be in effect.

## Identifying the WAN Interface and Datalink Protocol

The sections you'll refer to in this manual for WAN configuration depend on the IAD model and the datalink protocol you choose.

Voice and data traffic are each carried in their own PVCs (ATM protocol) or DLCIs (Frame Relay protocol). You may define up to eight PVCs or DLCIs for voice and data.

For a voice circuit, a single PVC or DLCI can carry the voice traffic for all voice ports on the IAD. (Refer to *Voice Path Configuration* on page 4-60.) The high-port IADs also have a Universal Serial Interface (USI) port. Menus for the USI port are included on the high-port IADs' WAN configuration menus.

First, identify your IAD and datalink protocol using the information listed in the tables below. Then, perform the tasks as directed.

<b>T1/E1, SDSL, or USI with Frame Relay</b>	<ol style="list-style-type: none"> <li>1. Configure T1/E1 (page 4-10), or configure SDSL (page 4-6), or configure USI (page 4-21)</li> <li>2. Set the datalink protocol to Frame Relay (page 4-21)</li> <li>3. Configure DLCIs (page 4-32)</li> <li>4. Configure Frame Relay options (page 4-35)</li> <li>5. Configure the voice path (page 4-60)</li> </ol>
<b>T1/E1, SDSL, ADSL, SHDSL with ATM</b>	<ol style="list-style-type: none"> <li>1. Configure T1/E1 (page 4-10), or configure SDSL (page 4-6), or configure ADSL (page 4-18), or configure SHDSL (page 4-19)</li> <li>2. Set the datalink protocol to ATM (page 4-21)</li> <li>3. Configure PVCs (page 4-24)</li> <li>4. Configure ATM (page 4-30)</li> <li>5. Configure the voice path (page 4-60)</li> </ol>

## WAN Configuration Menu

Configuring the IAD for voice transmissions across the WAN involves several tasks. Tasks in this chapter are described beginning at the WAN Configuration menu, which varies based on the WAN interface and datalink protocol.

**Figure 4.2** *WAN Configuration Menu - Configuring SDSL*

```

*****
*           WAN Configuration Menu           *
*****

          Configuring SDSL

          0. Quick Configuration
          1. Configure Datalink Protocol
          2. Configure Physical Interface
          3. Configure PVCs
          4. Configure ATM Options

```

**Figure 4.3** *WAN Configuration Menu (ATM) - Configuring T1/E1*

```

*****
*           WAN Configuration Menu           *
*****

          Configuring T1/E1

          1. Configure Datalink Protocol
          2. Configure Physical Interface
          3. Configure PVCs
          4. Configure ATM Options

```




---

**NOTICE:** *The options displayed on the WAN Configuration menu above are the options you will see if ATM is the configured Datalink Protocol (refer to “Configure Datalink Protocol” below).*

---




---

**NOTICE:** *You must sign on as Supervisor to configure the WAN interface. Be sure to reset the IAD when you have finished making changes to WAN settings. Resetting the IAD causes the configuration changes to take effect.*

---

**Figure 4.4** *WAN Configuration Menu (Frame Relay) - Configuring T1/E1*

```
*****
*           WAN Configuration Menu           *
*****

      Configuring T1/E1

1. Configure Datalink Protocol
2. Configure Physical Interface
3. Configure DLCIs
4. Configure FR Options
```

**Figure 4.5** *WAN Configuration Menu - Configuring ADSL*

```
*****
*           WAN Configuration Menu           *
*****

      Configuring G7070 ADSL ATU-R

1. Configure Datalink Protocol
2. Configure Physical Interface
3. Configure PUCs
4. Configure ATM Options
```

**Figure 4.6** *WAN Configuration Menu - Configuring SHDSL*

```
*****
*           WAN Configuration Menu           *
*****

      Configuring G2237 xDSL

1. Configure Datalink Protocol
2. Configure Physical Interface
3. Configure PUCs
4. Configure ATM Options
```

**Figure 4.7** *WAN Configuration Menu - Configuring USI*

```
*****
*           WAN Configuration Menu           *
*****

      Configuring Universal Serial

1. Configure Datalink Protocol
2. Configure Physical Interface
```

**Figure 4.8** *WAN Configuration Menu - Configuring TDM*

```
*****
*           WAN Configuration Menu           *
*****

      Configuring T1/E1 TDM Voice

1. Configure Datalink Protocol
2. Configure Physical Interface
```

**Figure 4.9** *WAN Configuration Menu (USI) (High-Port-Count IADs Only)*

```
*****
*           WAN Configuration Menu           *
*****

      Configuring Universal Serial

1. Configure Datalink Protocol
2. Configure Physical Interface
```

Although you must reset the IAD when you have completed WAN configuration, you may configure *all* WAN configuration (i.e., each numbered option) before resetting the IAD.

## **Configure Physical Interface – SDSL**

The tasks described in this section all begin on the SDSL Configuration menu (Figure 4.10). You should review and update each of these options as necessary, and always reset the IAD when you finish SDSL configuration.

To configure the SDSL interface, Type "2" (Configure Physical Interface) on the WAN Configuration menu to display the SDSL Configuration menu.

Figure 4.10 SDSL Configuration Menu

```
*****
*                SDSL Configuration                *
*****
Current SDSL configuration:
  CPE, AUTO Cycle, Bit Order: Sign.Mag,
  SPEED = 1744 Kbps, Conexant AutoBaud: Disabled

1. Toggle SDSL Mode (CO or CPE)
2. Set SDSL Speed to Auto Cycle (Nokia)
3. Set SDSL Speed to Auto Sense (Copper Mountain)
4. Enable/Disable Conexant AutoBaud Mode
5. Set SDSL Sync Delay (Lucent)
6. Set SDSL to AccessLan CPE Mode
7. Set SDSL for IMAS DSLAM (Nortel)
8. Set SDSL Speed Manually
9. SDSL Interface Mode (Bit Order)
C. Configure SDSL Auto Cycle Speed Table
P. Display SDSL Auto Cycle Speed Table

ESC to return to previous menu

->_
```



---

**NOTICE:** *The options you see on the SDSL Configuration menu depend on the specific DSLAM.*

---

**Toggle SDSL Mode  
(CPE or CO)**

To select CPE or CO Mode, follow the steps below.

- 1 Type "1" on the SDSL Configuration menu (Figure 4.10). The IAD displays the current SDSL Mode and prompts you to change it.
- 2 Type "1" to select CO, or type "2" to select CPE. The IAD sets the mode and redisplay the SDSL Configuration menu.



---

**NOTICE:** *The CO Mode is reserved for testing. CPE is the normal mode.*

---

**Set SDSL Speed to  
Auto Cycle (Nokia)**

To select Auto Cycle - Nokia DSLAM, type "2" on the SDSL Configuration menu to set the SDSL speed to Auto Cycle for connecting to a Nokia DSLAM.

The IAD saves the configuration and redisplay the SDSL Configuration menu.

**Set SDSL Speed to  
Auto Sense (Copper  
Mountain)**

To select Auto Sense – Copper Mountain DSLAM, type "3" on the SDSL Configuration menu (Figure 4.10) to set the SDSL speed to Auto Sense for connecting to a Copper Mountain DSLAM. The IAD saves the configuration and redisplay the SDSL Configuration menu.

- Enable/Disable  
Conexant Autobaud  
Mode**
- 1 Type "4" on the SDSL Configuration menu (Figure 4.10) to enable or disable Conexant Autobaud mode. The IAD displays the current setting and prompts you to change it.
  - 2 Type "E" to enable or "D" to disable Autobaud mode. The IAD saves the configuration and redisplay the SDSL Configuration menu.

- Set SDSL Sync Delay  
(Lucent)**
- To set the SDSL Sync Delay (Lucent), follow the steps listed below.
- 1 Type "5" on the SDSL Configuration menu (Figure 4.10) to enable Sync Delay, which is paired with Conexant Autobaud mode. The IAD displays the current Autobaud setting and prompts you to change it.
  - 2 Type "E" to enable or "D" to disable Autobaud mode. If you disable Autobaud, you must set the SDSL data rate manually. The IAD prompts you to enter the SDSL Rate.
  - 3 Enter the rate (144 to 2320 kbps, evenly divisible by 8) and press Enter.
  - 4 The IAD saves the configuration and redisplay the SDSL Configuration menu.

- Set SDSL to AccessLan  
CPE Mode**
- Type "6" on the SDSL Configuration menu (Figure 4.10) to set the IAD to CPE Mode for connecting to an AccessLan DSLAM. The IAD saves the configuration and redisplay the SDSL Configuration menu.

- Set SDSL IMAS  
DSLAM (Nortel)**
- 1 Type "7" on the SDSL Configuration menu (Figure 4.10) to set the SDSL first-try speed for connecting to an IMAS (Nortel) DSLAM. The IAD displays the IMAS First Speed Option menu (Figure 4.11).

**Figure 4.11** *IMAS First Speed Option Menu*

```

*****
*           IMAS First Speed Option           *
*****

      Select First Speed to Try

1. 2320 Kbps
2. 1744 Kbps
3. 1536 Kbps
4. 1152 Kbps
5. 768  Kbps
6. 384  Kbps
7. 192  Kbps

```

- 2 Type the option to select the appropriate SDSL speed.

The IAD saves the configuration and redisplay the SDSL Configuration menu.

- Set SDSL Speed  
Manually**
- 1 Type "8" on the SDSL Configuration menu (Figure 4.10) to set the SDSL speed manually. The IAD prompts you to enter the SDSL Data Rate.
  - 2 Type the rate (144 to 2320 kbps, evenly divisible by 8) and press Enter. The IAD asks you if you wish to set Data to Framed Mode.



- 3 Enter "Y" for Framed Mode, or any other character if you are connecting to a DSLAM other than a Nokia DSLAM.

The IAD saves the configuration and redisplay the SDSL Configuration menu.

**Set SDSL Interface Mode**

- 1 Type "9" on the SDSL Configuration menu (Figure 4.10) to set the SDSL interface mode (bit order). The IAD displays the current setting and prompts you to set the DSL Interface Mode.
- 2 Type "1" to set Interface Mode to Magnitude, Sign, or type "2" to set Interface Mode to Sign, Magnitude.

The IAD saves the configuration and redisplay the SDSL Configuration menu.

**Configure SDSL Auto Cycle Speed Table**

- 1 Type "C" on the SDSL Configuration menu (Figure 4.10) to configure any of the 14 SDSL auto cycle speed table entries. The IAD prompts you to enter the SDSL Auto Cycle Speed.
- 2 Type the value of the entry to configure. The IAD prompts you for the SDSL Data Rate.
- 3 Type the data rate (144 to 2320 kbps, evenly divisible by 8).

The IAD saves the configuration and redisplay the SDSL Configuration menu.

**Display SDSL Auto Cycle Speed Table**

Type "P" on the SDSL Configuration menu (Figure 4.10) to display the SDSL Auto Cycle Speed Table as shown in below.

**Figure 4.12** *SDSL Auto Cycle Speed Table*

Entry	SDSL Speed
1	2320000
2	2320000
3	1744000
4	1744000
5	1536000
6	1536000
7	1152000
8	1152000
9	768000
10	768000
11	384000
12	384000
13	192000
14	192000

## Quick Configuration for SDSL WAN




---

**NOTICE:** *The Quick Configuration menu is designed to easily configure predefined settings for specified DSLAMs.*

---

The 8000 Series contains a number of predefined configurations for physical connections and PVCs.

To use one of the predefined configurations, follow the steps below.

- 1 On the WAN Configuration Menu (Figure 4.4), type "5" to display the Quick Configuration menu.

**Figure 4.13** *Quick Configuration Menu*

```
*****
*           Quick Configuration           *
*****

** System will reset after changing configuration **

Current configuration:
  Differs from listed configurations

1. Lucent Stinger (Conexant Autobaud, Payload Scrambling)
2. Nokia (Auto Cycle)
3. Copper Mountain (Auto Sense)
4. Paradyne (Unframed 784kbps, Payload Scrambling)
5. AccessLan CPE
6. Nortel IMAS
7. ATM (Unframed, 1152kbps fixed)
8. Frame Relay (784kbps fixed)
```

- 2 Type the option corresponding to the DSLAM to which the IAD is connected. The IAD automatically resets.
- 3 To continue configuration, log back onto the IAD.

### **Configure Physical Interface – T1/E1**

The tasks described in this section all begin on the T1 or E1 Configuration menu. The tasks are described in order. Review and update each of the options as necessary, and reset the IAD when you finish WAN configuration.

Type "2" on the WAN Configuration menu (Figure 4.4) to display the T1 Configuration menu (Figure 4.14).

**Figure 4.14 T1 Configuration Menu**

```

*****
*           T1 Configuration Menu           *
*****

          T1 Frame Mode           = ESF
          Line Build Out          = 0 dB
          B8ZS coding              = ENABLED
          Channels Enabled         = 1-24
          Idle Channel Code       = 0x7F
          Tx Clock Source         = External (Loop Clocking)

1. Select Frame Mode (D4 or ESF)
2. Select Line Build Out
3. Select B8ZS or AMI
4. Configure Loopback
5. Configure Active Channels
6. Configure Idle Channel Code
8. Configure Clock Source
9. Change to E1 Mode

P. Display Physical Layer Stats and Alarm Log
Z. Clear Physical Layer Stats

```

The top part of the menu displays the current configuration. You can change the configuration by selecting the appropriate option in accordance with the details provided below for each option. Remember always to reset the IAD when you finish T1 configuration.

**Select Frame Mode (D4 or ESF)** To select the Frame Mode, follow the steps below.

- 1 Type "1" on the T1 Configuration menu (Figure 4.14) to select Frame Mode (D4 or ESF) and display the T1 Frame Mode menu:

**Figure 4.15 Select T1 Frame Mode Menu**

```

*****
*           Select T1 Frame Mode           *
*****

          T1 Frame Mode           = ESF

1. ESF Frame Mode
2. D4 (or SF) Frame Mode

```

- 2 Type "1" to select ESF Frame Mode, or "2" to select D4 Frame mode. The IAD resets the interface and redisplay the T1 Frame Mode menu.
- 3 Press Escape to return to the T1 Configuration menu.
- 4 Continue with other configuration tasks.

**Select Transmit Line Build Out** To select Line Build Out, follow the steps below.

- 1 Type "2" on the T1 Configuration menu (Figure 4.14) to display the Line Build Out menu.

**Figure 4.16** *Select Line Build Out Menu*

```
*****
*       Select Line Build Out       *
*****

                Line Build Out          = 0 dB

1. 0    To 133 Feet (Short haul)
2. 133 To 266 Feet (Short haul)
3. 266 To 399 Feet (Short haul)
4. 399 To 533 Feet (Short haul)
5. 533 To 655 Feet (Short haul)
6. 0    dB (Long haul)
7. -7.5 dB (Long haul)
8. -15  dB (Long haul)
9. -22.5 dB (Long haul)
```

- 2** Type the option to select the line build out that corresponds to the T1 span length in use. The IAD resets the interface and redisplay the Select Line Build Out menu.
- 3** Press Escape to return to the T1 Configuration menu and continue with other configuration tasks.

**Select B8ZS or AMI** To select B8ZS or AMI, follow the steps below.

- 1** To set zero suppression, type "3" on the T1 Configuration menu (Figure 4.14) to select B8ZS or AMI. The IAD displays the current setting and prompts you to change it.
- 2** Type "Y" to change the setting.
- 3** Press Escape to return to the T1 Configuration menu and continue with other configuration tasks.

**Configure Loopback** To configure loopback, follow the steps below.

- 1** Type "4" on the T1 Configuration menu (Figure 4.14) to configure loopback. The IAD displays the current setting for each type of loopback and ESP loopback commands, and the Loopback Configuration menu.
- 2** Type the option number "1", "2", "3", "4" or "5" to enable or disable loopbacks. The IAD makes the change and resets the interface.
- 3** Type "6" to enable or disable receipt of ESF loopback commands. (This option is valid only when Framing Mode is set to ESF). The IAD saves the changes and redisplay the Select Loopback Configuration menu.
- 4** Type "7" to configure the loopback time-out period.
- 5** Press Escape to return to the T1 Configuration menu and continue with other configuration tasks.

**Configure Active Channels** To configure Active Channels, follow the steps below.

- 1 Type "5" on the T1 Configuration menu (Figure 4.14) to select the Channel Configuration Menu (Figure 4.17). Use this menu to determine which DS0s have data.

**Figure 4.17** *Channel Configuration Menu*

```
*****
*   Channel Configuration Menu   *
*****

                Channels Enabled      = 1-24

1. Enable All Channels
2. Disable All Channels
3. Toggle Individual Channels
4. Add Channel Range
5. Auto Detect DS0 On Boot
6. Auto Detect DS0 After Carrier Fail
7. Auto Detect DS0 While Protocol Down
8. Disable Auto Detect DS0

S. Start DS0 Search Now
```

Each option on this menu is described in detail below.

### ***Enable All Channels***

Type "1" to enable all channels for voice traffic.

### ***Disable All Channels***

Type "2" to disable all channels for voice traffic.

### ***Toggle Individual Channels***

Type "3" to toggle channels on which to configure individual DS0s for voice traffic.

### ***Add Channel Range***

Type "4" to enable a range of channels on which to configure DS0s for voice traffic.



---

**NOTICE:** *The Channel Configuration menus options 5, 6, 7, 8, and S described below are only accessible on the 8208 and 8208s units.*

---

### ***Auto Detect DS0 On Boot***

Type "5" to automatically search for voice DS0s immediately upon system boot or reboot when the WAN has detected the carrier as "up."

### ***Auto Detect DS0 After Carrier Fail***

Type "6" to automatically search for voice DS0s every time the T1/E1 carrier has dropped and re-synced. For this option, the T1/E1 carrier can be physically

interrupted or the service provider can send AIS. Either will cause the T1/E1 framer to lose frame sync and initiate a voice DS0 search.

### ***Auto Detect DS0 While Protocol Down***

Type "7" to automatically search for voice DS0s while the T1/E1 carrier is "up," but the WAN layer protocol is "down." When this option is selected, the service provider changes to the voice DS0 assignment on the WAN layer. The WAN protocol should then go "down" (bounce/reset) and initiate a new voice DS0 search. DS0 detection will only occur when the WAN protocol transitions from "down" to "up."

### ***Disable Auto Detect DS0***

Type "8" to disable DS0 auto detection.

### ***Start DS0 Search***

Type "S" to immediately begin a search for voice DS0s.

### **Configure Idle Channel Code**

Type "6" on the T1 Configuration menu to assign a value to idle channels.

### **Configure Clock Source**

To Configure the Clock Source, follow the steps below.

- 1 Type "8" on the T1 Configuration menu to select Configure Transmit Clock Source, which will display the Select Tx Clock Source menu (Figure 4.18) with a status message.

**Figure 4.18** *Select Tx Clock Source Menu*

```
*****  
*   Select Tx Clock Source   *  
*****
```

**Tx Clock is derived from Rx clock (Slave Mode).**

1. External (Slave Mode)
2. Internal (Master Mode)

- 2 Type "1" to select External or Slave mode, or type "2" to select Internal or Master mode. The IAD saves the configuration and resets the interface.
- 3 Press Escape to return to the T1 Configuration menu and continue with other configuration tasks.
- 4 After you reset the IAD, you will see a prompt to type "1" to select External or "2" to select Internal mode. Enter your selection.

The IAD saves the configuration and resets the interface.

### **Change to E1 Mode**

Type "9" on the T1 Configuration menu (Figure 4.14) to switch from T1 to E1 mode (Figure 4.19). (This menu option changes to T1 when the IAD is configured for E1.)

**Figure 4.19** *E1 Configuration Menu*

```
*****
*           E1 Configuration Menu           *
*****

          E1 Frame Mode           = FAS
          Channels Enabled         = 1-31
          Idle Channel Code       = 0x7F
          Tx Clock Source         = External (Loop Clocking)

1. Select Frame/CRC4 Mode
3. Configure S-Bits
4. Configure Loopback
5. Configure Active Channels
6. Configure Idle Channel Code
8. Configure Clock Source
9. Change to T1 Mode

P. Display Physical Layer Stats and Alarm Log
2. Clear Physical Layer Stats
```

### **Select Frame/CRC4 Mode**

Type "1" on the E1 Configuration menu to display the E1 Frame Mode menu (Figure 4.20). From this menu, you may select the framing for the network side of the DSU/CSU (default is FAS).

**Figure 4.20** *E1 Frame Mode Menu*

```
*****
*           Select E1 Frame Mode           *
*****

          E1 Frame Mode           = FAS

1. FAS
2. FAS (CRC4 Enabled)
3. Multi-Frame CAS
4. Multi-Frame CAS (CRC4 Enabled)
```

### **Configure S-Bits**

Type "3" on the E1 Configuration menu to display the Configure S-Bits menu (Figure 4.21). Toggle to display the status of special bits found in timeslot zero.

Figure 4.21 *Configure S-Bits Menu*

```
*****
*           Configure S-Bits Menu           *
*****

Sa4 Bit           = Cleared
Sa5 Bit           = Cleared
Sa6 Bit           = Cleared
Sa7 Bit           = Cleared
Sa8 Bit           = Cleared

2. Toggle Sa4 Bit
3. Toggle Sa5 Bit
4. Toggle Sa6 Bit
5. Toggle Sa7 Bit
6. Toggle Sa8 Bit
```

**Configure Loopback** Type "4" on the E1 Configuration menu to select Configure Loopback, which will displace the menu shown in Figure 4.22

Figure 4.22 *Select Loopback Configuration*

```
*****
* Select Loopback Configuration *
*****

Active Loopback           : None
Loopback Timeout (Minutes) : 20 Minutes

1. Start/Stop Payload Loopback
2. Start/Stop Line Loopback
3. Start/Stop Local Loopback (Inward, Master mode only)

7. Configure Loopback Timeout
```

The Payload Loopback loops the data after the T1 framer back to the network. The Line Loopback loops the data before the T1 framer back to the network. The Local (Inward) Loopback loops the data after the T1 framer back to the user.

**Configure Active Channels** Type "5" on the E1 Configuration menu (Figure 4.19) to select Channel Configuration menu (Figure 4.23). Use this menu to determine which DS0s have data.



**Figure 4.23** *Channel Configuration Menu*

```
*****
*   Channel Configuration Menu   *
*****

          Channels Enabled      = 1-24

1. Enable All Channels
2. Disable All Channels
3. Toggle Individual Channels
4. Add Channel Range
5. Auto Detect DS0 On Boot
6. Auto Detect DS0 After Carrier Fail
7. Auto Detect DS0 While Protocol Down
8. Disable Auto Detect DS0

S. Start DS0 Search Now
```

This menu lets you enable or disable all channels, enable or disable individual channels, or select a range of channels to enable/disable.

**Configure Idle Channel Code** Type "6" on the E1 Configuration menu to assign a value to idle channels.

**Configure Clock Source** To Configure the Clock Source, follow the steps below.

**1** Type "8" on the E1 Configuration menu to select Configure Clock Source, which will display the Select Tx Clock Source menu (Figure 4.24) with a status message.

**Figure 4.24** *Select Tx Clock Source Menu*

```
*****
*   Select Tx Clock Source       *
*****
```

**Tx Clock is derived from Rx clock (Slave Mode).**

- 1. External (Slave Mode)**
- 2. Internal (Master Mode)**

**2** Type "1" to select External or Slave mode, or type "2" to select Internal or Master mode. The IAD saves the configuration and resets the interface.

**3** Press Escape to return to the E1 Configuration menu and continue with other configuration tasks.

**4** After you reset the IAD, you will see a prompt to type "1" to select External or "2" to select Internal mode. Enter your selection.

**Display Physical Layer Stats and Alarm Log** The physical layer statistics displays the T1/E1 error rate in errors per second for the past second. An event log (up to 5 kB) is maintained for certain events. The time stamp is relative to the last system reset. As new events are added, older events are discarded when the file size is maximized.

Events include the start and end of Telnet sessions, SNMP access with an invalid community name, system reset and system reset from menu command, and the WAN link going up or down.

- 1 Type "P" on the T1/E1 Configuration menu (Figure 4.14) to display the physical layer statistics and the alarm log.

**Figure 4.25** *Sample Physical Layer Stats and Alarm Log:*

```

T1/E1 Error Counters

Total Errors:
  Framing Bit Error           = 0
  CRC Error Count             = 0
  Line Code Violation         = 0
  Far End Block Error         = 0
  Rx Loss of Frame            = 0
  Severly Errored Frame       = 0

Errored Seconds:
  Framing Bit Error           = 0
  CRC Error Count             = 0
  Line Code Violation         = 0
  Far End Block Error         = 0
  Rx Loss of Frame            = 0
  Severly Errored Frame       = 0
  
```

- 2 Enter any key to continue paging through the report; press Escape to cancel and return to the T1/E1 Configuration menu.

**Clear Physical Layer Stats** Type "Z" on the T1/E1 Configuration menu (Figure 4.14) to clear all Physical Layer statistics.

## Configure Physical Interface – ADSL

The tasks described in this section all begin on the ADSL Configuration menu (Figure 4.26). You should review and update each of these options as necessary, and always reset the IAD when you finish ADSL configuration.

To configure the ADSL interface, Type "1" (Configure Physical Interface) on the WAN Configuration menu (Figure 4.5) to display the ADSL Configuration menu.

**Figure 4.26** *ADSL Configuration Menu*

```

*****
*           G7070 ADSL ATU-R Configuration           *
*****

1. Configure ADSL Standard
  
```




---

**NOTICE:** *The options you see on the ADSL Configuration menu depend on the specific DSLAM.*

---

**Set ADSL Standard**    **1** Type 1 to select Configure ADSL Standard. The IAD displays the ADSL Standards menu.

**Figure 4.27** *ADSL Standards Menu.*

```
*****
*           ADSL Standard to use for Startup           *
*****

      Current ADSL Standard :
      Multi-Mode

1. T1.413
2. G.LITE
3. G.DMT
4. Alcatel 1.4
5. Multi-Mode
6. ADI
7. Alcatel
```

**2** Type the option corresponding to the ATM Standard. The IAD sets the standard you select and displays the menu.




---

**NOTICE:** *If no default route is configured on the IAD, the first PPP interface that completes negotiation will be assigned as the default interface. If multiple PPP interfaces are configured, this could result in the wrong interface being assigned as the default. This applies to PPPoA and PPPoE.*

---

## Configure Physical Interface – SHDSL

The tasks described in this section all begin on the SHDSL Configuration menu (Figure 4.28). You should review and update each of these options as necessary, and always reset the IAD when you finish SHDSL configuration.

To configure the SHDSL interface, Type "2" (Configure Physical Interface) on the WAN Configuration menu (Figure 4.6) to display the SHDSL Configuration menu.

Figure 4.28 SHDSL Configuration Menu

```
*****
*           G2237 xDSL Configuration           *
*****

Current Interface Type is: G.SHDSL-A.

Mode: CPE, Rate Mode: FIXED, Line Rate: 2312K
Debug: DISABLED

1. Select xDSL Interface Type
2. Select CPE/CO Mode
3. Select Rate Mode
4. Select Line Rate
```

**Select SHDSL  
Interface Type**

To select the Interface Type, follow the steps below.

- 1 Type "1" on the SHDSL Configuration menu (Figure 4.28). The IAD displays the current SHDSL Interface Type menu. Type the option to select SHDSL Annex A for operation in the U.S. or Annex B for operation in Europe. The IAD sets the interface type and displays the menu
- 2 Press Escape to return to the SHDSL Configuration menu.

**Select CPE or CO  
Mode**

To select CPE or CO Mode, follow the steps below.

- 1 Type "2" on the SHDSL Configuration menu (Figure 4.28). The IAD displays the current SHDSL Mode and prompts you to change it.
- 2 Type "1" to select CO, or type "2" to select CPE. The IAD sets the mode and redisplay the SHDSL Configuration menu.



---

**NOTICE:** *The CO Mode is reserved for testing. CPE is the normal mode.*

---

**Enable/Disable  
Adaptive Rate Mode**

To configure the Adaptive Rate Mode, follow the steps below.

- 1 Type "3" on the SHDSL Configuration menu (Figure 4.28) to display the Configure SHDSL Rate Mode menu.
- 2 Type "1" to select Fixed, or type "2" to select Adaptive. The IAD sets the rate mode and displays the menu.
- 3 Press Escape to return to the SHDSL Configuration menu.

**Select Line Rate**

To select a Line Rate, follow the steps below.

- 1 Type "4" on the SHDSL Configuration menu (Figure 4.28) to display the current line rate and a prompt to change it.
- 2 Type a line rate value (between 64 and 2320 kpbs). This value must be divisible by 8. The IAD sets the rate and displays the SHDSL Configuration menu.

## Configure Physical Interface – USI

The tasks described below begin on the USI Configuration menu (Figure 4.29). Review and update these options as necessary and always reset the IAD when you have completed USI Interface configuration.

**Figure 4.29** *USI Configuration Menu*

```
*****
*           USI Configuration           *
*****
  1. Set WAN interface type
  2. Configure Data Rate and Clocking Options
```

- 1 Type "1" on the USI Configuration menu to see the menu below and select the physical layer protocol for the USI port. Select either RS-530 or V.35 for the physical interface.

**Figure 4.30** *USI Interface Type*

```
*****
*           USI Interface Type           *
*****
```

```
USI WAN mode is now: RS530 V.11 Termination Enabled
```

1. RS-530
2. V.35

- 2 Type "2" on the USI Configuration menu to select the USI data rate and clocking options. The data rate is in 64 kbps increments up to a maximum of 2.048 Mbps. The Receive Clock can be configured to use either an internal or external clock source.

**Figure 4.31** *Serial Interface Clock Speed Option Menu*

```
*****
* Serial Interface Clock Speed Option Menu *
*****
```

```
- Serial Data Rate is now: 1536000 Based on Internal Oscillator
- Receive Clock is External
```

2. Set Clock Speed Manually
3. Use Internal Receive Clock
4. Use External Receive Clock

To set the speed manually, enter the desired multiplier of 64 kbps (maximum is 32 or 2.048 Mbps).

## Configure Datalink Protocol

If you are setting up voice and data channels, you can select ATM or Frame Relay as you set up the channels as described below.

To select ATM or Frame Relay as the datalink protocol, on the WAN Configuration menu, type "1". The IAD displays the WAN Datalink Protocol

Configuration menu (Figure 4.32), identifying the current datalink protocol just below the banner.

**Figure 4.32** *WAN Datalink Protocol Configuration Menu*

```
*****
*           WAN Datalink Protocol Configuration Menu           *
*****

Current DataLink Protocol : TDM Voice + IP Plus compatible HDLC

Current Voice Protocol : CAS

2. Raw HDLC
3. Cisco compatible HDLC
4. IP-Plus compatible HDLC
5. PPP (over Raw HDLC)
6. ATM
7. Frame Relay
E. TDM Voice with Data
```



---

**NOTICE:** *The WAN Datalink Protocol Configuration menu sets up the IAD internet link for Level 2 Transmission Convergence onto the physical link. The following generic description of the options listed on this menu are for information only. Specific encapsulation options are shown and selected when configuring ATM PVCs (refer to page 4-24) or Frame Relay DLCIs (refer to page 4-32).*

---

### ***Raw HDLC***

Level 2 frame delineation, link control services, and error detection are provided at physical interface for non-encapsulated transport of IAD payload between two points.

### ***Cisco Compatible HDLC***

Same Level 2 functionality as described under Raw HDLC above, but with awareness of Cisco-implemented HDLC control field changes (e.g., modifications in the control bytes to allow transparent implementation of the Cisco Discovery Protocol).

### ***IP-Plus Compatible HDLC***

Provides support for IP Headers in the HDLC payload.

### ***PPP (Over Raw HDLC)***

Point-to-Point over raw HDLC encapsulation.

### ***ATM or Frame Relay***

Multiprotocol over ATM (RFC 1483) encapsulation or Multiprotocol over Frame Relay (RFC 1490) encapsulation.

When you select ATM as the datalink protocol, the IAD displays the PVC and ATM options on the WAN Configuration menu.

When you select Frame Relay, the IAD displays the Frame Relay options on the WAN Configuration menu – options 3 and 4 on the menu shown below.

### ***TDM Voice***

To configure, on a per-DS0 basis, voice traffic for the POTS ports and data traffic for the Ethernet port, follow the steps below.

- 1** From the WAN Configuration menu (Figure 4.8), type “1” to see the menu shown in Figure 4.33.

**Figure 4.33** *WAN Datalink Protocol for Voice Channels.*

```
*****
*      WAN Datalink Protocol Configuration Menu      *
*****

Current DataLink Protocol : TDM Voice + IP Plus compatible HDLC

Current Voice Protocol : CAS

2. Raw HDLC
3. Cisco compatible HDLC
4. IP-Plus compatible HDLC
5. PPP (over Raw HDLC)
6. ATM
7. Frame Relay
E. TDM Voice with Data
```

- 2** Type “E” to configure the TDM Voice with Data and bring up the Current Configuration Table shown in Figure 4.34.

**Figure 4.34** *Current Configuration Table*

```

*****
*      T1/E1 Channel Configuration Menu      *
*****

Current configuration table

          1 1 1 1 1 1 1 1 1 1 2 2 2 2
1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4
- - - - - - - - - - - - - - - - - - - - -
v v v U U U U D D D U U U U U U U U U U U

v=voice channel  D=data channel
U=unconfigured  x=not available

Voice Protocol : CAS - MEL TS16
Data Protocol  : ATM

1. Configure Voice Channels
2. Configure Voice Protocol
3. Configure Data Channels
4. Configure Data Protocol
5. Unconfigure All Channels

```

**3** Type "1" to select a channel range for voice as shown in Figure 4.35.

**Figure 4.35** *Configure Voice Channels*

```

->1
Enter Channel or Channel Range for voice (e.g., 1-8):

```

**4** Type "2" on the T1/E1 Channel Configuration menu (Figure 4.34) to select the signaling protocol for voice channels.

**Figure 4.36** *Select Signaling Protocol for Voice Channels*

```

*****
* Select Signaling Protocol For Voice Channels *
*****
2. CAS - ANSI T1.403
3. CAS - MEL TS16

```

**5** Type "3" on the T1/E1 Channel Configuration menu (Figure 4.34) to select a channel range for voice channels. You will see a screen similar to that shown in Figure 4.35.

**6** Type "4" on the T1/E1 Channel Configuration menu (Figure 4.34) to select the datalink protocol for the voice channels. Select Datalink Protocol for Voice Channels.

## Configure ATM PVCs

You may configure up to eight ATM PVCs on the IAD. Remember always to reset the IAD to make PVCs active.



- 1 Type "3" on the WAN "3" menu (Figure 4.4). The IAD displays the ATM PVC Configuration menu (Figure 4.37)




---

**NOTICE:** *Before you configure PVCs, you must first set the datalink protocol ATM. If option 3 on the WAN Configuration menu displays Configure DLCIs instead of Configure PVCs, your datalink protocol is set to Frame Relay instead of ATM.*

---

**Figure 4.37** *ATM PVC Configuration Menu*

```
*****
*           ATM PVC Config Menu           *
*****
1. Add New PVC
2. Modify Existing PVC
3. Delete PVC
4. Show Current PVCs
```

- 2 Type the option to perform a task. Each option is described below.

### **Add New PVC**

To add a new PVC, follow the steps below.

- 1 On the ATM PVC Configuration menu, type "1". The IAD prompts you to enter the VPI.
- 2 Type a VPI value between 0 and 255 (default 0) and press Enter. The IAD then prompts you for the VCI.
- 3 Type a VCI value between 32 and 65535 and press Enter. The IAD displays the ATM Encapsulation Configuration menu as shown in Figure 4.38.

**Figure 4.38** *ATM Encapsulation Configuration Menu*

```
*****
*           ATM Encapsulation Configuration           *
*****
Current Encapsulation : NONE
1. AAL5 (None)
2. AAL0 (None)
3. Proprietary Voice
4. AAL2 (LES, NBT)
5. RFC 1483 (MPoA)
6. RFC 2364 (PPPoA)
7. RFC 2516 (PPPoE)
```

- 4 Type the option for the encapsulation to configure for this PVC. The IAD displays the ATM Service Category Configuration menu (Figure 4.39). If you select either RFC 2364 (PPPoA) from the above menu, follow the on-screen messages to set the PPP authorization type.




---

**NOTICE:** *The WAN Datalink Protocol Configuration menu sets up the IAD internet link for Level 2 Transmission Convergence onto the physical*

---

link. The following generic description of the options listed on this menu are for information only. Specific encapsulation options are shown and selected when configuring ATM PVCs (refer to page 4-24) or Frame Relay DLCIs (refer to page 4-32).

---

- AAL5 or AAL0** 1 Type "1" on the ATM Encapsulation Configuration menu (Figure 4.38) to select AAL5, or "2" to select AAL0 encapsulation. The IAD displays the ATM Service Category Configuration menu (Figure 4.39).

**Figure 4.39** ATM Service Category Configuration Menu

```
*****
*  ATM Service Category Configuration  *
*****
  1. CBR
  2. UBR
  3. VBRnrt
  4. VBRrt
```

- 2 Type "1" to select CBR for high-priority data.  
– or –  
Type "2" to select UBR for low-priority data.  
– or –  
Type "3" to select VBRnrt for low-priority data.  
– or –  
Type "4" to select VBRrt for high-priority data.



---

**NOTICE:** *VBRrt is mapped to CBR and VBRnrt is mapped to UBR.; therefore, only the PCR values are used.*

---

- 3 Type the PCR value or press Enter to set the PCR to the maximum rate for the current line speed. The IAD saves the configuration and displays the ATM PVC Configuration menu (Figure 4.40).

**Figure 4.40** ATM Peak Cell Rate (PCR) Configuration Menu

```
*****
*  ATM Peak Cell Rate (PCR) Configuration  *
*****
  Current line speed for this interface is 1536000 bps

  Please type a PCR value, or
  Press ENTER to accept allowed maximum PCR value for this line speed

Enter Peak Cell Rate (PCR) [3622 cells per second] : _
```



---

**NOTICE:** *Do not use "0" for Voice PVC because "0" will use all available bandwidth, including CBR bandwidth that is not being used. Do not oversubscribe available PCR. Use "0" for only one (1) PVC. Refer to Peak Cell Rate (PCR) Considerations and Recommendations on page C-2.*

---

**Proprietary Voice Encapsulation**

Type "3" on the ATM Encapsulation Configuration (Figure 4.38) menu to select Proprietary Voice encapsulation over a specific PVC. The IAD saves the configuration and displays the ATM PVC Configuration menu.



---

**NOTICE:** *Proprietary Voice Encapsulation is used for Copper Com and Jetstream voice PVCs only.*

---

**AAL2 (LES, NBT)**

Type "4" on the ATM Encapsulation Configuration (Figure 4.38) menu to select AAL2 encapsulation over a specific PVC. The IAD displays the AAL2 Audio Profile Format menu displayed in Figure 4.41.

**Figure 4.41** *AAL2 Audio Profile Format*

```
*****
*   AAL2 Audio Profile Format   *
*****
Current Audio Profile Format : NONE
  1. ITU
  2. ATM Forum
```

If you select ITU, your options will include ITU#1 or ITU#2. If you select ATM Forum, you will choose from the following ATM Forum profiles: 7, 8, 9, 10, 11, or 12.

**RFC 1483 (MPoA), RFC 2364 (PPoA), or RFC 2516 (PPoE)**

**1** Type "5" on the ATM Encapsulation Configuration (Figure 4.38) menu to select RFC 1483 (MPoA), or type "6" to select RFC 2364 (PPoA), or type "7" to select RFC 2516 (PPoE). The IAD displays the menu shown in Figure 4.42.

**Figure 4.42** *ATM Encapsulation Configuration Menu*

```
*****
*   ATM Encapsulation Configuration   *
*****
  1. LLC Encapsulation
  2. VC Muxing
```

**2** Type "1" to select LLC Encapsulation or "2" to select VC Muxing. With either option, the IAD displays the menu shown in Figure 4.43.

**Figure 4.43** *LLC Encapsulation or VC Muxing Configuration Menu*

```
*****
*   ATM Encapsulation Configuration   *
*****
  1. IP Routing
  2. Bridging
  3. MER (MAC Encapsulated Routing)
```

**3** If you type "1" to select IP Routing, the IAD displays the same menu as shown in Figure 4.39 and then displays the menu shown in Figure 4.40. If

you type either "2" or "3", the IAD displays the menu shown in Figure 4.44.

**Figure 4.44** *PPP Authorization Menu*

```
PPP Authorization is currently None
Enter New Authorization type

0. None
1. PAP Client
2. PAP Server
3. CHAP Client
4. CHAP Server
```

- 4 The IAD displays the current PPP authorization and prompts you to change it. If you select options 1 through 4, the IAD displays the current PPP authorization user ID and prompts you to enter a new PPP user ID.
- 5 Enter the new user ID and press Enter and then type a password and press Enter. If you select option 0 (None), the IAD displays the IPCP IP Address Type menu.

**Figure 4.45** *IPCP Configuration Menu*

```
*****
*           IPCP IP Address Type Menu           *
*****
1. Static IP Address
2. IPCP Address Assignment
3. WAN Unnumbered IP
```

- 6 Type the option corresponding to the IP address you want to use. The IAD displays the status of the DNS server assignment for the selected port, and prompts you to enable or disable it:
- 7 Type "E" to enable, or "D" to disable the DNS server assignment for T1/E1 on this port. The IAD reports the change, displays the status of the DNS server assignment for the port, and prompts you to enable or disable it:
- 8 Type "E" to enable, or "D" to disable the IP mask assignment for T1/E1 on this port. The IAD transfers the IP address and mask assigned to a WAN port to a LAN port and then displays the ATM Service Category Configuration menu (Figure 4.39).
- 9 Type "1" to select CBR for high priority data  
– or –  
Type "2" to select UBR for low priority data. The IAD displays the Peak Cell Rate Configuration menu (Figure 4.40).
- 10 Type the PCR value or press Enter to set the PCR to the maximum rate for the current line speed. The IAD saves the configuration and displays the ATM PVC Configuration menu.
- 11 Type "4" on the ATM Encapsulation Configuration (Figure 4.38) menu to select RFC 1483 encapsulation with VC Muxing or type "5" to select RFC 1483 with LLC encapsulation. The IAD displays the ATM Service Category Configuration menu (Figure 4.39).

- 12** Type "1" to select CBR for high-priority data.
- or -
- Type "2" to select UBR for low-priority data.
- or -
- Type "3" to select VBRnrt for low-priority data.
- or -
- Type "4" to select VBRrt for high-priority data.




---

**NOTICE:** *VBRrt is mapped to CBR and VBRnrt is mapped to UBR.; therefore, only the PCR values are used.*

---

- 13** Type the PCR value or press Enter to set the PCR to the maximum rate for the current line speed. The IAD saves the configuration and displays the ATM PVC Configuration menu (Figure 4.37).

**Modify Existing PVC**

- 1** Type "2" on the ATM PVC Configuration menu (Figure 4.37). The IAD displays the following port table, and prompts you to select the appropriate port.

Port	VPI	VCI	Encapsulation Type	PCR	Service
1	0	40	RFC 1483 (with LLC Encapsulation)	0	UBR
				<b>Total =</b>	<b>0 cps</b>
				<b>Maximum PCR this interface can support =</b>	<b>3622 cps</b>

Select Port: [1-8] \_

- 2** Type the port number and press Enter. The IAD prompts you to enter the VPI:
- 3** Type a VPI value between 0 and 255 (default 0) and press Enter. The IAD then prompts you to enter the VCI:
- 4** Type a VCI value between 32 and 65535 (the default is 38 for data and 39 for voice) and press Enter. The IAD displays the ATM Encapsulation Configuration menu (Figure 4.38).

Select the encapsulation you want to assign to this PVC in accordance with the following paragraphs.

**Delete PVC**

To delete a PVC, follow the steps below.

- 1** Type "3" on the ATM PVC Configuration menu (Figure 4.37) to select Delete PVC. The IAD displays the port list and a prompt.

- 2 Type the port number to delete and press Enter.
- 3 To delete the PVC, type "Y", or cancel the deletion by typing any other character. The IAD saves the configuration and displays the PVC Configuration menu where you may continue with other PVC management tasks.

### *Show Current PVCs*

- 1 To display a list of current PVCs, type "4" on the ATM PVC Configuration menu (Figure 4.37) to display the port table with associated PVCs:
- 2 When you have finished viewing the list, press any key to return to the ATM PVC Configuration menu.

## **Configure ATM Options**

To configure ATM options, type "4" on the WAN Configuration menu (ATM) to display the ATM Configuration menu (Figure 4.46). Current datalink protocol on the WAN Configuration menu must be set to ATM to see the ATM Configuration menu. Remember always to reset the IAD when you finish ATM configuration. (You may wait to reset until all changes have been made.)

**Figure 4.46** *ATM Configuration Menu*

```
*****
*           ATM Configuration Menu           *
*****
 1. Configure Payload Scrambling
 2. Configure F4 OAM UPI
 3. Configure F4 OAM Type
 4. Display F4 OAM Configuration
 5. Send OAM Loopback
 6. Configure EmptyCells
```

Each of the options on this menu is described in detail below.

### *Configure Payload Scrambling*

You must enable payload scrambling (which is disabled by default) for the IAD to connect to a DSLAM that uses payload scrambling. To enable or disable payload scrambling, follow the steps below:

- 1 On the ATM Configuration menu, type "1" to see a prompt that lets you enable or disable Payload Scrambling.
- 2 To enable payload scrambling type "E", or type "D" to disable. The IAD saves the configuration and displays the ATM Configuration menu where you may continue with other ATM tasks.

### **Configure F4 OAM VPI**

One F4 OAM VPI may be configured at a time. When you are configuring an F4 OAM VPI, if one is not configured, the IAD displays the message, "F4 OAM not configured"; otherwise the current configuration is displayed.

To configure the F4 OAM VPI, follow the steps below.

- 1** On the ATM Configuration menu (Figure 4.46), type "2" to select Configure F4 OAM VPI. This value must match one of the WAN PVCs. For more information, refer to *Show Current PVCs* on page 4-30. The IAD displays the status and prompts you to enter a VPI.
- 2** Type the VPI on which to configure F4 OAM. The IAD saves the configuration and displays the ATM Configuration menu where you may continue with other ATM tasks.

### **Configure F4 OAM Type**

To configure the F4 OAM Type, follow the steps below.

- 1** On the ATM Configuration menu (Figure 4.46), type "3" to select Configure F4 OAM Type. The IAD displays the menu shown in Figure 4.47.

**Figure 4.47** *F4 OAM Type Configuration Menu*

```
*****  
*           F4 OAM Type Configuration Menu           *  
*****  
0. None  
4. F4 End to end OAM
```

- 2** Type "0" to set F4 OAM to none, or type "4" to set for End to End OAM. The IAD saves the configuration and displays the ATM Configuration menu where you may continue with other ATM tasks.

### **Display F4 OAM Configuration**

To display the F4 OAM Type currently set, type "4" on the ATM Configuration menu (Figure 4.46). The IAD displays the status message, and then displays the ATM Configuration menu.

### **Send OAM Loopback**

- 1** Type "5" on the ATM Configuration menu (Figure 4.46) to select Send OAM Loopback. The IAD displays a list of all configured F4 OAM ports and VPI values.
- 2** Type the port on which to send the OAM Loopback and press Enter. The IAD performs a loopback test on the selected port and reports the results, whether successful or unsuccessful.
- 3** Press any key to display the ATM Configuration menu.

**Configure EmptyCells** To configure Empty Cells, follow the steps below.

- 1 Type "6" on the ATM Configuration menu (Figure 4.46), to select Configure EmptyCells. The IAD displays the current status ("Idle" or "Unassigned") and prompts you to change it.
- 2 Type "1" to select Idle cells, or type "2" to select Unassigned cells.




---

**NOTICE:** *Empty cell IAD settings must match far-end settings.*

---

## Configure DLCIs

Type "3" on the WAN Configuration menu to display the Frame Relay DLCI Configuration menu. Remember always to reset the IAD after you finish DLCI configuration.




---

**NOTICE:** *Before you configure DLCIs, you must first set the datalink protocol to Frame Relay. If option 3 on the WAN Configuration menu displays "Configure PVCs" instead of "Configure DLCIs," your datalink protocol is set to ATM instead of Frame Relay.*

---

**Figure 4.48** *Frame Relay DLCI Configuration Menu*

```
*****
*           FR DLCI Config Menu           *
*****
1. Add New DLCI
2. Modify Existing DLCI
3. Delete DLCI
4. Show Current DLCIs
```

Each option on the menu is described below.

**Add New DLCI** To add a new DLCI, follow the steps below.

- 1 On the Frame Relay DLCI Configuration menu, type "1" to select Add New DLCI. The IAD prompts you to enter a new DLCI number.
- 2 Type a DLCI value between 16 and 1023 and press Enter. The IAD displays the Frame Relay Encapsulation Configuration menu (Figure 4.49).

**Figure 4.49** *Frame Relay Encapsulation Configuration Menu*

```
*****
*   FR Encapsulation Configuration   *
*****

Current Encapsulation : ATM RFC 1483 (Tunneling)

1. RAW (No Encapsulation)
2. Proprietary Voice DLCI
3. RFC 1490
4. ATM RFC 1483 (Tunneling)
5. RFC 1973 (PPP over Frame Relay)
```



- 3 Type the option corresponding to the encapsulation method you intend to use. The IAD displays the Frame Relay DLCI Options menu (Figure 4.50).

**Figure 4.50** *Frame Relay DLCI Options Menu*

```
*****
*           FR DLCI Options           *
*****
1. Configure Transmit CIR
2. Configure Receive CIR
3. Configure FRF.12 Fragmentation
```




---

**NOTICE:** *To continue without configuring CIR or FRF.12 Fragmentation, press Escape. CIR is not required for full bandwidth circuits.*

---

**Configure Transmit CIR**

To configure Transmit CIR, follow the steps below.

- 1 Type "1" on the Frame Relay DLCI Options menu to select Configure Transmit CIR. The IAD prompts you to enter the Committed Burst Size (Bc).
- 2 Type the Bc in number of bits. The IAD prompts you to enter the Circuit Throughput.
- 3 Type the Circuit Throughput and press Enter. The IAD prompts you to enter the Excess Burst Size (Be).
- 4 Type the excess burst value in number of bits and press Enter. The IAD displays the Frame Relay DLCI Options menu (Figure 4.50).
- 5 Press Escape to return to the Frame Relay DLCI Config menu and continue, or proceed to the next section.

**Configure Receive CIR**

To configure Receive CIR, follow the steps below.

- 1 Type "2" on the Frame Relay DLCI Options (Figure 4.50) menu to select Configure Receive CIR. The IAD prompts you to enter the Bc.
- 2 Type the Bc in number of bits. The IAD prompts you to enter the Circuit Throughput.
- 3 Type the Circuit Throughput in bits per second and press Enter. The IAD prompts you to enter the Be.
- 4 Type the Be value in number of bits and press Enter. The IAD displays the FR DLCI Options menu.
- 5 Press Escape to return to the Frame Relay DLCI Configuration menu and continue.

**Configure FRF.12 Fragmentation**

To configure FRF.12 Fragmentation, follow the steps below.

- 1 Type "3" on the Frame Relay DLCI Options menu (Figure 4.50) to display the End-to-End Fragmentation menu (Figure 4.51).

**Figure 4.51** *End-to-End Fragmentation Configuration Menu*

```

*****
* End-to-End Fragmentation Configuration *
*****
1. Enable/Disable End-to-End FRF.12
2. Set Fragment Size
    
```

- 2 Type "1" to select End-to-End FRF.12, or type "2" to manually set the fragment size. If you type "1", the IAD displays the status and prompts you to enable or disable End-to-End FRF.12. If you type "2", the IAD prompts you to enter the maximum fragment size.
- 3 Type the fragment size in bytes and press Enter. The IAD displays the End-to-End Fragmentation Configuration menu. Press Escape to return to the DLCI Configuration menu.

**Modify Existing DLCI** To modify an Existing DLCI, follow the steps below.

- 1 On the Frame Relay DLCI Configuration menu, type "2" to select Modify Existing DLCI. The IAD displays the port table and prompts you to select the appropriate port as shown in

**Figure 4.52** *Modify Existing DLCI Menu*

Port	DLCI	Encapsulation
----	-----	-----
1	32	ATM RFC 1483 (Tunneling)

Select Port: [1-8]

- 2 Type the port number corresponding to the DLCI you want to update and press Enter.
- 3 Type the new DLCI number and press Enter. The IAD displays the Frame Relay Encapsulation Configuration menu as shown in Figure 4.49.
- 4 Continue with the steps listed above under "Adding a new DLCI."

**Delete DLCI** To delete a DLCI, follow the steps below.

- 1 On the Frame Relay DLCI Configuration menu, type "3" to select Delete DLCI. The IAD displays the port table and prompts you to select a port.
- 2 Type the port number corresponding to the DLCI you want to delete. To permanently remove the DLCI configuration, type "Y". To cancel the operation, type "N".

**Show Current DLCIs** To display all currently configured DLCIs, follow the steps below.

- 1 Type "4" on the Frame Relay DLCI Configuration menu to display the port table.
- 2 Press any key to display the Frame Relay DLCI Configuration menu.

## Configure Frame Relay Options

To configure Frame Relay options, type "4" on the WAN Configuration menu. The IAD displays the Frame Relay menu (Figure 4.53).

**Figure 4.53** *Frame Relay Options Configuration Menu*

```
*****
*           Frame Relay Options           *
*****
  1. Configure Fragmentation
  2. Configure Management Protocol
  3. Configure Congestion Parameters
  4. Enable/Disable Copper Mountain CMCP
  5. Configure Priority DLCI
```

Each of the menu options is described in detail below.

### *Configure Fragmentation*

- 1 On the Frame Relay Options menu, type "1" to display the Frame Relay Fragmentation Configuration menu (Figure 4.54).

**Figure 4.54** *Frame Relay Fragmentation Configuration Menu*

```
*****
*   FR Fragmentation Configuration   *
*****
  1. Configure FRF.12 Fragmentation
  2. Configure Copper Mountain Fragmentation
```

- 2 Type "1" to select Configure FRF.12 Fragmentation and proceed to FRF.12 configuration.  
– or –  
Type "2" to select Copper Mountain Fragmentation and proceed to CopperMountain Fragmentation configuration.

Each of these configurations is described below.

**Frame Relay FRF.12 Configuration** Select FRF.12 Fragmentation to display the FRF.12 Configuration menu (Figure 4.55).

**Figure 4.55** *FRF.12 Configuration Menu*

```
*****
*   FR FRF.12 Configuration   *
*****
  1. Enable/Disable FRF.12
  2. Enable Automatic Fragment Sizing
  3. Set Manual Fragment Size
```

Each option on this menu is described in detail below.

### **Enable/Disable FRF.12**

To enable or disable FRF.12, follow the steps below.

- 1 Type "1" on the Frame Relay FRF.12 Configuration menu. The IAD displays FRF.12 Fragmentation status (enabled or disabled), and prompts you to change it.
- 2 Type "E" to enable End-to-End fragmentation, or type "D" to disable it. The IAD saves the configuration and displays the FRF.12 Configuration menu. Press Escape to continue.

### Enable Automatic Fragment Sizing

Type "2" on the Frame Relay FRF.12 Configuration menu to enable automatic fragment sizing. The IAD saves the configuration and displays the FR FRF.12 Configuration menu. Press Escape to continue.

### Set Manual Fragment Size

To manually set the Fragment Size, follow the steps below.

- 1 Type "3" on the Frame Relay FRF.12 Configuration menu to manually set fragment sizing. The IAD prompts you to enter the maximum fragment size.
- 2 Type the maximum fragment size in milliseconds or bytes and press Enter. The IAD saves the configuration and displays the FR FRF.12 Configuration menu. Press Escape to continue.

### Configure CopperMountain Fragmentation Configuration

Select Configure CopperMountain Fragmentation by typing "2" on the FR Fragmentation Configuration menu to display the CopperMountain FR FRF.12 Configuration menu (Figure 4.56).




---

**NOTICE:** *With CMCP enabled, the DSLAM controls fragmentation settings, and IAD configuration is not required.*

---

**Figure 4.56** *Copper Mountain FRF.12 Configuration Menu Proprietary for CopperMountain DSLAMs*

```
*****
*           FR FRF.12 Configuration           *
*****
  1. Enable/Disable CuMtn Fragmentation
  2. Set Real-Time DLCI
```

Each option on this menu is described in detail below.

### Enable/Disable Copper Mountain Fragmentation

- 1 Type "1" to display a prompt that lets you enable or disable CopperMountain fragmentation.
- 2 Type "E" to enable CopperMountain fragmentation or type "D" to disable. The IAD saves the configuration and displays the FR FRF.12 Configuration menu. Press Escape to continue.

## Set Real-Time DLCI

- 1 Type "2" to set up the IAD for real-time DLCI. The IAD displays the port table and prompts you to select a port.
- 2 Type the port number corresponding to the DLCI you want to set to real-time. The IAD saves the configuration and displays the FR FRF.12 Configuration menu. Press Escape to continue.

## Configure Management Protocol

To configure Management Protocol, follow the steps below.

- 1 Type "2" on the Frame Relay Options menu to display the Configure Management Protocol menu (Figure 4.57).

**Figure 4.57** *Frame Relay Management Protocol Menu*

```
*****
*   Frame Relay Management Protocol   *
*****
 0. None
 1. CCITT Q.933 Annex A Network (DCE)
 2. CCITT Q.933 Annex A User (DTE)
 3. CCITT Q.933 Annex A Both (DTE + DCE)
 4. ANSI T1.617 Annex D Network (DCE)
 5. ANSI T1.617 Annex D User (DTE)
 6. ANSI T1.617 Annex D Both (DTE + DCE)
 7. LMI (FRF.1.1) Network (DCE)
 8. LMI (FRF.1.1) User (DTE)
 9. LMI (FRF.1.1) Both (DTE + DCE)
```

- 2 Type the number that corresponds to the protocol on your network and press Enter.

## Configure Congestion Parameters

To configure Congestion Parameters, follow the steps below.

- 1 Type "3" on the Frame Relay Options menu to display the Frame Relay Congestion Configuration menu (Figure 4.58).

**Figure 4.58** *Frame Relay Congestion Configuration Menu*

```
*****
*   FR Congestion Configuration     *
*****

 1. Configure Transmit Congestion Parameters
 2. Configure Receive Congestion Parameters
```

- 2 Select Configure Transmit Congestion Parameters and then follow the on-screen messages to
  - FECN/BECN condition set size

- FECN/BECN condition clear size
- FECN/BECN max number of bytes to store

– or –

Select Configure Receive Congestion Parameters and then follow the on-screen messages to

- FECN/BECN condition set size
- FECN/BECN condition clear size
- FECN/BECN max number of bytes to store

**4** Reset the IAD for changes to take effect.

### ***Enable/Disable CopperMountain CMCP***




---

**NOTICE:** *When using a CopperMountain DSLAM, CMCP allows the DSLAM to configure many IAD parameters automatically. IAD parameters controlled by CMCP include fragmentation and voice gateway support. For more information, refer the CopperMountain DSLAM guide.*

---

- 1** Type "4" on the Frame Relay Options menu. The IAD displays the CMCP status and prompts you to change it.
- 2** Type "E" to enable CopperMountain CMCP or "D" to disable.

### ***Configure Priority DLCI***

Type "5" on the Frame Relay Options menu to configure a DLCI's priority. The IAD prompts you to enter a new priority DLCI.

## **Router Configuration**

---

This section describes how to configure the IAD as a router. You may configure the IAD as a router or a bridge, depending on your application.

Optionally, you may also configure some ports for routing and some ports for bridging. For example, you might use a bridge connection for Internet traffic and use a separate routed port for remote management. Alternatively, you can configure the bridge port on the WAN side with IPoBridge to use the bridged connection for remote management. Refer to *Basic Bridge Setup Tasks* on page 4-53.

A router is a network layer device that uses one or more metrics to determine the optimal path along which network traffic should be forwarded. Routers forward packets from one network to another based on network layer information.

A router generally improves overall efficiency for a complex network, but a bridge provides better speed and flexibility for the overall network.



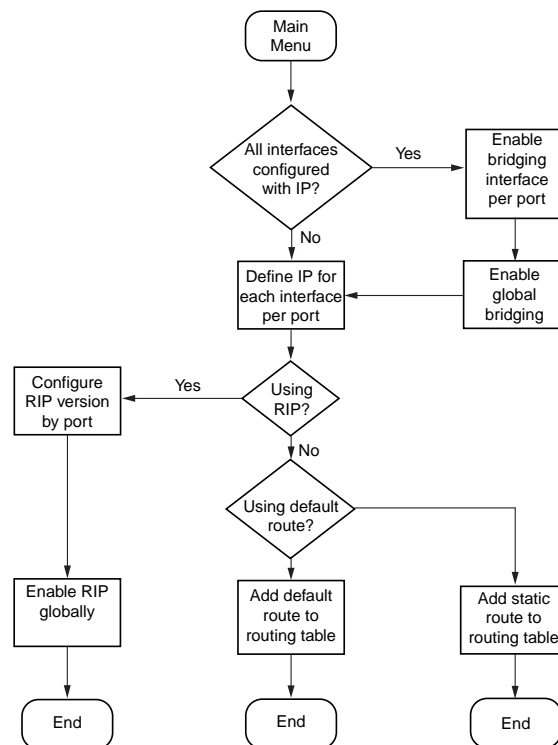
## Basic Router Setup Tasks

To configure the IAD as a router, complete the following tasks:

- Configure IP addresses on the LAN and WAN ports (page 4-40)
- Enable RIP poisoned reverse (recommended) (page 4-45), add a static route (page 4-42), or add a default route (page 4-43)
- Disable bridging globally (page 4-56) or by port (page 4-56)
- Disable Spanning Tree Protocol (Spanning Tree) globally (page 4-57) or by port (page 4-58)

Use the flowchart below to plan your tasks, based on your router configuration requirements.

**Figure 4.59** Router Configuration Task Flowchart



## Router Configuration Menu

Router tasks are all displayed and accessed on the Router Configuration menu (Figure 4.60) displayed by typing "2" on the Main menu (Figure 2.2). Remember always to reset the IAD (page 2-8) when you have finished router configuration for your changes to take effect.

Figure 4.60 Router Configuration Menu

```
*****
*      Router Configuration Menu      *
*****
C. Configure Port IP Address
U. Unconfigure Port IP Address
M. Configure Port Max Transmission Unit
S. Add/Remove a Static Route
R. Enable/Disable RIP
U. Configure RIP Version by Port
P. Configure RIP Poisoned Reverse by Port
N. Configure DNS Client
H. Configure DHCP Client
L. Configure DHCP Relay
T. Configure Telnet Server Port
A. Configure IP QoS
F. Configure IP Filtering
Q. Configure IP Header Compression
B. Configure LAN IP Broadcast Destination
G. Configure Domain Name
I. Configure Host Name
J. Remove Host and Domain Names
D. Display Route Table
```

You may sign on as Supervisor or Network Manager to configure the IAD as a router. Options that display in the Router Configuration menu are the same for both security levels.

## Configure Port IP Address

To configure the IAD as a router, you must assign an IP address to both the LAN and WAN ports, each with different subnet masks.



---

**NOTICE:** *You can assign up to eight IP addresses on each of the WAN and LAN ports.*

---

To configure an IP address, follow the steps below:

- 1 Type "C" on the Router Configuration menu (Figure 4.60) to select Configure Port IP address. The IAD displays the available interfaces. Type the number that corresponds with the interface you want to configure. (Sample shown below in Figure 4.61.)

Figure 4.61 Available Interfaces Display.

```
Available Interfaces :
  1. SDSL
  2. 10/100BaseT Ethernet
  0. (Abort)
Selection :
```

- 2 The IAD displays the port table for this interface and prompts for a port.



- 3** Type the port to configure and press Enter. The IAD displays the IP interfaces on the port you're configuring:
- 4** Enter the ID of the interface (0-7) to configure and press Enter. The IAD displays the current IP Address and prompts for a new one.
- 5** Type the new IP address and press Enter. The IAD displays the current Subnet Mask and prompts for a new one:
- 6** Type the new Subnet Mask address and press Enter. The IAD prompts you to determine traffic priority on this port:
- 7** Do one of the following:  
Set the interface to high priority to type "H"  
– or –  
Set the interface to normal priority to type "N"

Configuration is complete.

- 8** The IAD then prompts you to save the new information.
- 9** Type "Y" to confirm your changes, or press Escape to cancel. If you confirm, the IAD saves the settings. If bridging is enabled and an IP address is assigned on the WAN interface, the IAD displays an IP Over Bridge prompt.
- 10** Type "E" to enable IP Over Bridge on the WAN port, or "D" to disable it. The IAD saves the changes and displays the Router Configuration menu (Figure 4.60).
- 11** Repeat the steps listed above for each remaining port to configure.
- 12** Continue with other configuration tasks, or press Escape to return to the Main menu.
- 13** Reset the IAD when you finish router configuration.

## Unconfigure Port IP Address

To unconfigure a Port IP Address, follow the steps below.

- 1** Type "U" on the Router Configuration menu (Figure 4.60) to select Unconfigure Port IP Address. If more than one WAN port is installed or more than one PVC/DLCI exists, the IAD displays the interfaces on this IAD (sample shown in Figure 4.61).
- 2** Type the interface number to which the IP address is assigned. The IAD displays the port table for this interface and prompts you to select a port.
- 3** Type the port and press Enter. The IAD displays the IP interfaces on the port you've selected.
- 4** Enter the ID of the interface to delete and press Enter. The IAD deletes the IP address and saves the configuration.
- 5** Continue with other configuration tasks, or press Escape to return to the Router Configuration menu.

## Configure Port Maximum Transmission Unit (MTU)

The MTU setting controls IP fragmentation of packets transmitted through the specified port. Packet whose size is greater than the MTU value are fragmented to fit into the MTU size limit.

To set a maximum transmission unit value for a port, follow the steps below:

- 1 Type "M" on the Router Configuration menu (Figure 4.60) to select Configure Port Max Transmission Unit. The IAD displays the port table for this interface and prompts you to select a port.
- 2 Type the port number and press Enter. The IAD displays the current configuration and prompts you to change it.
- 3 Type the new MTU value (100-1500) and press Enter. (When set at 1500, IP fragmentation is disabled). The IAD saves the changes.
- 4 Continue with other configuration tasks, or press Escape to return to the Router Configuration menu.

For further information, refer to *Frame Relay Applications Notes* on page C-1.

## Add/Remove a Static or Source Route

To create, update, and/or delete static, source, and default routes, type "S" on the Router Configuration menu (Figure 4.60). The IAD displays the Router Modification menu, which contains commands to manage the IAD's route table:

**Figure 4.62** Router Modification Menu

```
*****  
*           Router Modification Menu           *  
*****  
  A. Add a Static Route  
  S. Add a Source Route  
  R. Remove a Route  
  F. Add/Change the Default Route  
  T. Remove the Default Route  
  D. Display Route Table
```

Each option on this menu is described in detail below.

**Add a Static Route** To add a Static Route, follow the steps below.

- 1 On the Router Modification menu type "A" to select Add a Static Route. The IAD prompts you to input the destination address:
- 2 Type the destination address to add and press Enter. The IAD displays the current subnet mask and prompts you to enter the network mask of the route.
- 3 Type the network mask and press Enter. The IAD prompts you for the gateway address.

- 4 Type the gateway address, press Enter. The static route is added. The IAD then asks if you want to save this route in the static configuration.
- 5 Type "Y" to confirm, or Escape to cancel. If you confirm, the Route Table is updated and the IAD prompts you to add more routes:
- 6 Type "Y" to add more routes, or Escape to cancel. Repeat these steps for each route that you want to add.
- 7 Continue with other configuration tasks, or press Escape to return to the Router Modification menu.

**Add a Source Route** To add a Source Route, follow the steps below.

- 1 On the Router Modification menu type "S" to select Add a Source Route. The IAD prompts you to input the destination address:
- 2 Type the destination address to add and press Enter. The IAD displays the current subnet mask and prompts you to enter the network mask of the route.
- 3 Type the network mask and press Enter. The IAD prompts you for the gateway address.
- 4 Type the gateway address, press Enter. The static route is added. The IAD then asks if you want to save this route in the source configuration.
- 5 Type "Y" to confirm, or Escape to cancel. If you confirm, the Route Table is updated and the IAD prompts you to add more routes:
- 6 Type "Y" to add more routes, or Escape to cancel. Repeat these steps for each route that you want to add.
- 7 Continue with other configuration tasks, or press Escape to return to the Router Modification menu.

**Remove a Route** To delete a static route from the Route Table, follow the steps below:

- 1 On the Router Modification menu, type "R" to select Remove a Route. The IAD prompts you to enter the address of the route to remove:
- 2 Type the IP address of the route to remove and press Enter. The IAD removes the route from the table and the IAD displays the Router Modification menu. Repeat these steps for each route that you want to remove.
- 3 Continue with other configuration tasks, or press Escape to return to the Main menu.

**Add or Change Default Route** To add or change a default route, follow the steps below.

- 1 On the Router Modification menu, type "F" to select Add/Change the Default Route. The IAD prompts you to enter the default gateway address. (You may type "0" for a list of interfaces):
- 2 Type the default gateway address and proceed to step 3 above or type "0" to display the port table.

- 3 Enter the number of the port and press Enter. The default route is set and the Route Table is will be updated when the IAD is reset.
- 4 Continue with other configuration tasks, or press Escape to return to the Router Modification menu.

**Remove Default Route** To remove a default route, follow the steps below.

- 1 On the Router Modification menu type "T" to select Remove the Default Route. The default route is immediately deleted and the Route Table is updated when the IAD is reset.
- 2 Continue with other configuration tasks, or press Escape to return to the Router Modification menu.

**Display Route Table** Type "D" on the Router Modification menu to display the Route Table.



---

**NOTICE:** *If no default route is configured on the IAD, the first PPP interface that completes negotiation will be assigned as the default interface. If multiple PPP interfaces are configured, this could result in the wrong interface being assigned as the default. This applies to PPP over HDLC, PPPoA, PPPoFR, and PPPoE.*

---

## Enable/Disable RIP

When you enable RIP, the IAD sends routing data to adjacent routers and dynamically learns the associated network topology. To enable RIP globally, follow the steps below.

- 1 Type "R" on the Router Configuration menu (Figure 4.60), to select Enable/Disable RIP. The IAD displays the RIP current status and prompts you to enable or disable RIP globally.
- 2 Type "E" to enable RIP globally, or "D" to disable it globally. The IAD saves the configuration and displays the Router Configuration menu (Figure 4.60).
- 3 Continue with other configuration tasks, or press Escape to return to the Main menu.



---

**NOTICE:** *For RIP to function correctly, you must enable RIP globally or locally (by port) and set the RIP version. The order in which you perform each procedure is irrelevant.*

---

## Configure RIP Version by Port

To configure RIP Version by Port, follow the steps below.

- 1 Type "V" on the Router Configuration menu (Figure 4.60) to select Configure RIP Version by Port. If more than one WAN port is installed or more than one PVC/DLCI exists, the IAD displays the interfaces on this IAD (sample shown in Figure 4.61).
- 2 Type the interface number to set. The IAD displays the port table for this interface and prompts you to select a port:

- 3 Type the port number to set and press Enter. The IAD displays the RIP configuration and status of the slot and port you're setting, and prompts you to select a new version:
- 4 Type the option number of the version to set. Setting the RIP version for this port is complete. The IAD saves the settings and displays the Router Configuration menu (Figure 4.60). Repeat these steps for each remaining port to set.
- 5 Continue with other configuration tasks, or press Escape to return to the Main menu.

## Configure RIP Poisoned Reverse by Port

To configure RIP Poisoned Reverse by port, follow the steps below.

- 1 Type "P" on the Router Configuration menu (Figure 4.60) to select Configure RIP Poisoned Reverse by Port. The IAD displays the interfaces on this IAD (sample shown in Figure 4.61)
- 2 Type the number of the port to enable or disable. The IAD displays the RIP status of this port and prompts you to enable or disable RIP Poisoned Reverse for that slot and port.
- 3 Type "E" to enable RIP Poisoned Reverse, or type "D" to disable it. The IAD saves the configuration, and displays the Router Configuration menu (Figure 4.60). Repeat these steps for each port for which you want to enable RIP poisoned reverse.
- 4 Continue with other configuration tasks, or press Escape to return to the Main menu.

## Configure DNS Client

DNS Client allows the IAD to use fully qualified domain names (for example, www.verilink.com). To configure the IAD as a DNS Client, type "N" on the Router Configuration menu (Figure 4.60). The IAD displays the DNS Client menu:

**Figure 4.63** *DNS Client Menu*

```
*****
*           DNS Client Menu           *
*****
  A. Set Primary DNS Server IP Address
  B. Set Secondary DNS Server IP Address
  T. Set DNS Server Timeout
  S. Display DNS Cache and Statistics
```

Each option on this menu is described in detail below.

### **Set Primary (or Secondary) DNS Server IP Address**

To set the Primary (or Secondary) DNS Server IP Address, follow the steps below.

- 1 On the DNS Client menu, type "A" to select Set DNS Server IP Address. The IAD displays the current address and prompts you to enter a new one.
- 2 Type the new DNS server address and press Enter. The IAD updates the configuration and displays the DNS Client menu.
- 3 Continue with other configuration tasks, or press Escape to return to the Router Modification menu.

**Set DNS Server Timeout** To set the DNS Server Timeout, follow the steps below.

- 1 On the DNS Client menu, type "T" to select Set DNS Server Timeout. The IAD displays the current value and lets you specify a new value.
- 2 Type the new timeout value (default 5) and press Enter. The IAD updates the configuration and displays the DNS Client menu.
- 3 Continue with other configuration tasks, or press Escape to return to the Router Modification menu.

**Display the DNS Cache and Statistics** To display information about the data in the DNS cache, type "S" on the DNS Client menu. When DNS Client is enabled, the IAD displays the information shown below.

```

IP Address      Timer Host Name
-----
0 Total Requests
0 Requests Serviced From Cache
0 Requests Sent to Server
0 Server Timeouts
0 Server Good Responses
0 Server Not Found Responses
0 Server Unexpected Responses
0 Errors Sending to Server

```

All DNS requests *except* SRV records are converted to HOSTENT structures. The IAD will cache a maximum of 10 records, which will remain cached until the shortest TTL in the record expires, *or* the least recently used record is deleted for a subsequent DNS request. Note the TTL values are supplied by the DNS server, *not* the IAD.

Press any key to return to the DNS Client menu when you have finished reviewing the information.

## Configure DHCP Client

- 1 Type "H" on the Router Configuration menu (Figure 4.60) to select Configure DHCP Client. If more than one WAN port is installed or more than one PVC or DLCI exists, the IAD displays the available interfaces (sample shown in Figure 4.61):
- 2 Type the interface number to set. The IAD displays the port table for this interface and prompts you for a port number.

- 3 Type the port to set and press Enter. The IAD displays the status of the selected slot and port, and prompts you to change it.
- 4 Type "E" to enable DHCP Client on this port, or "D" to disable it. The IAD saves the changes and displays the Router Configuration menu (Figure 4.60). Repeat these steps for each remaining port.
- 5 Continue with other configuration tasks, or press Escape to return to the Main menu.

## Configure DHCP Relay

DHCP Relay allows the IAD to forward DHCP requests from the LAN to a separate DHCP Server. To configure the IAD for DHCP Relay, type "L" on the Router Configuration menu (Figure 4.60). The IAD displays the DHCP Relay menu (Figure 4.64), which contains commands to configure DHCP Relay:

**Figure 4.64** *DHCP Relay Menu*

```
*****
*           DHCP Relay Menu           *
*****
  E. Enable/Disable DHCP Relay
  C. Configure DHCP Relay
  S. Display DHCP Relay Statistics
```

Each option on this menu is described in detail below.

**Enable/Disable DHCP Relay** When you enable DHCP Relay, you must provide a DHCP server IP address. To enable or disable DHCP Relay, follow the steps below:

- 1 On the DHCP Relay menu, type "E" to select Enable/Disable DHCP Relay. The IAD displays the current status and prompts you to change it.
- 2 Type "E" to enable DHCP Relay on this port, or "D" to disable it.
- 3 The IAD displays the current DHCP server IP address and prompts you to enter a new address.
- 4 Type the new DHCP Server IP address. The IAD saves the changes and displays the Router Configuration menu (Figure 4.60).
- 5 Continue with other configuration tasks, or press Escape to return to the Main menu.

**Configure DHCP Relay** To configure the DHCP Relay, follow the steps below.

- 1 On the DHCP Relay menu, type "C". The IAD displays the current IP address and prompts you to enter a new address.
- 2 Type the new DHCP Server IP address. The IAD saves the changes and displays the Router Configuration menu (Figure 4.60).
- 3 Continue with other configuration tasks, or press Escape to return to the Router Modification menu.

**Display DHCP Relay Statistics** To display information about DHCP, follow the steps below.

- 1 Type "S" on the DHCP Relay menu (Figure 4.64). When DHCP Relay is enabled, the IAD displays a report such as the one below.  

```
0 Client requests forwarded to DHCP server
0 Client requests dropped
0 Server responses forwarded to DHCP clients
0 Server responses dropped
0 Unknown server responses
0 Server requests timed out
```
- 2 Press any key to return to the DNS Client menu when you have finished reviewing the information.

## Configure Telnet Server Port

When using NAT on the IAD, you may want to configure a host behind NAT as a Telnet Server. In this case, Telnet requests are passed to the host, and not handled by the IAD. By changing the Telnet port, both the host and IAD may be accessed via Telnet.

To set the port for the Telnet Server, follow the steps below.

- 1 On the Router Configuration menu (Figure 4.60), type "T" to select Configure Telnet Server Port. The IAD displays the current IP address and prompts you to enter the new Telnet Server port.
- 2 Type the new Telnet Server port (the default is 23). The IAD saves the changes and displays the Router Configuration menu (Figure 4.60).
- 3 Continue with other configuration tasks, or press Escape to return to the Main menu.

## Configure IP QoS

Type "A" on the Router Configuration menu to select the Configure IP QoS menu.

**Figure 4.65** *IP QoS Menu*

```
*****
*                IP Qos Menu                *
*****
  D. Display QoS Settings
  C. Config QoS
```

**Display QoS Settings** Type "D" on the IP QoS menu to display the priority of the type of service (ToS) value. Use this field to create priorities for packets in the IAD. Figure 4.66 shows the default settings.



Figure 4.66 IP QoS Based on ToS Values (Default Settings)

IP QoS based on TOS values:

ToS	Priority
7	Highest
6	Highest
5	High
4	High
3	Normal
2	Normal
1	Low
0	Low

**Config QoS** Type "C" on the IP QoS menu to configure the priority level of a service. The priority level is 1 – 3 and is set in accordance with the ToS value.

### Configure IP Filtering

IP Filtering lets you specify rules for handling data packets transitioning an interface. Based on a set of rules, packets can be passed or blocked when entering or leaving an interface.

IP Filtering is one part of creating a Firewall to protect local networks from undesirable access.



---

**NOTICE:** Please refer to the Applications Notes on IP Filtering found in Appendix C for the general information and syntax needed to program the filter.

---



---

**NOTICE:** Because each packet must be tested against one or more filters, IP filtering may significantly affect IAD performance.

---

To use IP filtering, you must create a text file called *filter.st*. This file should be created and edited external to the IAD and then downloaded via TFTP or XMODEM. The syntax is defined under the Grammar section on page page C-7. To configure IP Filtering, Type "F" on the Router Configuration menu (Figure 4.60). The IAD displays the IP Filtering Configuration menu.

Figure 4.67 IP Filtering Configuration Menu

```
*****
*   IP Filtering Configuration Menu   *
*****
 1. read filter.st
 2. print filters
 3. unload all filters
 S. Show IP Filtering statistics
 F. Show per filter statistics
 2. Clear IP filtering statistics
```

If the *filter.st* file is present on the IAD, IP Filtering will be enabled. The IP Filtering Configuration Menu then lets you load and unload rule sets, print the current list of filters, and show and clear IP Filter Statistics.

Each option on the above menu is described in detail below.

**read filter.st** Type "1" to have the IAD load a new rule set from the *filter.st* file. Once you have uploaded the file, the IAD will begin filtering without your having to reboot the IAD. To upload a file to the file system, refer to *File System Menu* on page 3-18.

**print filters** Type "2" to display a list of currently installed input and output filters (Figure 4.68).

**Figure 4.68** *Display Input/Output Filters Menu*

#### Input Filters

```
0. block in on atm0 proto tcp from any to any port >= 8000
```

Press any key to continue...

#### Output Filters

```
0. block out on atm0 proto udp from 20.0.0.1/32 to any port >= 8000
```

**unload all filters** Temporarily deactivates IP Filtering.



---

**NOTICE:** *You must unload the old rule set before loading a new rule set.*

---

**Show IP Filtering statistics** Displays statistics for IP Filtering. Shows accumulated statistics for all Input and Output filters

**Show per filter statistics** Displays statistics for each active filter rule.

**Clear IP filtering statistics** Clears all accumulated statistics.

### Configure IP Header Compression (IPHC)

IPHC reduces the number of bytes transmitted across the WAN, thus conserving bandwidth.

To enable or disable IP header compression, follow the steps below:

- 1 On the Router Configuration menu (Figure 4.60), type "Q".
- 2 The IAD displays the port table and prompts you to enter a port.

- 3 Type the port number and press Enter. The IAD displays the header compression status and prompts you to enable or disable IP Header Compression for SDSL.
- 4 Type "E" to enable IP header compression on this port, or "D" to disable it. If you enable IP header compression, the IAD displays a message similar to the following:

```
Springtide Compatibility mode ENABLED (currently not
selectable)
```

The IAD saves the changes and displays the Router Configuration menu (Figure 4.60). Continue with other configuration tasks, or press Escape to return to the Main menu.

## Configure LAN IP Broadcast Destination

To set the LAN IP broadcast destination address (where all broadcast IP packets received on the LAN ports will be redirected), follow the steps below.

- 1 On the Router Configuration menu (Figure 4.60), type "B".
- 2 The IAD displays the current LAN IP broadcast destination address and prompts you to enter a new address.
- 3 Type the new IP address. The IAD saves the changes and displays the Router Configuration menu (Figure 4.60).
- 4 Continue with other configuration tasks, or press Escape to return to the Main menu.

## Configure Domain Name

To configure the Domain Name, follow the steps below.

- 1 On the Router Configuration menu (Figure 4.60), type "G".
- 2 The IAD displays the current Domain Name and prompts you to enter a new one.
- 3 Continue with other configuration tasks, or press Escape to return to the Main menu.

## Configure Host Name

To configure the Host Name, follow the steps below:

- 1 On the Router Configuration menu (Figure 4.60), type "I".
- 2 The IAD displays the current Host Name and prompts you to enter a new one.
- 3 Continue with other configuration tasks, or press Escape to return to the Main menu.

## Remove Host and Domain Names

To remove the Host and Domain Names, type “J” on the Router Configuration menu (Figure 4.60).

## Display Route Table

To display the Route table and view information about statically configured routes and dynamically learned ones, type “D” on the Router Configuration menu (Figure 4.60).

The IAD displays each network address and related information:

```

NETWORK DESTINATION    NETMASK    GATEWAY ADDRESS    INTERFACE    Metric    Type
*****
192.94.45.128          255.255.255.128  192.94.45.187     192.94.45.187    1         local
192.94.45.187          255.255.255.255  192.94.45.187     192.94.45.187    1         local
127.0.0.1              255.0.0.0        127.0.0.1         127.0.0.1        1         local
0.0.0.0                0.0.0.0          192.94.45.129     192.94.45.187    1         default
    
```

```

NETWORK SOURCE        NETMASK
*****
                                INTERFACE    Metric    Type
*****
    
```

```

Default Gateway : 192.94.45.129
Default Interface : 192.94.45.187
    
```

Route Table parameters are described in the following table.

Parameter	Description
Network Destination	network destination address
Netmask	IP subnet mask; number of bits reserved for the host ID
Gateway Address	IP address of packets sent to destination
Interface	IP address of outgoing interface
Metric	number of hops (routers) required to reach the specified gateway
Type	static   dynamic   RIP   local

## Bridge Configuration

This section describes how to configure the IAD as a bridge. A bridge is a device that connects and passes packets between two network segments that use the same communications protocol. A router generally improves overall efficiency for a complex network, but a bridge provides better speed and flexibility for the overall network.



---

**NOTICE:** *Verilink recommends that bridged network architecture be thoroughly understood prior to configuring the IAD. Suggested reading: “Interconnections: Bridges and Routers” by Radia Perlman, Addison-Wesley, 1992.*

---

Bridges operate at the data link layer (Layer 2) of the OSI reference model. In general, a bridge filters, forwards, or floods an incoming frame based on the MAC address of that frame.

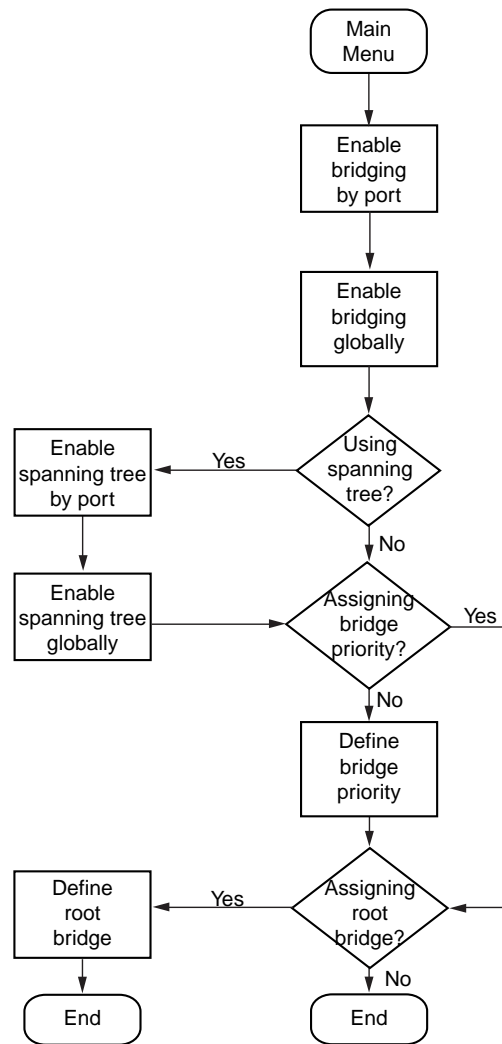
## Basic Bridge Setup Tasks

Although the IAD is preconfigured with bridging enabled, you should perform these tasks for your network:

- Enable bridging globally (page 4-56) or by port (page 4-56)
- Set the bridge aging timer (page 4-57)
- Disable RIP poisoned reverse globally (page 4-45) or by port (page 4-45)
- Enable Spanning Tree globally (page 4-57) or by port (page 4-58)

Use the flowchart below to plan your tasks, based on your requirements.

Figure 4.69 Bridge Configuration Task Flowchart



## Bridge Configuration Menu

Configuring the IAD as a bridge involves several tasks, all of which are displayed and accessed on the Bridge Configuration menu, displayed by typing "3" on the Main menu (Figure 2.2).

Figure 4.70 Bridge Configuration Menu

```
*****  
*           Bridge Configuration Menu           *  
*****  
G. Enable/Disable Bridging Globally  
P. Enable/Disable Bridging by Port  
A. Configure Bridge Aging Timer  
  
T. Enable/Disable Spanning Tree Globally  
O. Enable/Disable Spanning Tree by Port  
R. Configure Spanning Tree Bridge Priority  
Q. Configure Spanning Tree Port Priority  
H. Configure Spanning Tree Hello Time  
S. Configure Spanning Tree Max Age  
F. Configure Spanning Tree Forward Delay  
C. Configure Spanning Tree Path Cost  
  
D. Delete Bridge Forwarding Database Entry
```

You may sign on as Supervisor or Network Manager to configure the IAD as a bridge. Options that display in the Bridge Configuration menu are the same for both security levels.



---

**NOTICE:** *Be sure to reset the IAD when you have finished making changes to Bridge configuration. Resetting the IAD causes the configuration changes to take effect.*

---

## Enabling and Disabling Bridging

For bridging to function correctly, you must enable bridging by port and then set the bridge aging timer. At least two ports must be enabled for bridging to function. You must also disable RIP poisoned reverse. The order in which you perform the procedures is irrelevant.

To enable routing globally, you must disable bridging globally. However, you may enable routing on some ports and bridging on others, depending on your requirements.



---

**NOTICE:** *When bridging is disabled globally or on an interface (port) or an IP address is unconfigured, IP Over Bridge is disabled automatically.*

---

## IP Over Bridging

IP Over Bridging is intended for use when the IAD is in full bridged mode, and remote access (Telnet) and/or user authentication (RADIUS) are required.

To implement IP Over Bridging, enable bridging globally and by port (as described in the paragraphs below) on the WAN connection (at least one DLCI/PVC must be configured), and assign an IP address to the WAN interface. When these conditions have been met (either in Routing or Bridging configuration), the IAD will prompt you to enable or disable IP Over Bridging. When the IP address is unconfigured, IP Over Bridging is disabled

automatically. The IAD will also prompt you to enable or disable IP Over Bridging when bridging is being enabled on an interface that already has an IP address assigned.

When an IP address is unconfigured or when bridging is disabled globally or on an interface (port), IP Over Bridging is disabled automatically.

When IP Over Bridging is enabled, the IAD examines all Ethernet packets that have its MAC address as a destination. The ARP packets and IP packets with a destination IP address that is assigned to an interface on the IAD are processed as IP packets normally are, including ARP resolution. All other packets are processed in the usual way that a bridge processes them.

When the IAD should send an IP packet out (for example, in response to a ping, or RADIUS authentication), the ARP resolution is performed in a manner similar to the way it's accomplished on Ethernet. If the destination Mac address is not known, the ARP broadcast request is sent to all interfaces. The interface that receives the reply is used to send the actual IP packet.



---

**NOTICE:** *When using IP Over Bridging with CopperMountain HDIA or CopperVPN, the default route for the IP interface should be specified using the IP address of the router, rather than a WAN port number.*

---

## Enable/Disable Bridging Globally

To enable or disable bridging globally, follow the steps below.

- 1 On the Bridge Configuration menu (Figure 4.70), type "G" to display the status of bridging and a prompt to enable or disable Bridging globally.
- 2 Type "E" to enable bridging globally, or "D" to disable it globally. The IAD saves the configuration and displays the Bridge Configuration menu (Figure 4.70).
- 3 Continue with other configuration tasks, or press Escape to return to the Bridge Configuration menu.

## Enable/Disable Bridging by Port

To enable or disable bridging by port, follow the steps below:

- 1 Type "P" on the Bridge Configuration (Figure 4.70) menu to select Enable/Disable Bridging by Port. The IAD displays the interfaces available on this IAD as shown in Figure 4.61.
- 2 Type the number of the interface for which you want to enable bridging. The IAD displays a port table and prompts you to select the port.
- 3 Type the number of the port. The IAD displays the status of bridging on this interface and port, and prompts you to enable or disable it.
- 4 Type "E" to enable bridging on this port, or "D" to disable it. The IAD updates the configuration and displays the Bridge Configuration menu (Figure 4.70).



- 5 Type "Y" to confirm your changes, or press Escape to cancel. If you confirm, the IAD saves the settings. If bridging is enabled and an IP address is assigned on the WAN interface, the IAD displays the IP Over Bridge prompt, which asks if you wish to enable or disable IP Over Bridge on the WAN port.
- 6 Type "E" to enable IP Over Bridge on the WAN port, or "D" to disable it. The IAD updates the configuration and displays the Bridge Configuration menu (Figure 4.70).
- 7 Repeat these steps for each port on which you want to enable or disable bridging.
- 8 Continue with other configuration tasks, or press Escape to return to the Bridge Configuration menu.

## Bridge Aging Timer

The bridge aging timer establishes the amount of time the IAD keeps a MAC address in the bridging table. When the timer expires, the IAD deletes the address from the database.

To set the bridge aging timer, follow the steps below.

- 1 Type "A" on the Bridge Configuration menu (Figure 4.70) to select Configure Bridge Aging Timer. The IAD prompts you to enter the Bridge Aging Time.
- 2 Type the aging time (range 1 to 3600 seconds) and press Enter. The IAD updates the timer. Press any key to display the Bridge Configuration menu (Figure 4.70).
- 3 Continue with other configuration tasks, or press Escape to return to the Bridge Configuration menu.

## Enabling and Disabling Spanning Tree

A network that has many bridges creates the potential for network loops. A loop presents conflicting information about the segment on which a specific address is located and forces the bridge to forward all data.

When configuring the IAD as a router, you must disable Spanning Tree both globally and by port.



---

**NOTICE:** *When you enable Spanning Tree, the IAD reconfigures the bridge network to transfer data along an optimum route to its destination.*

---

## Enable/Disable Spanning Tree Globally

To enable or disable Spanning Tree globally, follow the steps below.

- 1 On the Bridge Configuration menu (Figure 4.70), type "T" to select Enable/Disable Spanning Tree Globally. The IAD displays the status of bridging and prompts you to disable or enable it.

- 2 Type "E" to enable spanning tree globally, or "D" to disable it globally. The IAD saves, then displays the Bridge Configuration menu.
- 3 Continue with other tasks, or press Escape to return to the Main menu.

### **Enable/Disable Spanning Tree by Port**

To enable or disable Spanning Tree by port, follow the steps below.

- 1 On the Bridge Configuration menu (Figure 4.70), type "O" to select Enable/Disable Spanning Tree by Port. The IAD displays the interfaces available on this IAD as shown in Figure 4.61
- 2 Type the number of the interface for which you want to enable Spanning Tree. The IAD displays a port table. If more than one interface is configured on the selected port, the IAD displays a list of interfaces.
- 3 Type the number of the port. The IAD displays the status of this interface and port and prompts you to enable or disable Spanning tree for that interface and port.
- 4 Type "E" to enable Spanning Tree on this port, or "D" to disable it. The IAD saves the new configuration then displays the Bridge Configuration (Figure 4.70) menu.
- 5 Repeat these steps for each port you want to enable or disable Spanning Tree.

### **Configure Spanning Tree Bridge Priority**

The Spanning Tree algorithm selects the bridge with the lowest priority on the network as the Root Bridge.

To set the Spanning Tree bridge priority (a value between 1 and 65,565 – default 32,768), follow the steps below.

- 1 Type "R" on the Bridge Configuration menu to select Configure Spanning Tree Bridge Priority. The IAD displays a prompt for you to enter the priority.
- 2 Type the priority and press Enter. The IAD updates the configuration.
- 3 Press any key to display the Bridge Configuration menu (Figure 4.70).
- 4 Continue with other configuration tasks or Escape to return to the Main menu.

### **Configure Spanning Tree Port Priority**

The spanning tree algorithm uses the spanning tree bridge priority to determine which bridge to use as the Ethernet LAN destination when two or more bridges are bridging between the same LAN.

To set the Spanning Tree priority by port (range 0 to 255 – default 128, the lower the value, the higher the priority), follow the steps below.

- 1 On the Bridge Configuration menu (Figure 4.70), type "Q" to select Configure Spanning Tree Port Priority. The IAD displays the interfaces available on this IAD as shown in Figure 4.61
- 2 Type the number of the interface for which you want to set the priority. The IAD displays a port table. If more than one interface is configured on the selected port, the IAD displays a list of interfaces:
- 3 Type the number of the port. The IAD prompts you to enter a priority for the selected Slot and Port.
- 4 Type the priority value and press Enter. The IAD updates the configuration and displays the Bridge Configuration menu.
- 5 Repeat these steps for each port on which you want to set the priority.
- 6 Continue with other configuration tasks, or press Escape to return to the Bridge Configuration menu.

### **Configure Spanning Tree Hello Time**

To set the Spanning Tree hello time (a value between 1 and 10 seconds—default 2), follow the steps below:

- 1 Type "H" on the Bridge Configuration menu (Figure 4.70) to select Configure Spanning Tree Hello Time. The IAD prompts you to enter the Bridge Hello Time.
- 2 Type the value and press Enter. The IAD updates the configuration.
- 3 Press any key to return to the Bridge Configuration menu and continue with other configuration tasks.

### **Configure Spanning Tree Maximum Age**

To set the Spanning Tree maximum age, (a value between 6-40 seconds—default 20), follow the steps below.

- 1 Type "S" on the Bridge Configuration menu (Figure 4.70) to select Configure Spanning Tree Max Age. The IAD prompts you to enter the Spanning Tree Max Age.
- 2 Type the maximum age value and press Enter. The IAD updates the configuration.
- 3 Press any key to return to the Bridge Configuration menu and continue with other configuration tasks.

### **Configure Spanning Tree Forward Delay**

To set the Spanning Tree forward delay (a value between 4-30 seconds—default 15), follow the steps below.

- 1 Type "F" on the Bridge Configuration menu (Figure 4.70) to select Configure Spanning Tree Forward Delay. The IAD prompts you to enter the Spanning Tree Forward Delay.

- 2 Type the forward delay value and press Enter. The IAD updates the configuration.
- 3 Press any key to return to the Bridge Configuration menu and continue with other configuration tasks.

## Configure Spanning Tree Path Cost

When there are multiple paths to the Root Bridge, the Spanning Tree algorithm selects the port with the lowest total path cost as the route port.

To set the Spanning Tree path cost (a value between 1 and 65,535—default 32,768), follow the steps below.

- 1 Type "C" on the Bridge Configuration menu to select Configure Spanning Tree Path Cost. The IAD displays the interfaces available on this IAD as shown in Figure 4.61.
- 2 Type the interface number. The IAD displays a port table. If more than one interface is configured on the selected port, the IAD displays a list of interfaces:
- 3 Type the number of the port. The IAD displays the current setting and prompts you to enter the Path Cost for the selected Slot and Port.
- 4 Type the path cost value and press Enter. The IAD updates the configuration.
- 5 Press any key to return to the Bridge Configuration menu and continue with other configuration tasks.

## Delete Bridge Forwarding Database Entry

To delete an Ethernet address from the bridge forwarding database, follow the steps below.

- 1 Type "D" on the Bridge Configuration menu (Figure 4.70) to select Delete Bridge Forwarding Database Entry. The IAD prompts you to enter the Ethernet address.
- 2 Type the MAC address of the Ethernet port and press Enter. The IAD deletes the database entry and updates the configuration.
- 3 Press any key to return to the Bridge Configuration menu and continue with other configuration tasks.

## Voice Path Configuration

---

After you have defined the voice PVCs or DLCIs on the IAD, configure the voice path for voice operation.



---

**NOTICE:** *When the IAD prompts you for input, the current value is displayed in parentheses. To conveniently accept the current value, just press Enter.*

---

## Basic Voice Path Setup Tasks

To configure voice path settings, you should complete the following tasks:

- Set a voice gateway (page 4-61)
- Set the jitter delay (page 4-77)
- Select country mode (page 4-83)
- Select DuSlic mode (page 4-83)
- Configure voice gateway options (page 4-61)



---

**NOTICE:** *You must reset the IAD for configuration changes to take effect.*

---

## Voice Configuration Menu

Configuring the voice path settings involves several tasks. These are all displayed and accessed on the Voice Configuration menu, displayed by typing "P" on the Main menu (Figure 2.2). Remember always to reset the IAD when you have finished voice configuration for your changes to take effect.

**Figure 4.71** *Voice Configuration Menu*

```
*****  
*           Voice Configuration           *  
*****  
  U. Set Voice Gateway  
  J. Setup Jitter Buffer  
  P. Voice Port Settings  
  U. Display Compander Mode (u-Law, A-Law)  
  C. Set Country Mode  
  S. Set DuSLIC Mode  
  G. Enable/Disable G726 Annex A
```



---

**NOTICE:** *You must sign on as Supervisor to configure voice path settings. Be sure to reset the IAD when you are done making changes to the voice path settings. Resetting the IAD causes the configuration changes to take effect.*

---

## Set Voice Gateway

To select a voice gateway, type "V" on the Voice Configuration menu. The IAD displays the Voice Gateway Selection menu, which contains a list of valid voice gateways for this IAD.



---

**NOTICE:** *Figure 4.72 displays the list of valid gateways. Only the "s" versions support MGCP and SIP.*

---

**Figure 4.72** *Voice Gateway Selection (SIP)*

```
*****
*           Voice Gateway Selection           *
*****

Current Voice Gateway is SIP 1.0

0. No Voice Gateway
1. AAL2/LES CAS
2. Jetstream
3. CopperCom
4. AAL2/LES CCS-ELCP
5. MGCP 1.0
6. SIP 1.0
```



---

**NOTICE:** *After you have selected the voice gateway, power cycle the IAD. The menus below will then become available on the Main menu and will be shown as the last available option at the bottom of the menu.*

---

### **AAL2/LES CAS**

ATM Adaptation Layer 2/Loop Emulation Services (AAL2/LES) is a broadband local loop emulation service (specifically telephony) that uses the ATM AAL2 adaptation layer.

When the voice gateway is specified as AAL2/LES CAS (af-vmoa-0145), type "E" on the Main menu (Figure 2.2) to display the AAL2/LES Call Control menu (Figure 4.73). The AAL2 parameters must match those of the voice gateway.

**Figure 4.73** *AAL2/LES Call Control Menu*

```
*****
*           AAL2/LES Call Control           *
*****

C. Configuration
D. Debug Control
S. Statistics
```

Each of the options on this menu is described in detail below.

### **Configuration**

Type "C" on the AAL2/LES Call Control menu to display the AAL2/LES Configuration menu.

**Figure 4.74** *AAL2/LES Configuration Menu*

```
AAL2/LES is MANUALLY configured.

Port Control (bit mapping) is 0x00000000

CAS signaling is GR303-ABCD.
CAS refreshing is DISABLED.
Idle CAS refreshing is DISABLED.

Max. CPS-SDU size is 0 octets.

"Combined use" timer is 0 millisecond(s).

User state control (USC) is DISABLED.

Dialled digit (outband) is DISABLED.

C. -MANUAL- Configuration
A. Accelerated Networks
L. Lucent
G. General Bandwidth
M. MetaSwitch
Z. Zhone
```

To configure the IAD for a specific AAL2/LES gateway, type the option corresponding with one of the gateways listed in the AAL2/LES Configuration menu. The IAD configures the voice gateway for the selected gateway and displays the AAL2/LES Manual Configuration menu. Included in the settings is a message indicating the IAD will be configured for the selected gateway after reset.

**Manual Configuration**

Type "C" on the AAL2/LES Configuration menu to display the AAL2/LES Manual Configuration menu (current settings eliminated from this example):

**Figure 4.75** *AAL2/LES Manual Configuration Menu*

```
AAL2/LES is MANUALLY configured.

Port Control (bit mapping) is 0x00000000

CAS signaling is GR303-ABCD.
CAS refreshing is DISABLED.
Idle CAS refreshing is DISABLED.

Max. CPS-SDU size is 0 octets.

"Combined use" timer is 0 millisecond(s).

User state control (USC) is DISABLED.

Dialled digit (outband) is DISABLED.
```

Each of the options on this menu is described in detail below.

### ***Enable/Disable Ports***

- 1** Type "P" on the AAL2/LES Manual Configuration menu to enable and disable ports.
- 2** Enter a zero (0) in each port location to disable the port; enter a 1 in each port location to enable the port. Press Enter to complete the step. The IAD displays the AAL2/LES Manual Configuration menu.

### ***Set CAS Refreshing Rate***

- 1** Type "R" on the AAL2/LES Manual Configuration menu to set the CAS refresh rate.
- 2** Enter a zero ("0") to disable CAS refresh, or enable CAS refresh by entering a non-zero refresh rate value. The IAD displays the AAL2/LES Manual Configuration menu.
- 3** Reset the IAD before enabling Idle CAS refresh.

### ***Enable/Disable Idle CAS Refreshing***

- 1** Type "I" on the AAL2/LES Manual Configuration menu to enable or disable idle CAS refreshing. You can only enable idle CAS refresh when CAS refresh is enabled (immediately preceding).
- 2** Type "E" to enable Idle CAS refresh, or D to disable Idle CAS refresh. The IAD displays the AAL2/LES Manual Configuration menu, and indicates in the message section that the change in the Idle CAS refresh will take place when the IAD is reset.

### ***Change Maximum CPS-SDU Size; 45/64 Octets***

Type "S" on the AAL2/LES Manual Configuration menu to switch the maximum CPS payload size between 45 and 64 octets. The IAD displays the AAL2/LES Manual Configuration menu. Included in the settings is a payload size message indicating 45 or 64 octets.

### ***Set "Combine Use" Timer***

- 1** Type "T" on the AAL2/LES Manual Configuration menu to modify the combined use timer (in 5 ms increments).
- 2** Type the new timer period and press Enter. The IAD updates the setting and displays the menu.

### ***Enable/Disable User State Control***

Type "U" on the AAL2/LES Manual Configuration menu to enable or disable user state control by toggling the state. The IAD displays the AAL2/LES Manual Configuration menu. Included in the settings is a USC message indicating that it is enabled or disabled.



### ***Enable/Disable Dialed Digit***

- 1 Type "E" on the AAL2/LES Manual Configuration menu to enable or disable dialed digit by toggling the state. The IAD displays the AAL2/LES Manual Configuration menu. Included in the settings is a message indicating that dialed digit will be enabled or disabled after reset.

### ***Manual ATM Pace Control***

Type "A" to set ATM Pace Control manually.

**Figure 4.76** *Manual ATM Pace Control Menu*

```
*****
*           Manual ATM Pace Control           *
*****

Manual ATM pace control is disabled
Audio bit rate margin is 0%
Minimum signaling bit rate is 0bps

P. Manual ATM Pace Control
A. Audio Bit Rate Margin
M. Minimum Signaling Bit Rate
```

Ensure that you have set the IAD configuration parameters to match those of the voice gateway. Each option on this menu is described in detail below.

### **Manual ATM Pace Control**

- 1 Type "P" on the Manual ATM Pace Control menu to enable or disable pace control.
- 2 Type "E" to enable pace control, or "D" to disable pace control.

### **Audio Bit Rate Margin**

- 1 Type "A" on the Manual ATM Pace Control menu to set the audio bit rate margin.
- 2 Enter the new bit rate margin (0 to 50) and press Enter. (Zero (0) implements automatic audio bit rate.)

### **Set Minimum Signaling Bit Rate**

- 1 Type "M" on the Manual ATM Pace Control menu to set the audio bit rate margin.
- 2 Enter the new bit rate margin and press Enter.

### ***Statistics***

Type "S" on the AAL2/LES Call Control menu to display the AAL2/LES Statistics menu:

Figure 4.77 AAL2/LES Statistics Menu

```

*****
*           AAL2/LES Statistics           *
*****

D. Display Audio/CAS/Alarm Statistics
C. Clear Statistics

ESC to return to previous menu

->d

<<< Audio, CAS and Alarm Statistics >>>

----- Tx ----- Rx -----
Line   Audio   CAS   Dropped   Alarm   Audio   CAS   Dropped   Alarm
-----


```

Each option on this menu is described in detail below.

- Display Audio/CAS/Alarm Statistics**
  - 1 Type "D" on the AAL2/LES Statistics menu to display transmitted and received audio, CAS, dropped, and alarm statistics by line.
  - 2 Press Escape to return to the menu, or any other key to refresh the statistics and display the table.
- Clear Statistics** Type "C" on the AAL2/LES Statistics menu to clear all statistics. The IAD resets the values to zero and displays the menu.

**JetStream**

When you have specified the JetStream Voice Gateway, type "E" on the Main menu (Figure 2.2) to display the Call Control Settings menu for JetStream:

Figure 4.78 Call Control Settings Menu for JetStream Voice Gateway

**Call Control Settings**

- A. StatsDisplay
- B. Display Error Stats
- R. Ring Test
- S. Display IAD state
- T. Trace
- U. Pick sound heard if insufficient WAN B/W to complete call
- P. Enable/Disable App Controlled ATM Pacing
- Y. Zero ErrorStats
- Z. Zero StatsDisplay

Each option on this menu is described in detail below.

**StatsDisplay** Type "A" to display the JetStream Voice Gateway statistics report.

```
0 POTS TX PKTS
0 POTS TX BYTES
0 POTS TX DROPPED
0 POTS TX DROPPED VOICEPATH CLOSED
0 L2 RX PKTS
0 L2 RX BYTES
0 L2 TX PKTS
0 L2 TX BYTES
```

**Display Error Stats** Type "B" to display the JetStream Voice Gateway error statistics.

```
0 Dropped Segment Enqueued to Adaptation messages
0 Dropped Control Enqueued to Management messages
0 Control Dequeue failures
0 L2 Timer Start Failures
0 L2 Timer Stop Failures
0 Management Message Dequeue failures
0 Dropped Management Enqueued to Call Control messages
0 Dropped Management Enqueued to L2 messages
```

**Ring Test** This command is reserved for use by Verilink network engineers only.

**Display IAD State** Type "S" on the Call Control Settings menu (Figure 4.78) to display the on hook state for each port. The IAD displays the following information:

```
Port 02 is offhook Call Control state = Idle POTS state = Disabled
Port 03 is offhook Call Control state = Idle POTS state = Disabled
Port 04 is offhook Call Control state = Idle POTS state = Disabled
Port 05 is offhook Call Control state = Idle POTS state = Disabled
Port 06 is offhook Call Control state = Idle POTS state = Disabled
Port 07 is offhook Call Control state = Idle POTS state = Disabled
Port 08 is offhook Call Control state = Idle POTS state = Disabled
Received Segmentation Layer CRC failures since powerup = 0
```

**Trace** This option for use by JetStream or Verilink network engineers to configure Trace settings.

**Pick Sound Heard if Insufficient WAN B/W to Complete Call** 1 Type "V" on the Call Control Settings (Figure 4.78) menu to select the type of dial tone heard by the telephone user if there is insufficient WAN bandwidth to complete a call. The IAD displays the Insufficient Bandwidth Indication Setting menu (Figure 4.79) and the current setting:

**Figure 4.79** *Insufficient Bandwidth Indication Setting Menu*

```
***** Insufficient Bandwidth Indication Setting *****  
  
Current sound setting = Silence  
  
0. Play Silence  
1. Play Fast Beeping  
-----
```

- 2** Type "0" to replace the dial tone with silence, or type "1" to replace dial tone with a fast beeping sound.
- 3** Press Escape to return to the Call Control Setting menu and continue configuration.

**Zero ErrorStats** Type "Y" on the Call Control Settings menu to reset the JetStream statistics.

**Zero Stats Display** Type "Z" on the Call Control Settings menu to display the JetStream statistics.

### ***CopperCom***

When your IAD is configured for connection to a Coppercom Voice Gateway (option "V" on the VoicePath Configuration menu – P-V), type "E" on the Main menu (Figure 2.2) to display the CopperCom Call Control menu.

**Figure 4.80** *CopperCom Call Control Menu*

```
*****  
*           CopperCom Call Control           *  
*****  
  
S. Statistics  
C. Configure  
D. Debug Control
```

Each option on this menu is described in detail below.

**Statistics** Type "S" on the CopperCom Call Control menu to display the CopperCom Statistics menu.

**Figure 4.81** *CopperCom Statistics Menu*

```
*****  
*           CopperCom Statistics           *  
*****  
  
D. Display Statistics  
C. Clear Statistics
```

Each of the options on this menu is described in detail below.

## Display Statistics

- 1 Type "D" to display CopperCom statistics. Clear CopperCom Statistics
- 2 Type "A" to reset CopperCom statistics. The IAD sets the statistics to zero and redisplay the CopperCom Statistics menu.

Press Escape to return to the CopperCom Call Control menu.

## Clear Statistics

Type "C" to clear CopperCom statistics.

**Configure** Type "C" on the CopperCom Call Control menu to display the CopperCom Configuration menu.

**Figure 4.82** *CopperCom Configuration Menu*

```
*****  
*           CopperCom Configuration  
*****  
  
D. Display Configuration  
C. Compression Format  
F. Framing Format
```

Each option on this menu is described in detail below.

## Display Configuration

Type "D" on the CopperCom Configuration menu to display the current configuration settings. tiple packets

## Compression Format

To set compression globally or by port, follow the steps below.

- 1 Type "C" on the CopperCom Configuration menu to set the compression format.
- 2 Type the port number, or type "0" to set the compression for all ports. The IAD displays a port prompt.
- 3 Type the option for the selected compression. The IAD saves the changes and redisplay the menu.
- 4 Press Escape to return to the CopperCom Configuration menu and continue configuration.

## Framing Format

- 1 Type "F" on the CopperCom Configuration menu to display a CopperCom Configuration menu with Frame Relay Mode options:

**Figure 4.83** *CopperCom Configuration Menu with Frame Relay Mode Options*

```
*****
*           CopperCom Configuration           *
*****

Current Frame Relay Mode = 44 octets & Multiple packets

1. 36 octet packet, Single packet per frame
2. 44 octet packet, Multiple packets per frame
```

- 2 Type "1" to select a 36 octet packet, using a single packet per frame, or type "2" to select a 44 octet packet, with multiple packets per frame. The IAD saves the changes and displays the menu.
- 3 Press Escape to return to the CopperCom Configuration menu and continue configuration.

### **AAL2/LES CCS-ELCP**

ATM Adaptation Layer 2/Loop Emulation Services (AAL2/LES) is a broadband local loop emulation service (specifically telephony) that uses the ATM AAL2 adaptation layer. CCS-ELCP is defined by ETSI EN 300 432-1 and ETSI EN 300 347-1.

When the voice gateway is specified as AAL2/LES CCS-ELCP (also known as V5.2 signaling), type "E" on the Main menu (Figure 2.2) to display the AAL2/LES CCS-ELCP menu:

**Figure 4.84** *AAL2/LES CCS-ELCP Menu*

```
*****
*           AAL2/LES CCS-ELCP           *
*****
C. Configuration
D. Debugging
S. Statistics
```

Each option on this menu is described in detail below.

**Configuration** Type "C" on the AAL2/LES CCS-ELCP menu to display the AAL2 LES CCS-ELCP Manual Configuration menu:

**Figure 4.85** *AAL2/LES CCS-ELCP Configuration Menu*

```
*****
*           Configuration           *
*****
U. Variant and Interface Management
N. PSTN NPL Parameters
S. Static CID Allocation
U. User State Control
T. Combined Use Timer
A. Manual ATM Pace Control
```

## Variant/Interface Management

Use of commands in the Variant/Interface Management menu is reserved for use by Verilink network engineers only.

**Figure 4.86** *Variant/Interface Management Menu*

```
*****
*   Variant/Interface Management   *
*****
  D. Display Variant
  P. Configure PSTN Port
  I. Configure ISDN Port
  L. Load Variant
  U. Unload Variant
  W. Save Variant
  X. Delete Saved Variant
  R. Restart Interface
  S. Shut Down Interface
```

**Debugging** The use of this option is reserved for Verilink network engineers only. Enabling debug options may significantly affect IAD performance.

**Statistics** Type "S" on the AAL2/LES CCS-ELCP menu to display the AAL2 Channel Statistics menu:

**Figure 4.87** *AAL2 Channel Statistics Menu*

```
*****
*   AAL2 Channel Statistics   *
*****
  D. Display AAL2 Channel Statistics
  C. Clear AAL2 Channel Statistics
  --- . . . .
```

### Display AAL2 Channel Statistics

Type "D" to display the AAL2 Channel (Audio and Alarm) Statistics. Press Escape to return to the menu. Press C to reset the statistics, or press any other key to refresh the statistics and display them again.

### Clear AAL2 Channel Statistics

Type "C" to reset the AAL2 channel statistics.

### *MGCP 1.0 (Supported Only in VoIP versions as denoted by an "s" in the Model Number)*

You may select Manage MGCP Embedded Client by typing "O" on the Main menu (Figure 2.2) to display the MGCP Management menu (Figure 4.88).



---

**NOTICE:** *The IAD only displays option "O" to manage VoIP embedded client on the main menu. The embedded client can be either MGCP or SIP.*

---

Figure 4.88 MGCP Management Menu

```
*****
*                               MGCP Management Menu                               *
*****
C. Configure MGCP parameters
I. Display MGCP parameters
E. CODEC selection Menu
S. Display MGCP statistics
R. Remove a connection
A. Port Administration
P. Configure Default Packet Size
```

Each of the options on this menu is described in detail below.

**Configure MGCP Parameters**

- 1** Type "C" on the MGCP Management menu (Figure 4.88) to set the Transmit and Receive parameters for MGCP. The IAD can support up to four call agents. These may be specified via IP address or DNS name. The IAD displays the Notified Entity prompt for the first call agent and asks you to enter the DNS Name or the IP address.
- 2** Type the DNS name (*mg1.acme.com*, for example), or the IP address of the call agent and press Enter. The IAD updates the IP address of the MGCP Call Agent (which controls call setup and teardown for all call features under MGCP) for the entity, increases the entity index by one and prompts you to complete the entries for call agents or press Enter to leave the agent(s) unconfigured.
- 3** The IAD next prompts you to enter the listening port. Enter the listening port of the Notified Entity:
- 4** Type the port number (usually 2427 or 2727) that the call agent is listening on, and press Enter. The IAD displays the available interfaces and prompts you to select an interface from those available.
- 5** Type the option number to select the signaling interface for MGCP to use (typically the WAN interface). The IAD displays the port table for this interface and prompts you to enter a port.
- 6** Type the port to configure and press Enter. The IAD displays a bracketing prompt.
- 7** Type "Y" to wrap the port in brackets for call agent API compatibility, or "N", and press Enter. The IAD prompts you for the outbound signaling packets TOS field value:
- 8** Type the field value and press Enter. The IAD prompts you for the RTP transport packets TOS field value:
- 9** Type the field value and press Enter. The IAD saves the settings and redisplay the MGCP/NCS Management menu so you may continue configuring MGCP/NCS.

**CODEC Selection Menu**

Type "E" on the MGCP Management menu to select the CODEC option you wish to use. The default is G.729a. The use of 726 and 729a are mutually exclusive; the IAD will configure only one or the other.



**Display MGCP Statistics** Type "S" on the MGCP Management menu (Figure 4.88) to display the endpoint (line) and connection statistics. If no calls are active, the IAD indicates if the Endpoint is currently connected to its Notified Entity or not. If MGCP configuration is not correct, the IAD displays a message warning you that the configuration is invalid and initialization is incomplete.

**Remove a Connection**

- 1 Type "R" on the MGCP Management menu (Figure 4.88) to remove a lost connection.
- 2 Type the number of the Connection ID to delete and press Enter.

**Port Administration** Type "A" on the MGCP Management menu to (Figure 4.88) to display the Port Administration menu (Figure 4.89).

**Figure 4.89** *Port Administration Menu*

```
*****
*                               *
*           Port Administration   *
*                               *
*****
  1. Set Admin State for all ports
  2. Display current Admin State
  3. Configure Admin State per port
  4. Restart Endpoint
```




---

**NOTICE:** *These options are only available when you log in at the Network Administrator or Supervisor levels.*

---

### Set Admin State for All Ports

- 1 Type "1" on the Port Administration menu (Figure 4.89) to enable or disable the admin state for all ports.
- 2 Type "E" to enable the admin state, or "D" to disable it. The IAD saves the mode you've selected and redisplay the Port Administration menu.
- 3 Press Escape to return to the Voice Configuration menu and continue with other voice path configuration.

### Display Current Admin State

To display the Current Admin State, follow the steps below.

- 1 Type "2" on the Port Administration menu (Figure 4.89) to display the current admin state by port number. The IAD displays the report:
- 2 Press any key to return to the Port Administration menu.

### Configure Admin State per Port

To configure the Admin State per port, follow the steps below.

- 1 Type "3" on the Port Administration menu (Figure 4.89) to enable or disable the admin state for a specific port. The IAD prompts you to enter a port.

- 2 Type the port number to set. The IAD prompts you to enable or disable Port Administration for that port.
- 3 Type "E" to enable the admin state, or "D" to disable it. The IAD saves the mode you've selected and redisplay the Current Admin State menu.
- 4 Press Escape to return to the Port Administration menu and continue with other voice path configuration.

### Restart Endpoint

To restart an Endpoint, follow the steps below.

- 1 Type "4" on the Port Administration menu (Figure 4.89) to reset the connection between the Voice Port phone and the MGCP voice gateway. (Use this option if one side of the link incorrectly identifies a call as up and the other side thinks the call as down.)
- 2 To reset the connection, type the number of the port and press Enter.

### Configure Default Packet Size

To configure the Default Packet Size, follow the steps below.

- 1 Type "P" on the MGCP Management (Figure 4.88) menu. The IAD prompts you to enter the packet size.
- 2 Type the packet size value in microseconds and press Enter. The IAD saves the new packet size and redisplay the menu.
- 3 Press Escape to return to the MGCP menu and continue with other voice path configuration.

### *SIP (Supported Only in VoIP versions as denoted by an "s" in the Model Number)*

You may select Manage MGCP Embedded Client by typing "O" on the Main menu (Figure 2.2) to display the SIP Management menu (Figure 4.88).




---

**NOTICE:** *The IAD only displays option "O" to manage VoIP embedded client on the main menu. The embedded client can be either MGCP or SIP.*

---

Figure 4.90 SIP Management Menu

```

*****
*                               SIP Management Menu                               *
*****
C. Configure SIP parameters
I. Display SIP parameters
N. Config Individual SIP parameters
E. CODEC selection Menu
S. Display SIP statistics
A. Port Administration
P. Configure Default Packet Size

```

### Configure SIP Parameters

To Configure SIP parameters, follow the steps below.

- 1 Type "C" on the SIP Management menu (Figure 4.90) to set the Transmit and Receive parameters for SIP.
- 2 Enter the DNS name or IP address for the SIP proxy (*siptest.somewhere.com*, for example, including the dotted IP address or the FQDN of a SIP proxy). The currently configured proxy is displayed in the brackets. After typing the text, press Enter.
- 3 Enter the DNS name or IP address for the SIP proxy backup (*siptest.somewhere.com*, for example, including the dotted IP address or the FQDN of a SIP proxy backup). The currently configured proxy backup is displayed in the brackets. After typing the text, press Enter.
- 4 The IAD prompts you for the line prefix, which is part of an endpoint (phone line) name common to all endpoints on the IAD. Endpoints are named in the following manner: line\_prefixXX, where XX is the endpoint number. For example, the prefix blackphone will produce names blackphone01 and blackphone02 on an IAD using the first two phone lines. After typing the text (or to keep the line unmodified), press Enter.
- 5 The IAD prompts you for a password, which is required to authenticate the proxy. After typing the text (or to keep the line unmodified), press Enter.
- 6 The IAD will display the SIP signaling parameters, and you may configure the VPI/VCI. This interface/own IP address is used to send/receive SIP signaling packets and is the same interface/port/connection configured elsewhere in the IAD.
- 7 Enter the starting RTP to be used for voice transport. This interface/own IP address is used for RTP voice streams. The starting port number is the port number used by the first phone line, and the port numbers increment by two for each line. You may type in a new value and then press Enter, or press Enter without typing in a new value to retain the old value.
- 8 The IAD displays the RTP transport parameters. This is the same interface/port/connection configured elsewhere in the IAD.
- 9 Enter the TOS byte of the SIP signaling packets [0-7]. You may enter a new value or press Enter to retain the old value. The TOS values are prioritized in the IP QoS menus.
- 10 Enter the TOS byte of the RTP voice streams [0-7]. You may enter a new value or press Enter to retain the old value. The TOS values are prioritized in the IP QoS menus.

<b>Display SIP Parameters</b>	Type "I" on the SIP Management menu (Figure 4.90) to display the configured SIP parameters.
<b>Config Individual SIP Parameters</b>	Type "N" on the SIP Management (Figure 4.90) menu to display Individual SIP parameters. This allows individual setting of parameters needed for SIP.
<b>CODEC Selection Menu</b>	Type "E" on the SIP Management menu (Figure 4.90) to select the CODEC option you wish to use. The default is G.729a. The use of 726 and 729a are mutually exclusive; the IAD will configure only one or the other.

**Display SIP Statistics** Type "S" on the SIP Management menu (Figure 4.90) to display the endpoint (line) and connection statistics. If no calls are active, the IAD indicates whether or not the endpoint is currently connected to its Notified Entity.

If SIP configuration is not correct, the IAD displays a message warning you that the configuration is invalid and initialization is incomplete.

**Port Administration** Type "A" on the SIP Management menu (Figure 4.90) to display the Port Administration Menu (Figure 4.91).

**Figure 4.91** *Port Administration Menu*

```
*****  
*                               Port Administration Menu                               *  
*****  
  1. Set Admin State for all ports  
  2. Display current Admin State  
  3. Configure Admin State per port  
  4. Register port  
  5. Register All ports
```

### **Set Admin State for all Ports**

Lets you enable or disable all ports on the IAD.

### **Display Current Admin State**

Displays the current Admin State of all ports.

### **Configure Admin State per Port**

Lets you enable or disable individual ports.

### **Register Port**

Lets you register a port with a SIP proxy.

### **Register All Ports**

Registers all enabled lines with a SIP proxy.

**Configure Default Packet Size** To configure the Default Packet Size, follow the steps below.

- 1** Type "P" on the SIP Management menu (Figure 4.90). The IAD prompts you to enter the packet size.
- 2** Type the packet size value in microseconds and press Enter. The IAD saves the new packet size and redisplay the menu.
- 3** Press Escape to return to the SIP menu and continue with other voice path configuration.

In addition to the above configuration settings, there are some global settings that may be required for the proper operation of the SIP client. If you use FRDN for the SIP proxy entry above, you must configure the DNS server. Refer to *Configure DNS Client* on page 4-45.

You may also configure a dial plan via external means. The default dial plan built into the SIP application is shown below.

```

" [2-9] 11 "
" [0-1] [2-9] 11 "
" 0 [#T] "
" 00 "
" 01 [2-9] xx. [#T] "
" *xx "
" 011x. [3t] "
" [0-1] xxxxxxxx [#T] "
" [0-1] [2-9] xxxxxxxxxx "
" [2-9] xxxxxxxxxx "
" [2-9] xxxxxx [#T] "
" 101xxxx. [#T] "
" xxxx [#T] "

```

You may upload a file by the name of *dialplan.st* to the IAD to change the default dial plan. Each line of that file defines a dial string just like the example above. For the syntax of the dial plan, refer to the Dial Plan Application Note under *Dial Plan* on page C-12.

## Set Jitter Delay

Inter-arrival jitter is the difference in relative transit time for two packets. It is the difference between the packet's RTP time-stamp and the receiver's clock at the time of arrival of the packet.

As shown in the equation below, this is equivalent to the difference in the relative transit time for two packets: the relative transit time is the difference between a packet's RTP time-stamp and the receiver's clock at the time of arrival, measured in the same units.

If  $S_i$  is the RTP time-stamp from packet  $i$  and  $R_i$  is the time of arrival in RTP time-stamp units for packet  $i$ , then for two packets  $i$  and  $j$ ,  $D$  may be expressed as:

$$D(ij) = (R_j - R_i) - (S_j - S_i) = (R_j - S_j) - (R_i - S_i)$$

The interval jitter is calculated continuously as each data packet  $i$  is received from source  $SSRC-n$ , using this difference  $D$  for that packet and of the previous packet  $i-1$  in order of arrival (not necessarily in sequence), according to the formula:

$$J = J + (\{D(i-1, i)\} - J) / 16$$

The Jitter Delay should be set only by a Network Administrator. To set jitter delay (0 to 50 ms – default is 0 ms), follow the steps below.

- 1 Type "J" on the Voice Configuration menu (Figure 4.71) to select Set Jitter Delay. The IAD prompts you to enter the number of milliseconds to delay.

- 2 Type the delay value and press Enter. The IAD saves the jitter delay and displays the Voice Configuration menu so you can continue with other voice path configuration.

## Voice Port Settings

To display the Voice Port Configuration Menu (Figure 4.92), type "P" on the Voice Configuration menu (Figure 4.71). Voice port settings should be changed only under certain circumstances. Please consult Verilink technical support prior to changing these setups.

**Figure 4.92** *Voice Port Configuration Menu*

```
*****
*           Voice Port Configuration           *
*****
S. Set Start Mode (Loop Start/Ground Start)
O. Set On Hook Transmission Mode of Ground Start Lines
E. Configure Echo Cancellation Default Settings
G. Set Loop Gain
P. Configure Pulse Dial Detection Settings
```

### *Set Start Mode (Loop Start/Ground Start)*

To set start mode (for POTS only), type "S" on the Voice Configuration menu (Figure 4.71) to display the Start Mode Selection menu (Figure 4.93).

**Figure 4.93** *Start Mode Selection Menu*

```
*****
*           Start Mode Selection             *
*****
1. Set All Ports to Loop Start
2. Set All Ports to Ground Start
3. Display Start Mode
4. Configure Individual Port
```




---

**NOTICE:** *The loop start and ground start features apply to ATM signaling only.*

---

Each option on this menu is described in detail below.

#### **Set All Ports to Loop Start**

- 1 Type "1" to select Set All Ports to Loop Start. The IAD sets all ports to Loop Start and saves the configuration.
- 2 Press any key to return to the Start Mode Selection menu or press escape to continue with other voice path configuration.
- 3 Reset the IAD when you finish voice path configuration.

#### **Set All Ports to Ground Start**

To set All Ports to Ground Start, follow the steps below.

- 1 Type "2" on the Start Mode Selection menu (Figure 4.93) to select Set All Ports to Ground Start. The IAD sets all ports to Ground Start and saves the configuration.
- 2 Press any key to return to the Start Mode Selection menu or press Escape to continue with other voice path configuration.
- 3 Reset the IAD when you finish voice path configuration.



---

**NOTICE:** For "Ground Start" applications all elements in the voice path must be set to "Ground Start."

---

**Display Start Mode** To display Start Mode, follow the steps below.

- 1 To display a list of telephone ports and their current start mode, type "3" on the Start Mode Selection menu (Figure 4.93). The IAD displays a list of ports and the mode of each.
- 2 Press any key to return to the Start Mode Selection menu or press Escape to continue with other voice path configuration.

**Configure Individual Port** To configure Start Mode on an individual port, follow the steps below.

- 1 Type "4" on the Start Mode Selection menu (Figure 4.93). For each port, the IAD prompts you to type one of the following options for each port.
  - 1—Loop Start
  - 2—Ground Start
  - 3—DID Wnk
  - 4—E&M Wnk
  - 5—RAW ABCD
  - 0 or Enter—no change
- 2 After you have updated each port, Press Enter a final time. The IAD updates the settings and saves the configuration.
- 3 Press any key to return to the Start Mode Selection menu or press Escape to continue with other voice path configuration.

### ***Set On Hook Transmission Mode of Ground Start Lines***

To set On-Hook Transmission mode (OHT) (POTS only) for ground start lines, follow the steps below.

- 1 Type "0" on the Voice Configuration menu (Figure 4.71) to display the Ground Start OHT Mode Selection menu (Figure 4.94).

**Figure 4.94** *Ground Start OHT Mode Selection Menu*

```
*****
*   Ground Start OHT Mode Selection   *
*****

On Hook Transmission for a Ground Start Line is DISABLED.

E. ENABLE Ground Start On Hook Transmission
D. DISABLE Ground Start On Hook Transmission
```

- 2 Type "E" to enable onhook transmission mode, or "D" to disable it. The IAD saves the mode you've selected and redisplay the Ground Start OHT Mode Selection menu.
- 3 Press Escape to return to the Voice Configuration menu and continue with other voice path configuration.

### **Configure Echo Cancellation Default Settings**

To set echo cancellation default settings, type "E" on the Voice Configuration menu (Figure 4.71) to display the Echo Cancellation Default Settings Configuration menu (Figure 4.95).

**Figure 4.95** *Echo Cancellation Default Settings Configure Menu*

```
*****
* Echo Cancellation Default Settings Configure Menu *
*****

1. Set Echo Cancellation default setting for all ports
2. Display current Echo Cancellation default settings
3. Configure Echo Cancellation default setting per port
```

Each of the options on this menu is described in detail below.

#### **Set Echo Cancellation Default Setting for All Ports**

- 1 Type "1" on the Echo Cancellation Default Settings Configuration Menu (Figure 4.95) to enable or disable echo cancellation for all ports.
- 2 Type "E" to enable echo cancellation for all ports, or "D" to disable it. The IAD saves the mode you've selected and redisplay the Echo Cancellation Default Settings Configuration menu.
- 3 Press Escape to continue with other voice path configuration.

#### **Displaying Current Echo Cancellation Default Settings**

- To display the Current Echo Cancellation default settings, follow the steps below.
- 1 Type "2" on the Echo Cancellation Default Settings Configuration Menu (Figure 4.95) to display the echo cancellation setting on each port. The IAD lists each port and whether echo cancellation is enabled or disabled.
  - 2 Press any key to return to the Echo Cancellation Default Settings Configuration menu.



### Configure Echo Cancellation Default Setting per Port

To configure the Echo Cancellation default setting per port, follow the steps below.

- 1 Type "3" on the Echo Cancellation Default Settings Configuration menu (Figure 4.95) to enable or disable echo cancellation for a specific port. The IAD prompts you to choose a line or port.
- 2 Type the port number to set. The IAD prompts you to enable or disable echo cancellation for that port.
- 3 Type "E" to enable echo cancellation, or "D" to disable it. The IAD saves the mode you've selected and redisplay the Echo Cancellation Default Settings Configuration menu.
- 4 Press Escape to continue with other voice path configuration.

### Set Loop Gain

When a country mode is selected, default loop gain values for that country are assigned to the IAD. If the IAD feeds telephone circuits into a legacy PBX or other equipment that defines transmit and receive levels to the network, the loop gain value must match the value of the circuit it supplies. The levels are determined and set by the PBX or terminating equipment manufacturer.

Adjusting the loop gain on the IAD can also compensate for telephone volume's being too loud or too soft.



---

**NOTICE:** *Loop gain values should be set only by your Network Administrator.*

---

To set loop gain values, type "G" on the Voice Configuration menu (Figure 4.71) to display the Configure Loop Gain menu (Figure 4.96).

**Figure 4.96** *Configure Loop Gain Menu*

```
*****
*           Configure Loop Gain Menu           *
*****
  1. Set Loop Gain for all ports
  2. Display current Loop Gain settings
  3. Configure Loop Gain setting per port
```

Each of the options on this menu is described in detail below.

### Set Loop Gain for All Ports

To set the Transmit (-9 to 3 dB – default -2 dB) and Receive (-9 to 3 dB – default -4 dB) Loop Gain values for all ports, follow the steps below.

- 1 Type "1" on the Configure Loop Gain menu (Figure 4.96) to select Set Loop Gain for all ports. The IAD prompts you to enter the Transmit Loop Gain for all ports.
- 2 Type the value (include a dash for negative values) and press Enter. The IAD displays prompts you to enter the Receive Loop Gain for all ports.

- 3 Type the value (include a dash for negative values) and press Enter. The IAD saves the loop gain values and displays the Configure Loop Gain menu (Figure 4.96).
- 4 Press Escape to return to the Voice Configuration menu and continue voice path configuration.

**Display Loop Gain Settings** To display the Loop Gain settings, follow the steps below.

- 1 Type "2" on the Configure Loop Gain menu (Figure 4.96). The IAD displays the loop gain values for each telephone port on the IAD.
- 2 Press any key to return to the Configure Loop Gain menu or press Escape to return to the Voice Configuration menu and continue with other voice path configuration.

**Configure Loop Gain Setting by Port** To set Transmit and Receive Loop Gain values by port, follow the steps below.

- 1 Type "3" on the Configure Loop Gain menu (Figure 4.96). The IAD prompts you to select a port or line to configure.:
- 2 Type the line number and press Enter. The IAD prompts you to enter the Transmit Loop Gain for all ports.
- 3 Type the value (include a dash for negative values) and press Enter. The IAD prompts you to enter the Receive Loop Gain for all ports.
- 4 Type the value (include a dash for negative values) and press Enter. The IAD saves the loop gain values and redisplay the Configure Loop Gain menu.
- 5 Press Escape to return to the Voice Configuration menu and continue voice path configuration.

### *Configure Pulse Dial Detection Settings*

**Figure 4.97** *Pulse Dial Detection Settings Configuration Menu*

```
*****
*   Pulse Dial Detection Settings Configure Menu   *
*****
1. Set Pulse Dial Detection setting for all ports
2. Display current Pulse Dial Detection settings
3. Configure Pulse Dial Detection setting per port
```

### **Display Comander Mode ( $\mu$ -law, A-law)**

- 1 To display the Comander Mode, type "U" on the Voice Configuration menu. The screen will display whether  $\mu$ -law, A-law is the current Comander Mode.
- 2 Press Escape to return to the Voice Configuration menu and continue with other voice path configuration.

---

**NOTICE:** Normally, u-Law is used in North America and a-Law is used in Europe.

---

## Set Country Mode

Figure 4.98 Country Mode Selection Menu

```
*****
*           Country Mode Selection           *
*****

Current Country Name is United States of America
A. United States of America
```

## Set DuSLIC Mode

To set DuSLIC Mode (for POTS only), follow the steps below. (The following are configured when a Country Mode is selected.)

- 1 Type "T" on the Voice Configuration menu (Figure 4.71) to display the DuSLIC Mode Selection menu.

Figure 4.99 DuSLIC Mode Selection Menu

```
*****
*           DuSLIC Mode Selection           *
*****

Current DuSLIC coefficient file is USA - 24ma offset 60Volt
A. USA - 24ma offset 60Volt
B. USA - 32ma offset 60Volt
C. USA - 24ma balanced 85Volt
D. USA - 32ma balanced 85Volt
E. USA - 24ma unbalanced 48Volt
F. USA - 32ma unbalanced 48Volt
```

- 2 Type the option of the control mode to set. The IAD saves the mode you've selected and redisplay the menu.
- 3 Press Escape to return to the Voice Configuration menu and continue with other voice path configuration.

## Enable/Disable G726 Annex A

Type "G" on the Voice Configuration menu (Figure 4.71) to enable/disable G726 Annex A.

---

# Interworking Connections

---

To communicate over WANs, end-user stations and the network cloud have typ-

ically been required to use the same type of transmission protocol. This limitation has prevented different network protocols such as Frame Relay and ATM from being linked. However, the High POTS Port IAD's Frame Relay-to-ATM Network/Service Interworking (FRF.5/FRF.8) feature allows Frame Relay and ATM networks to exchange data, despite differing network protocols. The functional requirements for linking Frame Relay and ATM networks are provided by the Frame Relay/ATM PVC Network/Service Interworking Implementation Agreement specified in Frame Relay Forum (FRF) document numbers FRF.5. and FRF.8. Before setting the interworking options, you must first configure the Frame Relay options for the USI port, and the ATM options for the WAN port. Interworking can be configured to support FRF.5 or FRF.8 and will support a maximum of four VCs. When FRF.5 or FRF.8 interworking is configured on a PVC or DLCI, it is switched at the Layer 2 level. Data does not go up the IP or bridge stacks, so configuring bridging or an IP address on an interworked PVC or DLCI is not possible. FRF.8 Frame/ATM service Interworking maps Frame datalink connection identifiers (DLCIs) to ATM permanent virtual circuits (PVCs). FRF.5 provides network Interworking functionality that allows Frame Relay end users to communicate over an intermediate ATM network.

---

**NOTICE:** *When configuring the Network port and the USI port, it is important to ensure the correct encapsulations are used. On the Network port, use RFC 1483(with LLC Encapsulation) PVCs. On the USI port, RFC 1490 DLCIs are valid for interworking.*

---

To access the Interworking feature, select "I" on the Main menu, which will display the Connections menu shown in Figure 4.100.

**Figure 4.100** *Connections Menu*

```
*****
*           Connections Menu           *
*****
  1. Add Interworking Connection
  2. Delete Interworking Connection
  3. Display Interworking Connections
  4. Default Interworking Connections
```

Select select "1" to add an Interworking Connection. The following menu will be displayed:

**Figure 4.101** *Interworking Connections Menu*

```
Create an interworking connection (FRF5 or FRF8)

Select the Frame Relay interface for the interworking

Available WAN Interfaces :
  1. T1/E1
  4. Universal Serial
  0. (Abort)
Selection : _
```

After making your selection, select the desired port from the next menu. You will then select the appropriate ATM interface from the available WAN interfaces and once again will select the desired port. At this point, you will select either FRF5 or FRF 8 Interworking protocol from the menu as shown below.

**Figure 4.102** *Available Interworking Types Menu*

```
Available interworking types:

1. FRF5
2. FRF8

Esc to Exit
Select interworking protocol: _
```

When FRF.5 is selected, the ATM channel implements FRF.5 Network Interworking, providing a Frame Relay link that can transport data for one or more DLCIs. When FRF.8 is selected, the ATM channel implements FRF.8.1 Service Interworking, providing a conversion from a Frame Relay PVC to this ATM PVC.

## FRF.5

If you select FRF5, the menu below will be displayed.

**Figure 4.103** *FRF.5 DE Mapping Menu*

```
*****
*          FRF.5 DE Mapping          *
*****
  0. Set FR-SSCS, ATM = 0
  1. Set FR-SSCS, ATM = 1
  B. Use both FR-SSCS and ATM
```

If you select "0" or "1", the DE field in the Q.922 core frame is copied unchanged into the DE field in the FR-SSCS header and the ATM Cell Loss Priority (CLP) of every ATM cell generated by the segmentation process of that frame will be set to a constant value (either 0 or 1).

If you select "B" (refer to the menu below), the Discard Eligibility (DE) field in the Q.922 core frame is copied unchanged into the DE field in the FR-SSCS header and is mapped to the ATM Cell Loss Priority (CLP) of every ATM cell generated by the segmentation process of that frame.

**Figure 4.104** *FRF.5 CLPI Mapping Menu*

```
*****
*           FRF.5 CLPI Mapping           *
*****
  A. Set FR-SSCS according to ATM
  B. Use both FR-SSCS and ATM
```

If you select "A", no mapping is performed from the ATM layer to the Q.922 core layer. The FR-SSCS DE field is copied unchanged to the Q.922 core frame DE field independent of CLP indication(s) received at the ATM layer.

If you select "B", then if one or more ATM cells belonging to a frame has its CLP field set to one or if the DE field of the FR-SSCS PDU is set to one, the IAD will set the DE field of the Q.922 core frame.

## FRF.8

If you select FRF8 from the Available Interworking Types menu (Figure 4.102), the menu below will be displayed.

**Figure 4.105** *FRF.8 Translation Menu*

```
*****
*           FRF.8 Translation           *
*****
  T. True
  F. False
```

The selection of one of these options will determine how upper layer user protocol encapsulation is handled. If you select "T", the FRF.8 Interworking function maps between the two encapsulations, translating between RFC 1490 and RFC 1483. If you select "F", there is no translation of the data. It is transported transparently between frame Relay DLCI and the ATM PVC. The IAD forwards encapsulations unaltered; no mapping or fragmentation/reassembly is performed on the data.

Select "T" to see the menu below displayed.

**Figure 4.106** *FRF.8 DE Mapping*

```
*****
*           FRF.8 DE Mapping           *
*****
  0. Always 0
  1. Always 1
  M. Map FR DE to ATM CLPI
```

If you select "0", the discarding of cells will never be allowed, and if you select "1", discards will never be allowed.

If you select "M" (refer to the menu below), this allows bi-directional mapping of the Frame Relay DE to the ATM CLPI. The purpose of this is to identify in the protocol header that this frame may discard the frame if congestion is indicated.

**Figure 4.107** FRF.8 FECN Mapping

```
*****
*       FRF.8 FECN Mapping       *
*****
  0. Always 0
  1. Always 1
  M. Map FR FECN to ATM EFCI
```

If you select "0", no congestion will always be indicated, and if you select "1", congestion will always be indicated.

If you select "M", this allows bi-directional mapping of the Frame Relay Forward Explicit Congestion Notification (FECN) to the ATM Explicit Forward Congestion Indication (EFCI). The purpose of this is to identify in the protocol header that the network has congestion.

## Firewall Configuration

---

Firewall configuration (also known as IP filtering) allows you to specify a combination of parameters the IAD uses to selectively eliminate IP traffic.

Refer to the IP Filtering Application Note contained in *Appendix C*.

### Creating a Firewall via IP Filtering and NAT

IP Filtering, in conjunction with NAT, can provide a Firewall for securing the local network from unwanted and possibly harmful traffic. By defining a set of rules (IP Filtering) and open ports (NAT), you may selectively block traffic and deny access to the local network.

IP Filtering controls IP traffic traveling through an interface by selectively passing or discarding IP packets based on criteria expressed in the form of a "filter." A filter is simply a set of rules that determine whether a packet should be passed or discarded as it crosses an interface. An interface is any port that carries IP traffic. On the IAD, it can be one of the following: Ethernet port, PPP connection, ATM PVC, or FR DCLI.

IP Filtering can selectively pass or discard IP packets based on one or more of the following properties:

- Protocol (IP, ICMP, TCP, and UDP)
- Protocol flags (for TCP and ICMP only)
- Source and/or Destination IP address
- Source and/or Destination port number

For more information on defining and using a filter rule set, see IP Filtering Application note on page C-4.

For more information, see *Configure IP Filtering* on page 4-49.

# DHCP Server Configuration

---

This section describes the tasks required to configure the Dynamic Host Configuration Protocol (DHCP) server on the LAN connection.

DHCP allows for dynamic allocation of network addresses and configurations to newly attached hosts. DHCP reduces the amount of work required to administer a large network.

## Basic DHCP Server Setup Tasks

When DHCP is enabled, it dynamically assigns an IP address to each device assigned to the DHCP server on the IAD. You must identify the Ethernet Interface to correctly implement DHCP Server on your IAD.

You must complete at least these tasks to configure the DHCP server:

- Enable DHCP (default is disabled) (page 4-89)
- Configure the DHCP server parameters (page 4-89)
- Configure the DHCP address range pool (page 4-90)

## DHCP Server Configuration Menu

The DHCP Server commands are all displayed on the DHCP Server Configuration menu, which is displayed by typing "D" on the Main menu (Figure 2.2). Remember always to reset the IAD when you have finished making DHCP Server configuration changes.

**Figure 4.108** *DHCP Server Configuration Menu*

```
*****
*      DHCP Server Configuration Menu      *
*****
E. Enable/Disable DHCP
H. Enable/Disable Checking for Additional DHCP Servers
I. Configure DHCP Server Parameters
P. Configure DHCP Address Range Pool
C. Configure DHCP Client Entry
F. Display DHCP Configuration
S. Display DHCP Server Statistics
A. Display DHCP Server Assigned Addresses
U. Display DHCP Server Unassigned Addresses
D. Display DHCP Entry Details
X. Delete A DHCP Client Entry
Y. Delete A DHCP Assignment Entry
```

You may sign on as Supervisor or Network Manager to configure the IAD for use as a DHCP Server. Options that display in the DHCP Server Configuration menu are the same for both security levels.



---

**NOTICE:** *You must reset the IAD (page 2-8) after configuring the IAD as a DHCP Server for the configuration changes to take effect.*

---



## Enable/Disable DHCP Server

When you enable DHCP Server, the IAD sequentially displays and processes the required configuration commands beginning with Enable DHCP Server.

To enable or disable DHCP Server, follow the steps below:

- 1 Type "C" on the DHCP Server Configuration menu to select Enable/Disable DHCP. If DHCP Relay is enabled, the IAD prompts you to disable DHCP Relay because DHCP Server and DHCP Relay cannot be configured at the same time. If DHCP Relay is not enabled, the IAD prompts you to enable or disable DHCP server.
- 2 Type "E" to enable DHCP Server, to type "D" to disable DHCP Server and proceed to Step 1 in the next section.

## Enable/Disable Checking Additional DHCP Servers

When the IAD boots, you may configure the internal DHCP server to check for additional DHCP servers on the LAN. If an external DHCP server is discovered, the IAD-based DHCP service is disabled. To enable or disable checking for external DHCP servers, follow the steps below.

- 1 Type "D" DHCP Server Configuration menu to select Enable/Disable Checking for Additional DHCP Servers. The IAD prompts you to enable/disable Checking for Additional DHCP Servers.
- 2 Type "E" to enable checking, or D to disable checking.
- 3 Proceed to Step 1 under Configuring DHCP Server Parameters below.

## Configure DHCP Server Parameters

- 1 Type "I" on the DHCP Server Configuration menu, or continue from the Checking Additional DHCP Servers section above. The IAD displays the gateway address and prompts you to enter a new one.
- 2 Type the IP address of the gateway and press Enter. If there is no gateway available, type the address of the Ethernet port. The IAD displays the current DNS Server address and prompts you to enter a new DNS Server IP address.
- 3 Type the new DNS Server address, or type 255 . 255 . 255 . 255 to use a DNS Server assigned from another port. Press Enter to continue. The IAD displays the current NetBIOS Server address and prompts you to enter a new NetBIOS Server IP address.
- 4 Type the IP address of the new NetBIOS Server and press Enter. The IAD displays the current Subnet Mask and prompts you to enter a new one.
- 5 Type the new subnet mask and press Enter. The IAD displays the current Domain name and prompts you to enter a new one.
- 6 Type the new domain name and press Enter. The IAD displays the current Lease Time and prompts you to enter a new DHCP Lease Time.

- 7** Type the new Lease Time value in seconds, and press Enter. The IAD displays the NetBIOS Type Configuration menu.
- 8** Type the option for the NetBIOS node type, and press Enter.
- 9** Press Escape to return to the DHCP Server Configuration menu and continue configuring DHCP Server.

## **Configure DHCP Address Range Pool**

You must configure the DHCP address range pool to set the range of IP addresses to return to the DHCP clients. All IP addresses must be on the same subnet.

To configure the DHCP address range pool, follow the steps below:

- 1** Type "P" on the DHCP Server Configuration menu to select Configure DHCP Address Range Pool. The IAD displays the current High IP address and prompts you to enter a new one.
- 2** Type the new High IP address and press Enter. The IAD displays the current Low IP address and prompts you to enter a new one.
- 3** Type the new Low IP address and press Enter. The IAD displays the DHCP Server Configuration menu.

## **Configure DHCP Client Entry**

You can configure up to 10 static DHCP client entries by following the steps below.

- 1** Type "C" on the DHCP Server Configuration menu to configure DHCP Client Entry settings. The IAD displays the gateway address and prompts you to enter the Client entry number to configure.
- 2** Type the client entry number you're configuring, and press Enter. The IAD displays the current Mac address for this entry and prompts you to enter a new one.
- 3** Type the MAC address in the template provided. The IAD displays the current Host name and prompts you to enter a new one.
- 4** Type the new host name and press Enter. The IAD displays an update option. Type "Y" to override the Lease Time default for this entry, "N" to use the default value, or proceed to Step 5.
- 5** Type the lease time for this entry and press Enter. The IAD displays an update option. Type "Y" to override the IP address default value, "N" to use the default value, or proceed to Step 6.
- 6** Type the IP address for this entry and press Enter. The IAD displays an update option. Type "Y" to override the Subnet Mask address default value, "N" to use the default value, or proceed to Step 7.

- 7 Type the Subnet Mask for this entry and press Enter. The IAD displays an update option. Type "Y" to override the default gateway, "N" to use the default value, or proceed to Step 8.
- 8 Type the default gateway address for this entry and press Enter. The IAD displays an update option. Type "Y" to override the DNS Server IP address default value, "N" to use the default value, or proceed to Step 9.
- 9 Type the default DNS Server IP address for this entry and press Enter. The IAD displays an update option. Type "Y" to override the NetBIOS Server IP address default value, "N" to use the default value, or proceed to Step 10.
- 10 Type the default NetBIOS Server IP address for this entry and press Enter. The IAD displays an update option. Type "Y" to override the NetBIOS Node Type default value, "N" to use the default value, or proceed to Step 11.
- 11 Type the default NetBIOS node type for this entry and press Enter. The IAD saves the configuration.

## Display DHCP Configuration

Type "F" on the DHCP Server Configuration menu to display the current configuration of the DHCP Server:

```
DHCP Server on T1/E1 port 1
Checking for additional DHCP Servers is disabled.
Default gateway: None Default DNS server: None
Default NetBIOS server: None
Default subnet: 255.255.255.0 Default lease: 3600 seconds
Domain name:
Low address: 0.0.0.0 High address: 0.0.0.0
```

Each field is described in the table below.

Field	Description
Net Interface	active slot number.
Default gateway	IP address of packets sent to DHCP Clients.
Default DNS server	IP address of the DNS server.
Default subnet	IP subnet mask; number of bits reserved for host ID.
Domain name	defines the entity that owns the IP address. For example, commengines.com.
Default lease	length of time to keep the Internet connection active.
High address	maximum IP address to assign.
Low address	minimum IP address to assign.
Client Number	client entry number.
Host name	name of the host.
IP address	IP address of outgoing interface.

Field	Description
Subnet mask	IP subnet mask; number of bits reserved for host ID.
Lease time	length of time to keep the Internet connection active.
Gateway	IP address of packets sent to destination.
DNS Server	IP address of the DNS server.

When you have finished viewing the information, press any key to return to the DHCP Server Configuration menu (Figure 4.108).

## Display DHCP Server Statistics

Type "S" on the DHCP Server Configuration menu to display DHCP Server statistics. The IAD displays the following information about the DHCP Server.

Statistics
plain bootp requests received
plain bootp replys sent
discover packets sent
offer packets sent
dhcp request packets received
declines received
releases received
acks sent
nacks sent
requests for other servers
protocol errors

For the IAD to display this information, you must attach DHCP Client devices that use DHCP to obtain an IP address from the IAD.

## Display DHCP Server Assigned and Unassigned Addresses

Type "A" on the DHCP Server Configuration menu to display DHCP Server Assigned Addresses, or type "U" to display DHCP Server Unassigned Addresses. The IAD displays the following information about the DHCP Server assigned addresses:

Field	Description
IP	IP address of the device, assigned by the IAD.

Field	Description
Client ID	Ethernet MAC address for the device.
Status	How the IP address is assigned to the device—via DHCP or manually.

For the IAD to display this information, you must attach DHCP Client devices that use DHCP to obtain an IP address from the IAD.

## Display DHCP Entry Details

Type “D” on the DHCP Server Configuration menu to display DHCP entry details. The IAD displays the following information about the DHCP entries:

Value	Description
IP address	IP address of the device.
Client ID	Ethernet MAC address for the device.
Status	how the IP address is assigned to the device—via DHCP server, or manually.
Subnet	IP subnet mask; number of bits reserved for host ID.
Gateway	IP address of packets sent to destination.
DNS	P address of the DNS server.
Lease	length of time to keep the Internet connection active.
Type	type of IP address: static or dynamic.
Name	name of the device.

For the IAD to display this information, you must attach DHCP Client devices that use DHCP to obtain an IP address from the IAD.

## Delete a DHCP Client Entry

To delete a DHCP Client Entry, follow the steps below.

- 1 Type “X” on the DHCP Server Configuration menu to delete a DHCP client entry.
- 2 Type the number of the client entry to delete and press Enter. The IAD deletes the client entry from the table and saves the new configuration.

## Delete a DHCP Assignment Entry

To delete a DHCP Assignment Entry, follow the steps below.

- 1 Type “Y” on the DHCP Server Configuration menu to delete a DHCP Assignment Entry. The IAD prompts you for the DHCP entry index number to delete.

- 2 Type the index number to delete and press Enter. The IAD deletes the assigned IP address from the Display DHCP Server Assigned Addresses command and saves the new configuration.

## Multicast Configuration

---

Multicast (point-to-multipoint) is a communication feature that allows a source host to send a message to a group of destination hosts. Multicasting reduces traffic on the local network by sending only one (multicast) packet out to a higher-bandwidth relay point.

Multicasting differs from broadcasting in that a receiver must join a multicast group to receive group messages. Each multicast group has its own group address, which is a Class D IP address—224.0.0.0—239.255.255.255.

### Multicast Configuration Menu

Type “M” on the Main menu (Figure 2.2) to display the Multicast Configuration menu.

**Figure 4.109** *Multicast Configuration Menu*

```
*****
*           Multicast Configuration Menu           *
*****
E. Enable/Disable Global IP Multicasting
P. Config PIM - Dense Mode by Port
S. Add/Change Multicast Route Source
G. Show IGMP Group
Q. Show IGMP Querier
M. Show Multicast Routing Table
N. Show PIM Neighbor
```

The Multicast Configuration menu contains commands to configure IP Multicast Routing. The IAD displays the Multicast Configuration menu only when DHCP Server is enabled and the IAD has been reset.

When you have completed multicast configuration, reset the IAD for the changes to take effect.

### Enable/Disable Global IP Multicasting

To enable or disable global IP Multicasting, follow the steps below:

- 1 Type “E” on the Multicast Configuration menu (Figure 4.109) to select Enable/Disable Global IP Multicasting.
- 2 Type “E” to enable IP multicasting, or type “D” to disable it. The IAD saves the new configuration and displays the Multicast Configuration menu.

You must enable Multicast Routing to send, receive, and route IP multicast packets. Otherwise, multicast packets are dropped automatically.

## Configure PIM – Dense Mode by Port

- 1 Type "P" on the Multicast Configuration menu to configure Protocol-Independent Multicast (PIM) version dense mode by port and interface. The IAD displays the available interfaces and prompts you to select one as shown in Figure 4.39.
- 2 Type the option number to select the interface. The IAD displays the port table for this interface and prompts you to select a port.
- 3 Type the port to configure and press Enter. The IAD displays the PIM status for this port and prompts you to enable or disable PIM.
- 3 Type "E" to enable PIM on this port, or type D to disable it. The IAD saves the new configuration and displays the Multicast Configuration menu.

## Add/Change Multicast Route Source

Reverse Path Forwarding (RPF) checks the IP address of the sender of the packet and then finds the best outgoing interface from its normal IP routing table.

Type "S" on the Multicast Configuration menu to add or change the Multicast Route Source. The IAD displays the Multicast Routing Source menu:

Figure 4.110 Multicast Routing Source Menu

```
*****  
*      Multicast Routing Source Menu      *  
*****  
A. Add a Multicast Routing Source  
R. Remove a Multicast Routing Source  
S. Show Multicast Routing Source  
.
```

### Adding a Multicast Routing Source

- 1 Type "A" on the Multicast Routing Source menu to add a Multicast Routing Source. The IAD creates a multicast routing source and adds it to the Multicast Routing Source Table. The IAD prompts you to enter an IP address for the Source.
- 2 Type the Source IP address and press Enter. The IAD displays the current subnet mask and prompts you to enter a new one.
- 3 Type the new subnet address and press Enter. The IAD displays the available interfaces and prompts you to select one as shown in Figure 4.39.
- 4 Type the option number to select the interface. The IAD displays the port table for this interface and prompts you to select a port.
- 5 Type the port to configure and press Enter. The IAD saves the new configuration and displays the Multicast Configuration menu.

### Remove a Multicast Routing Source

To remove a Multicast Routing Source, follow the steps below.

- 1 Type "R" on the Multicast Routing Source menu. The IAD prompts you to enter an IP address for the Source.

- 2 Type the source IP address and press Enter. The IAD displays the current subnet mask and prompts you to enter a new one.
- 3 Type the new subnet address and press Enter. The IAD displays the available interfaces and prompts you to select one as shown in Figure 4.39.
- 4 Type the option number to select the interface. The IAD displays the port table (sample shown above) for this interface and prompts you to select a port.
- 5 Type the port to delete and press Enter. The IAD The IAD permanently removes the multicast routing source from the Multicast Routing Source Table and displays the Multicast Configuration menu.

**Show Multicast Routing Source** To display the Multicast Routing Source, follow the steps below.

- 1 Type "S" on the Multicast Routing Source menu to display the Multicast Routing Source Table.

```

NETWORK ADDRESS      NETMASK      INCOMING INTERFACE
*****
0.0.0.0              0.0.0.0      192.168.xxx.xxx  192.168.xxx.xxx  1  default

```

- 2 Press any key to continue.

## Show IGMP Group

IGMP is a communication protocol that operates between a router (The IAD) and its local subnet (Ethernet-connection) hosts. The router sends periodic IGMP query packets to the subnet to check for any hosts that have joined or would like to join a group.

- 1 Type "G" on the Multicast Configuration Menu to display the IGMP Group. The IAD displays all Internet Group Management Group (IGMP) groups for each interface and their expiration times.

### IGMP Groups

Interface 10/100BaseT Ethernet:

```

224.0.0.1 (Default Local Join) Expires: NEVER
224.0.0.2 (Default Local Join) Expires: NEVER
224.0.0.13 (Default Local Join) Expires: NEVER

```

- 2 Press any key to continue.

## Show IGMP Querier

The IGMP Querier is the IGMP router that has the highest IP address among the others. It sends periodic IGMP Query messages and handles IGMP Membership Report and Leave messages.



- 1 Type "Q" on the Multicast Configuration menu to display the IGMP Querier. The IAD displays the IGMP Querier for each interface and its expiration time:

**IGMP Querier**

**Interface 10/100BaseT Ethernet:**  
**140.242.59.65 (this interface)**

- 2 Press any key to continue.

## Show Multicast Routing Table

Type "M" on the Multicast Configuration menu to display the Multicast Routing Table. The IAD displays the following information:

```
( Source, Group )
( * , 230.253.84.168)Expires: 130s
  Incoming interface: Null, RPF Neighbor 0.0.0.0
  Outgoing interface list:
  SDSL VPI/VCI 0*38
  10/100BaseT Ethernet
(Source, Group)
( * , 237.152.172.93)Expires: 42s
  Incoming interface: Null, RPF Neighbor 0.0.0.0
  Outgoing interface list:
  SDSL VPI/VCI 0*38
```

Field	Description
Source	IP address of the sender/source.
Group	IP address of the multicast group (Class D IP address).
State	Pruned or Expired. Pruned means that the state sent a Prune message to the upstream neighbor, asking them to stop sending Multicast Group messages to this interface. Expired means expiration time for the Prune state.
Expires	Expiration timer for the multicast routing state.
Static Mroute	The source is a user-assigned Multicast Routing Source.
Incoming interface	Incoming interface for the multicast packet.
RPF Neighbor	IP address of the upstream PIM neighbor.

Field	Description
Outgoing Interfaces	List of the outgoing interfaces to which the multicast packet will forward.
Pruned	If an outgoing interface is Pruned, this means that the interface received a PIM Prune message.

Since Multicast packets are forwarded according to the preceding information, this table is the key for IP Multicasting.

## Show PIM Neighbor

- 1 Type "N" on the Multicast Configuration menu to display the PIM Neighbor. The IAD displays the neighbor for each interface and its expiration times.
- 2 Press any key to continue.

## NAT Configuration

---

This section describes the steps required to configure Network Address Translation (NAT).

NAT multiplexes traffic from the internal network and presents it to the Internet as if it is from a single source that has only one IP address.

The NAT Local Server may be configured with a range of both TCP and UDP ports, which benefits applications including video conferencing and multi-user games.

Setting up IP networks without NAT may be complex—each requires an IP address, subnet mask, a DNS address and a default router.

NAT reduces this complexity by

- Modifying IP addresses and checksum without affecting traffic
- Automatic network configuration when using DHCP
- Packet-level filtering and routing
- Traffic logging




---

**NOTICE:** *If you enter an element of NAT information incorrectly, the network connection will not function and there may be no indication of what is wrong.*

---

Refer to the NAT Application Note in *Appendix C* for further information.

## NAT Configuration Menu

Enabling and managing NAT involves several tasks. These are all displayed and accessed on the NAT Configuration menu, which is displayed by typing "N" on the Main menu (Figure 2.2).

Figure 4.111 NAT Configuration Menu

```
*****
*           NAT Configuration Menu           *
*****
P. Enable/Disable NAT Translation by Port
T. Configure NAT TCP Timeout
U. Configure NAT UDP Timeout
R. Configure NAT Port Range
N. Configure NAT Local Server Entry
A. Configure NAT Alias Entry
F. Display NAT Configuration
S. Display NAT Statistics
C. Display NAT Connection Table
D. Display NAT Connection Details
O. Display NAT Local Server Table
E. Display NAT Alias Table
X. Delete IP Address from NAT Tables
Y. Delete NAT Local Server Entry
Z. Delete NAT Alias Entry
```

You may sign on as Supervisor or Network Manager to configure NAT. Options that display in the NAT Configuration menu depend on your security level. The menus shown are at the Supervisor security level.

---

**NOTICE:** *You must reset the IAD when you have finished making changes to NAT configuration for configuration changes to take effect.*

---

The table below lists the default NAT settings.

Parameter	Range	Default
NAT Translation by Port	Enabled   Disabled	Disabled
NAT TCP Timeout	60 to 3600 seconds	300 seconds
NAT UDP Timeout	60 to 3600 seconds	120 seconds
NAT port range – low end	5000 to 65534	5000
NAT port range – high end	50000 to 65535	65535

A significant advantage of NAT is that you can configure it without changing hosts or routers, other than those few routers on which NAT is configured. NAT multiplexes internal network traffic and presents it to the Internet as if it is from a single source with one IP address.

## Enable/Disable NAT Translation by Port

Each IAD is configured with NAT disabled. To enable NAT translation, follow the steps below.

- 1 Type "P" on the NAT Configuration menu. If at least one virtual circuit on the WAN exists and the LAN port is also configured with an IP address, or more than one PVC/DLCI exists, the IAD displays the interfaces (sample following) on this IAD as shown in Figure 4.39. Otherwise, the IAD displays the WAN port table and prompts you to select a port.
- 2 Type the port number on which to enable NAT and press Enter. The IAD prompts you to enable or disable NAT.
- 3 Type "E" to enable NAT, or "D" to disable. The IAD saves the setting and displays the NAT Configuration menu.
- 4 Continue with other NAT configuration tasks, or press Escape to return to the Main menu.

## Configure NAT TCP and UDP Timeouts

Under normal circumstances, the timeout default setting is adequate. However, if users interact with products including multiple-player IP games or video conferencing, you may need to configure the timeout.

The local server protocol you select determines which timeout to configure. TDP and UDP are similar, except that TCP tracks TCP clients on a per-connection basis and removes them from the table as soon as the connection closes.

To configure a NAT timeout, follow the steps below.

- 1 On the NAT Configuration menu, type "T" to select TCP connections, or type "U" to select UDP connections. The IAD displays a TCP or UDP prompt.
- 2 Type the timeout value and press Enter. The IAD displays the NAT Configuration menu.
- 3 Continue with other NAT configuration tasks, or press Escape to return to the Main menu (Figure 2.2).
- 4 Reset the IAD.

## Configure NAT Port Range

The size of the NAT port range defines the number of simultaneous connections permitted. A small port range limits the number of connections. Since the range that you assign must be outside the range of assigned ports, do not set port ranges below 5,000.

Under normal circumstances, the port range default setting is adequate. However, if you interact with products including multiple-player IP games or video conferencing, you need to configure the port range setting.

To multiplex several connections to a single destination, the IAD assigns all packets unique port numbers. Each IP packet starts with a header that contain

the source and destination addresses, as well as two port numbers. The addresses specify the two routers at each end, while the two port numbers ensure the unique identification of each router pair.

When the IAD sends TCP or UDP connection from a local port to an Internet port, it changes the sent IP address to the address of the Internet port. Similarly, it changes the TCP or UDP connection port number to a unique value within the NAT port range.

You can display the NAT settings with the Display NAT Local Server Table command.



---

**NOTICE:** *Ensure that the NAT port range does not include any ports that use applications such as HTTP, TFTP, and so on.*

---

To configure the NAT port range, follow the steps below:

- 1 Type "R" on the NAT Configuration menu to select the Configure NAT Port Range. The IAD displays the low-end port range and prompts you to enter a Low-end value.
- 2 Type the Low-end value and press Enter. The IAD displays the High-end port range and prompts you to enter a value.

**Enter High End of NAT Port Range (50000..65534): (50000)**

- 3 Type the High-end value and press Enter. The IAD saves the configuration and displays the NAT Configuration menu.
- 4 Continue with other NAT configuration tasks, or press Escape to return to the Main menu.

## Configure NAT Local Server Entry

To configure the NAT local server entry, follow the steps below:

- 1 Type "N" on the NAT Configuration menu to select Configure NAT Local Server Entry. The IAD prompts you to enter a NAT Local Server.
- 2 Type the number of the Local Server entry and press Enter. The IAD displays the current IP address and prompts you to enter a new one.

Type the local server translated IP address and press Enter. The IAD displays the Protocol Configuration menu. The protocol may be unknown, or it may be set.

**Figure 4.112** NAT Local Server Protocol Configuration Menu

```
*****  
*      NAT Local Server Protocol Configuration Menu      *  
*****
```

Current NAT Local Server Protocol is Unknown

1. TCP
2. UDP
3. ESP (IPSec)
4. AH (IPSec)
5. Both TCP and UDP

- 4 Type the option number of the protocol (usually TCP or UDP) to use. The IAD displays the menu with the new status message.
- 5 Press Escape to continue. The IAD prompts you to enter the Translated Port number:
- 6 Type the translated port number (range = 1-65535) and press Enter. The IAD prompts you to enter the Local Server Standard Port number:
- 7 Type the Standard Port Number (range = 1-65535) and press Enter. If you did *not* choose TCP and UDP for protocol, the IAD displays the following message:

```
Updating NAT Local Server entry 1, Translated IP address  
95.4.4.4  
Translated Port 100 is accessible as Standard Port 65535
```

If you chose TCP and UDP for protocol, the IAD prompts you to enter the number of consecutive ports to use.

- 8 Type the number of consecutive ports to use and press Enter. The IAD displays a port report, saves the NAT configuration, and displays the NAT Configuration menu.
- 9 Continue with other NAT configuration tasks, or press Escape to return to the Main menu.

## Configure NAT Alias Entry

Each NAT alias entry allows a device on the LAN (inside of NAT) to be accessible from the Internet via a unique IP address. The IAD only translates IP addresses for alias entries—port numbers are not changed.

You can create up to seven direct public-to-private IP address mappings via the NAT alias table.

First, assign each public IP address using option C – Configure Port IP Address on the Router Configuration menu (Figure 4.60) – to entries 1 through 7 on the PVC or DLCI with a 255.255.255.255 subnet mask. Next, make alias entries to map each local IP address to a corresponding public IP address.

These NAT alias entries allow IP traffic to the public IP address to pass directly through, port for port, to the corresponding private IP address.

To configure each NAT alias entry, follow the steps below.

- 1 Type "A" on the NAT Configuration menu to select Configure NAT Alias Entry. The IAD displays the next unassigned entry and prompts you to enter the NAT Alias Entry to configure.
- 2 Type the number of the alias entry to configure. The IAD displays the current local IP address and prompts you to enter a new NAT Alias Local IP Address.
- 3 Type the IP address of the device on the LAN. (It must be a statically assigned IP address; do not use DHCP to assign this address.) The IAD displays the current Internet IP Address and prompts you to enter a new one.
- 4 Type the new NAT alias IP address and press Enter. The IAD displays the information you've entered and updates the configuration.
- 5 When the operation is complete, press any key to display the NAT Configuration menu.
- 6 Continue with other NAT configuration tasks, or press Escape to return to the Main menu.

## Display NAT Statistics

When NAT is enabled, you can review statistics gathered as NAT operates. To display NAT statistics, type "S" on the NAT Configuration menu. Press any key to return to the NAT Configuration menu.

Report Entry	Description
Timeouts	TCP and UDP Timeout values.
Local to inet	Number of packets and bytes transferring to the Internet.
inet to Local	Number of packets and bytes receiving from the Internet.
Connections	Number of active TCP, UDP and ICMP connections, as well as the number created and deleted.
Total Fragments	Total fragments: local to internet, and internet to local
First Fragments	Number of first fragments: local to internet, and internet to local
Queued Fragments	Number of queued fragments: local to internet, and internet to local
Deleted Fragments	Number of queued fragments: local to internet, and internet to local
Fragment Entries	Number of created and deleted fragment entries.
Errors	Number of checksum, retries and bad packets.
Total IP packets	Number of IP packets—reserved addresses and discarded packets.

## Display NAT Connection Table

When NAT is enabled, you can display the current open connections. To display the connection table, type "C" on the NAT Configuration menu. The IAD displays the NAT connection table.

The IAD will advise you if there are no open connections. Press any key to return to the NAT Configuration menu.

Report Entry	Description
TCP/UDP/ICMP, etc.	IP address:Port—IP address plus port number of the foreign device; zero if ICMP protocol. IP address:Port:—IP address plus port number of the local (LAN) device; zero if ICMP protocol. These two values are separated by the symbol <->
out_port	Port number assigned by NAT which is translated by NAT to/from the local port.
pkts	Out: packets sent from the local device to the foreign device. In: packets sent from the foreign device to the local device.
state	TCP state number (TCP only)
idle	Idle time in seconds for the connection

## Display NAT Connection Details

When NAT is enabled, you can display details about a specific connection.

- 1 To display the connection details, type "D" on the NAT Configuration menu and enter the public IP address. The IAD prompts you for the outside port number of the connection.
- 2 Type the outside port number and press Enter. The IAD displays the NAT connection details. The IAD will advise you if there are no connections open.
- 3 Press any key to return to the NAT Configuration menu.

Report Entry	Description
Foreign IP	IP address of the foreign device
Local IP	IP address of the local (LAN) device
Outside port	Port number assigned by NAT which is translated by NAT to/from the local port.
Inside port	Port number of the local (LAN) device; zero if ICMP protocol
Foreign port	Port number of the foreign device; zero if ICMP protocol
Outgoing packets/# bytes	Packets sent from the local device to the foreign device.
Incoming packets/# bytes	packets sent from the foreign device to the local device.



Report Entry	Description
Type	TCP or UDP
Seconds since use	Idle time in seconds for the connection
TCP/UDP Sequence	TCP sequence number
Ack	TCP ack number
State	TCP state number (TCP only)
Retrys: local, foreign:	local—TCP retransmissions from local device to foreign device. foreign—TCP retransmissions from foreign device to local device.
Bad checksum: local, foreign	local—packets with bad TCP checksums from local device. foreign—packets with bad TCP checksums from foreign device.

## Display NAT Local Server Table

When NAT is enabled, you can display the entries in the local server table.

- 1 To display the table, type "O" on the NAT Configuration menu.
- 2 Press any key to return to the NAT Configuration menu.

Report Entry	Description
Entry	Table entry number
Local IP Address	IP address in use
Local Port	local port number
Internet Port	Internet port number
Protocol	The protocol used—TCP or UDP

## Display NAT Alias Table

When NAT is enabled, you can display the entries in the NAT alias table. To display the table, type "E" on the NAT Configuration menu. Press any key to return to the NAT Configuration menu.

Report Entry	Description
Entry number	Table entry number (1 to 7)
Local IP Address	Local, or LAN IP address
Internet IP Address	Internet IP address assigned

## Delete IP Address from NAT Tables

To delete an entry from the NAT Tables, follow the steps below.

- 1 Type "X" on the NAT Configuration menu. The IAD prompts for the IP address.
- 2 Type the IP address to delete and press Enter. The IAD updates the table, and displays the NAT Configuration menu.

## Delete NAT Local Server Entry

To delete a local server entry, follow the steps below:

- 1 Type "Y" on the NAT Configuration menu. The IAD prompts for the entry number to delete.
- 2 Type the number of the table entry and press Enter. The IAD displays the following:

```
Deleting NAT Local Server entry 1, Translated IP address
115.3.3.1
Translated Port 2, Standard Port 3
```

The IAD updates the table, and displays the NAT Configuration menu.

## Delete NAT Alias Entry

To delete a NAT alias entry, follow the steps below.

- 1 Type "Z" on the NAT Configuration menu. The IAD prompts for the alias entry to delete.
- 2 Type the number of the entry and press Enter. The IAD updates the table, and displays the NAT Configuration menu.

# Setting PPP Options

---

When the IAD receives a TERM REQ from the upstream router, all PPP ports are configured, including PPP over HDLC (USI or T1), PPP over ATM, PPP over Frame Relay, and PPP over Ethernet over ATM. To access these PPP options, follow the steps below.

- 1 Select "Q" on the Main menu (Figure 2.2) to display the PPP Configuration menu (Figure 4.113).

**Figure 4.113** PPP Configuration

```
*****
*           PPP Configuration Menu           *
*****
```

PPP restart is currently upon output data.

```
D. Configure PPP to restart upon output data
I. Configure PPP to restart immediately
```

- 2 Select "D" to immediately restart PPP only after the IAD is ready to send data upstream.

- 3 Select "I" to immediately restart PPP upon receipt of a TERM REQ from the upstream router.

## Setting Derived Timing Options

---

Use the Derived Timing options to enable and disable Derived Timing.

### Derived Timing Menu

To configure Derived Timing settings, type "T" (Telephony Clock Recovery) on the Main menu (Figure 2.2), which will bring up the Derived Timing menu (Figure 4.114).

**Figure 4.114** *Derived Timing Menu*

```
*****  
*           Derived Timing           *  
*****  
1. Enable/Disable Derived Timing
```

Each of the options on this menu is described in detail below.

### Enable/Disable Derived Timing

When Derived Timing is enabled, the IAD adjusts its clock source based on the arrival rate of voice packets.

To enable or disable derived timing, follow these steps:

- 1 Type "1" on the Derived Timing menu. The IAD displays the current setting and prompts you to change it:
- 2 Type "Y" to change the current setting. The IAD saves the configuration and then displays the Derived Timing menu.
- 3 Press Escape to return to the Main menu.
- 4 Reset the IAD.



# REPORTS

This chapter describes the report subsystem in the IAD. The report subsystem allows you to display information about the current configuration of the IAD, and collect, display, and clear statistics on various network and media interfaces. You can also display reports about routing and bridging, and other reports about the operation of the IAD.

These reports are often helpful when troubleshooting. You can often determine what settings may be incorrect, or identify the source of a voice or data network problem.

## Reports Menu

---

To display the Reports menu, type "1" on the Main menu (Figure 2.2).

**Figure 5.1** *Reports Menu*

```
*****
*           Reports Menu           *
*****
C. Display Current Configuration
N. Display Network Statistics
I. Display Interface Statistics
M. Display Media Statistics
R. Display Route Table
A. Display ARP Table
B. Display Bridge Forwarding Database
S. Display Bridge Status
P. Display PPP Authorization Entries
U. Display System Uptime
O. Display Memory Statistic
E. Display Tasks Run Time
D. Display All Statistics
Z. Zero All Statistics
```

Most options on the Reports menu generate a specific report. However, the Network Statistics, Interface Statistics, and Media Statistics options display a menu of several related reports and commands to reset accumulated statistics.

To display a report or group of reports, or to clear statistics for a particular protocol or interface, select the option and refer to the details regarding each option below.



**NOTICE:** *When viewing a report, press any key to display the next page, or return to the Reports menu at the end of the report. Press Escape to return to the Reports menu at any time.*

## Current Configuration Report

To display the Current Configuration report, enter "C" on the Reports menu (Figure 5.1). The Current Configuration report displays configuration settings and information about the installed interfaces on your IAD.

Details are displayed for each of the IAD's ports and interfaces. The parameters are repeated, and not described again in the table.

The information displayed in the Current Configuration report is listed in the table below. The contents of this report vary based on the IAD configuration, interfaces, and ports.

Parameter	Description
Software version	version of IAD firmware
Serial Number	serial number of the IAD
Contains # DSP chip(s)	no. of DSP chips in the IAD
Derived Timing	Status: enabled   disabled
Routing Information Protocol	Status: enabled   disabled globally
Bridging	Status: enabled   disabled globally
Bridge Database Aging Time	1-3600 seconds (default 300 seconds)
Spanning Tree	enabled   disabled globally
Spanning Tree bridge priority	1-65,535 (default 32,768)
Spanning Tree hello time	1-10 seconds (default 2 seconds)
Spanning Tree max age	6-40 seconds (default 20 seconds)
Spanning Tree forward delay	4-30 seconds (default 15 seconds)
Simple Network Management Protocol (SNMP) (IP and EOC)	Status: enabled   disabled
SNMP System Contact	user-defined (maximum 39 characters)
SNMP System Name	user-defined (maximum 39 characters)
SNMP System Location	user-defined (maximum 39 characters)
SNMP Community	name must match the SNMP host (maximum = 39 alphanumeric characters); If SNMP is enabled and the SNMP Community Name is null, SNMP goes into read-only mode.
SNMP Trap Host IP Address	IP address of the SNMP trap host
Multicasting	Status: enabled   disabled

Parameter	Description
Telnet Server Port	port number of the Telnet server
DNS Server IP Address	IP address of the DNS server
DNS Server Timeout	current timeout value in seconds (5 to 20)
Application Information	loaded program files
Support File Information	loaded support files
Interface type	SDSL   T1/E1   ADSL   SHDSL   Ethernet
Admin state	Status: enabled   disabled
Physical state	online   offline
WAN DataLink Protocol	Totally Transparent   Raw HDLC   Cisco compatible HDLC   IP-Plus compatible HDLC   PPP (over Raw HDLC)   ATM   Frame Relay
xDSL Type	SHDSL Annex A (U.S.)   SHDSL Annex B (Europe)
ADSL Standard for Startup	T1.413   G.LITE   G.DMT   A;cate; 1.4   Multi-Mode   ADI   ALCATEL
SHDSL Mode	Customer Premises Equipment (CPE) or Central Office (CO)
SDSL Mode	Customer Premises Equipment (CPE) or Central Office (CO)
Firmware Version	version of firmware
Line Rate	Auto   Fixed   1152 kbps   768 kbps   384 kbps   192 kbps   2320 kbps or manually set
Payload Scrambling	enabled   disabled (ATM only)
Frame Relay Management	maintenance protocol (Frame Relay only)
T1/E1 Only	
T1 Frame Mode	ESF   D4
E1 Frame Mode	FAS   FASC (CRC4 enabled)   Multi-Frame CAS   Multi-Frame CAS (CRC4 enabled)
Binary 8 Zero Substitution (B8ZS)	enabled   disabled
Line Build Out	Distance in feet: 0 to 133   133 to 266   266 to 399   399 to 533   533 to 655   -7.5 dB   -15 dB   -22.5 dB
Tx Clock Source	external   internal
Tx Channels Enabled	
Rx Channels Enabled	
HDB3 coding	enabled   disabled
Payload Scrambling	enabled   disabled
Port #	
Sa4 Bit	set   cleared
Sa5 Bit	set   cleared

Parameter	Description
Sa6 Bit	set   cleared
Sa7 Bit	set   cleared
Sa8 Bit	set   cleared
Rcv Clk Source	Internal   External
RIP	enabled   disabled
Poisoned Reverse	enabled   disabled
Dynamic Host Configuration Protocol (DHCP) Client	enabled   disabled
Bridging	enabled   disabled
Spanning Tree	enabled   disabled
Port Priority	0-255 (default = 128)
Path Cost	1-65,535 (default = 32,768)
PPP Auth Type (WAN port)	None   PAP Client   PAP Server   CHAP Client   CHAP Server
Userid	PAP User ID
Password	PPP password
Peer Name	PPP peer name
DLCI—Frame Relay Only	RAW (No Encapsulation)   Proprietary Voice DLCI   RFC 1490   ATM RFC 1483 (Tunneling)
VPI/VCI—ATM Only	AAL5 (None)   AAL0 (None)   Proprietary Voice   RFC 1483 (using VC Muxing)   RFC 1483 (with LLC Encapsulation)   RFC 2364 (PPPoATM with LLC Encapsulation)   RFC 2364 (PPPoATM using VC Muxing)   AAL1/CES   AAL2/LES
MTU	maximum transmission unit per port
IP Interfaces on Port #	
ID	host ID
IPAddr	IP Addresses for the ID (maximum = 8)
IPMask	no. of bits reserved for host ID (max. 8)
Priority	NORMAL   HIGH
Ethernet address	Ethernet address (Ethernet)
Full duplex	Enabled   Disabled (Ethernet)

## Network Statistics Reports

The Network Statistics menu contains commands to display statistical information about the packets handled by the IP routing engine and information regarding higher level services, and to clear network statistics for specific protocols.

Type "N" on the Reports menu to display the Network Statistics menu:



**Figure 5.2** *Network Statistics Menu*

```

*****
*                    Network Statistics                    *
*****

C. Display ICMP Statistics
G. Display IGMP Statistics
I. Display IP Statistics
P. Display PIM Statistics
T. Display TCP Statistics
U. Display UDP Statistics
Z. Clear a Network Statistic
    
```

To display a specific report, enter the option. For detailed information about each report in the Network Statistics menu, or information on how to clear network statistics, proceed to the appropriate section below.

### ICMP Statistics Report

To display the Internet Control Message Protocol (ICMP) Statistics report, type "C" on the Network Statistics menu. The ICMP Statistics report displays details about ICMP received packets, sent packets, and queries, reports, and messages sent and received.

Parameter	Description
<b>Received Packet Information</b>	
packets received	Total ICMP packets received.
discarded for lack of resources	Discarded received packets due to lack of resources—kernel memory, packet buffers, etc.
discarded due to internal errors	Discarded received packets due to internal software errors.
discarded for other reasons: <ul style="list-style-type: none"> <li>- unrecognized codes</li> <li>- bad checksum</li> <li>- packets smaller than header</li> <li>- redirects from non-gateways</li> </ul>	Discarded packets due to these reasons:  Not used. Value of the Checksums field in header is incorrect. Size of the ICMP header is larger than the packet size. ICMP Redirect packet from non-gateway.
<b>Sent Packet Information</b>	
packets sent	Total ICMP packets sent.
discarded for lack of resources	Discarded transmitted packets due to lack of resources, such as kernel memory or packet buffers.
discarded due to internal errors	Discarded transmitted packets due to internal software errors.
with illegal type or code	Discarded transmitted packets due to internal errors.
Messages, Requests, and Replies Received	

<b>Parameter</b>	<b>Description</b>
Destination Unreachables received	No. of ICMP Destination Unreachable messages received.
Time Exceededs received	No. of ICMP Time Exceeded messages received.
Parameter Problems received	No. of ICMP Parameter Problem messages received.
Source Quenches received	No. of ICMP Source Quench message received.
Redirects received	No. of ICMP Redirect message received.
Echo Requests received	No. of ICMP Echo Request message received.
Echo Replies received	No. of Echo Reply messages received.
Timestamp Requests received	No. of ICMP Timestamp Requests messages received.
Timestamp Replies received	No. of ICMP Timestamp Replies messages received.
Information Requests received	No. of ICMP Information Requests messages received.
Information Replies received	No. of ICMP Information Replies messages received.
Other types received	No. of other ICMP types messages received.
<b>Messages, Requests, and Replies Sent</b>	
Destination Unreachables sent	No. of ICMP Destination Unreachable messages sent.
Time Exceededs sent	No. of ICMP Time Exceeded messages sent.
Parameter Problems sent	No. of ICMP Parameter Problem messages sent.
Source Quenches sent	No. of ICMP Source Quench message sent.
Redirects sent	No. of ICMP Redirect message sent.
Echo Requests sent	No. of ICMP Echo Request message sent.
Echo Replies sent	No. of ICMP Echo Reply messages sent.
Time-stamp Requests sent	No. of ICMP Timestamp Requests messages sent.
Time-stamp Replies sent	No. of ICMP Timestamp Replies messages sent.
Information Requests sent	No. of ICMP Information Requests messages sent.
Information Replies sent	No. of ICMP Information Replies messages sent.
Other types sent	No. of other ICMP types messages sent.

## **IGMP Statistics Report**

To display the Internet Group Message Protocol (IGMP) Statistics report, type "G" on the Network Statistics menu. The IGMP Statistics report displays details about IGMP received packets, sent packets, and queries, reports, and messages sent and received.

<b>Parameter</b>	<b>Description</b>
<b>Received Packet Information</b>	
packets received	Total IGMP packets received.

<b>Parameter</b>	<b>Description</b>
discarded for lack of resources	Discarded received packets due to lack of resources such as kernel memory or packet buffers.
discarded due to internal errors	Discarded received packets due to internal software errors.
discarded for other reasons: - unrecognized codes - bad checksums  - packets smaller than header	Discarded packets due to other reasons:  Not used Value of the Checksums field in header is incorrect.  Size of IGMP header is larger than packet size.
<b>Sent Packet Information</b>	
packets sent	Total IGMP packets sent.
discarded for lack of resources	Discarded transmitted packets due to lack of resources, such as kernel memory or packet buffers.
discarded due to internal errors	Discarded transmitted packets due to internal software errors.
with illegal type or code	Discarded transmitted packets due to internal errors.
<b>Queries, Reports and Messages Received</b>	
Membership Query received	No. of IGMP Membership Query messages received.
Ver. 1 Membership Report received	No. of IGMP Version 1 Membership Report messages received.
Ver. 2 Membership Report received	No. of IGMP Version 2 Membership report messages received.
Leave-group message received	No. of IGMP Leave Group messages received.
DVMRP routing message received	No. of IGMP DVMRP routing message messages received.
PIM routing message received	No. of IGMP PIM routing messages received.
Traceroute response received	No. of IGMP Traceroute resp messages received.
Mcast traceroute messages received	No. of IGMP Multicast Traceroute messages received.
Other messages received	No. of other IGMP type messages received.
<b>Queries, Reports and Messages Sent</b>	
Membership Query sent	No. of IGMP Membership Query messages sent.
Ver. 1 Membership Report sent	No. of IGMP Version 1 Membership Report messages sent.
Ver. 2 Membership Report sent	No. of IGMP Version 2 Membership report messages sent.
Leave-group message sent	No. of IGMP Leave Group messages sent.
DVMRP routing message sent	No. of IGMP DVMRP routing message messages sent.

Parameter	Description
PIM routing message sent	No. of IGMP PIM routing messages sent.
Traceroute resp sent	No. of IGMP Traceroute resp messages sent.
Mcast traceroute messages sent	No. of IGMP Multicast Traceroute messages sent.
Other messages sent	No. of other IGMP type messages sent.

## IP Statistics Report

To display the Internet Protocol (IP) Statistics report, type "I" on the Network Statistics menu. The IP Statistics report displays details about all IP packets sent and received on the network

Parameter	Description
<b>Received Packet Information</b>	
packets received	Total IP packets received.
packets delivered to upper layer	No. of incoming IP packets delivered to upper layer/ Layer 4 or higher (such as ICMP, IGMP, PIM, TCP and UDP packets)
packets forwarded	No. of incoming IP packets forwarded to other route/interface
discarded for lack of resources	Discarded received packets due to lack of resources: kernel memory, packet buffers etc.
discarded due to internal errors	Discarded received packets due to internal software errors.
discarded for other reasons:	Discarded received packets due to other reasons listed in the following:
- with header errors	Bad IP header format
- with an illegal source	Illegal Source IP address in the IP header
- with an illegal destination	Illegal Destination IP address in the IP header
- bad versions	Version field value in IP header is incorrect.
- bad checksums	Value of Checksum field in IP header is incorrect.
- with headers too small	Size of the IP header is less than 20 bytes.
- packets smaller than header	Size of IP header is larger than packet size.
- packets larger than frame	IP packet size is larger than internal packet buffer.
- with unrecognized protocol	Value of Protocol Type field in IP header is unrecognized.
- with zero TTL	Value of TTL in the IP header reaches zero.
fragments received	Value of Fragment field in the IP header is on.
fragmented packets reassembled	No. of reassembled fragmented packets.
fragments discarded	No. of discarded fragmented packets.

Parameter	Description
<b>Sent Packet Information</b>	
packets sent	Total IP packet sent.
discarded for lack of resources	Total transmitted IP packet discarded due to lack of resources: kernel memory, packet buffer, etc.
discarded due to internal errors	Total transmitted IP packet being discard due to internal errors.
destinations found unreachable	Destination IP address could not be reached for outgoing packet.
fragments sent	Total fragmented sent.
packets fragmented	Total outgoing IP packet being fragmented.
fragmentation failures	Total fragmentation failures for outgoing IP packets.

## PIM Statistics Report

To display the Protocol Independent Multicast (PIM) Statistics report, type "P" on the Network Statistics menu. The PIM Statistics report displays detailed information about PIM packets sent and received.

Parameter	Description
<b>Received Packet Information</b>	
packets received	Total PIM packets received.
discarded for lack of resources	Discarded received packets due to resources, such as kernel memory or packet buffers.
discarded due to internal errors	Discarded received packets due to internal software errors.
discarded for other reasons: - unrecognized codes - bad checksums - packets smaller than header	Discarded received packets due to: Packet header codes could not be recognized. Bad packet header checksums Packet header size is bigger than packet buffer size
<b>Sent Packet Information</b>	
packets sent	Total PIM packets sent.
discarded for lack of resources	Discarded transmitted packets due to lack of resources: kernel memory, packet buffers, etc.
discarded due to internal errors	Discarded transmitted packets due to internal software errors.
with illegal type or code	Discarded transmitted packets due to internal errors.
<b>Received Messages Information</b>	
Hello received	No. of PIM Hello messages received.
Register received	No. of PIM Register messages received.
Register Stop received	No. of PIM Register-Stop messages received.
Join/Prune received	No. of PIM Join/Prune messages received.

Parameter	Description
Bootstrap received	No. of PIM Bootstrap messages received.
Assert received	No. of PIM Assert messages received.
Graft received	No. of PIM Graft messages received.
Graft Ack received	No. of PIM Graft Acknowledgment messages received.
Cand RP Adv received	No. of PIM messages received.
other messages received	No. of PIM messages received.
<b>Sent Messages Information</b>	
Hello sent	No. of PIM Hello messages sent.
Register sent	No. of PIM Register messages sent.
Register Stop sent	No. of PIM Register-Stop messages sent.
Join/Prune sent	No. of PIM Join/Prune messages sent.
Boosters sent	No. of PIM Bootstrap messages sent.
Assert sent	No. of PIM Assert messages sent.
Graft sent	No. of PIM Graft messages sent.
Graft Ack sent	No. of PIM Graft Acknowledgment messages sent.
Cand RP Adv sent	No. of PIM messages sent.
other messages sent	No. of PIM messages sent.

## TCP Statistics Report

To display the Transport Control Protocol (TCP) Statistics report, type "T" on the Network Statistics menu. The TCP Statistics report displays detailed information about TCP packets sent and received.

Parameter	Description
<b>Received Packet Information</b>	
packets received	Total TCP packets received.
discarded for lack of resources	Discarded received packets due to lack of resources: kernel memory or packet buffers.
discarded due to internal errors	Discarded received packets due to internal software errors.
discarded for other reasons:	Discarded received packets due to other reasons listed in the following:
- with destination port zero	Destination port value in TCP header is zero.
- bad checksums	Checksum value in TCP header is incorrect.
- with headers too small	Size of the TCP header is less than 20 bytes.
- packets smaller than header	Packet size is less than the TCP header size.
- packets larger than frame	Packet is larger than the internal packet buffer.

<b>Parameter</b>	<b>Description</b>
- acks for unsent data	Unacceptable/invalid/unsent acknowledge number in the TCP header.
- with data outside window	The remote host has sent data beyond the window that the software could advertise.
- with data after close	TCP packets received in a Closed state/connection.
segments with data	Total segments received, including those received in error. This count includes segments received on currently established connections.
segments with duplicate data	No. of segments received with duplicate data.
segments with only an ACK	Not used
segments with a duplicate ACK	Not used
segments with a RST	No. of segments received with the RST (Reset) Flag bit on in the TCP header.
window probes	Not used
window updates	Not used
<b>Sent Packet Information</b>	
packets sent	Total TCP packets sent.
discarded for lack of resources	Discarded transmitted packets due to lack of resources: kernel memory or packet buffers.
discarded due to internal errors	Discarded transmitted packets due to internal software errors.
with illegal destination port	Destination port field value in TCP header is illegal.
segments with data	Total segments sent.
segments with retransmitted data	No. of retransmitted TCP data packet.
segments with only an ACK	Not used
segments with a delayed ACK	Not used
segments with a RST	No. of unsolicited reset (RST) segment sent.
window probes	Not used
window updates	Not used
active opens	No. of TCP connections opened.
passive opens	No. of TCP passive connections opened.
connections currently established	No. of TCP connections currently established.
connections gracefully closed	No. of TCP connections gracefully closed.
connections aborted	Not used
failed connection attempts	Not used

## UDP Statistics Report

To display the User Datagram Protocol (UDP) Statistics report, type "U" on the Network Statistics menu. The UDP Statistics report displays detailed information about UDP packets sent and received.

Parameter	Description
<b>Received Packet Information</b>	
packets received	Total UDP packets received.
discarded for lack of resources	Discarded received packets due to lack of resource—kernel memory, packet buffers, etc.
discarded due to internal errors	Discarded received packets due to internal software errors.
discarded for other reasons:	Discarded received packets due to other reasons listed in the following:
- with destination port zero	Destination Port field value in UDP header is zero.
- bad checksums	Checksum field value in UDP header is incorrect.
- packets smaller than header	Size of UDP header is less than 8 bytes.
- packets larger than frame	Packet size is less than the UDP header size.
- unopen ports	Packet is larger than the internal packet buffer.
<b>Sent Packet Information</b>	
packets sent	Total UDP packets sent.
discarded for lack of resources	Discarded transmitted packets due to lack of resources: kernel memory, packet buffers, etc.
discarded due to internal errors	Discarded received packets due to internal software errors.
with illegal destination port	Destination Port field value in UDP header is illegal.

## Clear Network Statistics

To clear network statistics, type "Z" on the Network Statistics menu. The IAD displays the Clear Network Statistics menu:

**Figure 5.3** *Clear Network Statistics Menu*

```

*****
*                               Clear Statistics                               *
*****

C. Clear ICMP Statistics
G. Clear IGMP Statistics
I. Clear IP Statistics
P. Clear PIM Statistics
T. Clear TCP Statistics
U. Clear UDP Statistics

```



To permanently reset statistics for a specific protocol, type the option. The IAD immediately resets all statistics for the specified protocol, and displays the menu.

Continue resetting network statistics, or press Escape to return to the Network Statistics menu.

## Interface Statistics Reports

Type "I" on the Reports menu to display the Interface Statistics menu. This menu contains commands to display information about the packets handled between layer 2 and layer 3 on a per-port basis, and to clear statistics for specific protocols.

To display specific interface statistics, follow the steps below.

- 1 Select an interface and optionally a port. The IAD then displays the report. The IAD displays the interfaces from which you may choose on this IAD.

```
*****
*                               *
*           Interface Statistics           *
*****

I. Display Interface Statistics
B. Display Bridge Statistics
A. Display ATM PVC Statistics
Z. Clear a Statistic
```

- 2 Select the interface. The IAD displays the port table and prompts you to select a port.

```
Port      DLCI      Encapsulation
----      -
1         32         RFC 1490

Select Port: [1-8]
```

- 3 Type the port number and press Enter. The IAD displays the Interface Statistics menu:



---

**NOTICE:** *The commands that display on the Interface Statistics menu vary, based on the WAN module and configuration of the IAD.*

---

**Figure 5.4** *Interface Statistics Menu (With IAD Configured for Frame Relay)*

```
*****
*                               *
*           Interface Statistics           *
*****

I. Display Interface Statistics
B. Display Bridge Statistics
D. Display DLCI Statistics
Z. Clear a Statistic
```

**Figure 5.5** Interface Statistics Menu (With IAD Configured for ATM)

```

*****
*                               *
*                               *
*****

I. Display Interface Statistics
B. Display Bridge Statistics
A. Display ATM PVC Statistics
Z. Clear a Statistic
    
```

**4** To display a specific report, type the option. For detailed information about each report in the Interface Statistics menu, or for information on how to clear interface statistics, proceed to the appropriate section below.



**NOTICE:** When viewing Interface Statistics reports, press the space bar to display the next page. When have finished viewing, press any key to display the report, or press Escape to return to the Interface Statistics menu.

### Display Interface Statistics



**NOTICE:** For T1/E1 Physical Layer Statistics, refer to T1 Configuration Menu on page 4-11.

To display the Interface Statistics report, type “I” on the Interface Statistics menu. This report provides details about all packets sent and received on the selected interface.

Parameter	Description
<b>Received Packet Information</b>	
packets received	No. of packet received from this interface.
discarded for lack of resources	Discarded received packets due to lack of resources: kernel memory or packet buffers.
discarded due to internal errors	Discarded received packets due to internal software errors, such as lack of packet buffer.
discarded for other reasons	Discarded received packets due to other reasons, such as lack of packet buffer.
<b>Sent Packet Information</b>	
packets sent	No. of packet sent from this interface.
discarded for lack of resources	Discarded transmitted packets due to lack of resources: kernel memory or packet buffers.
discarded due to internal errors	Discarded transmitted packets due to internal software errors, such as lack of packet buffer.
discarded for other reasons	Discarded transmitted packets due to other reasons, such as lack of packet buffer.
<b>Packets Received by Type</b>	

Parameter	Description
octets rcvd	Total octets/bytes received from interface.
unicast rcvd	No. of Unicast Packets received from interface
multicast rcvd	No. of Multicast Packets received from interface
broadcast rcvd	No. of Broadcast Packets received from interface
<b>Packets Sent by Type</b>	
octets sent	Total octets/bytes sent from interface.
unicast sent	No. of Unicast Packets sent from interface
multicast sent	No. of Multicast Packets sent from interface
broadcast sent	No. of Broadcast Packets sent from interface

## Display DLCI Statistics

To display the DLCI Statistics (Data Link Connection Identifier) report, Type "A" on the Interface Statistics menu shown in Figure 5.4.

This option is displayed only when Frame Relay is selected as the data link protocol.

Parameter	Description
Committed Burst	No. of committed info rate (bytes per measurement interval)
Excess Burst	No. of excess info rate (bytes per measurement interval)
Throughput	Expected average throughput (bytes/second)
Rx Frames	No. of frames received.
<b>Received Frame Information</b>	
Rx Bytes	Total data received in bytes.
Rx Discarded Frames	No. of discarded received frames due to: - Received Frames are larger than size of PDU - Received Frames Headers are smaller than the standard HDLC header size. - Validity of address bits settings in HDLC header is incorrect. - Checksum Field value in header is incorrect. - The received DLCI number does not match the DLCI connections on the IAD.
Rx FECN	No. of FECN = 1 frames received.
Rx BECN	No. of BECN = 1 frames received.
Rx DE	No. of DE = 1 frame received
Rx Excess Rate	No. of frames received within excess info rate
Rx Committed Rate	No. of frames received within committed info rate
<b>Transmitted Frame Information</b>	

Parameter	Description
Tx Frames	No. of frames transmitted.
Tx Bytes	No. of data transmitted in bytes.
Tx Discarded Frame	No. of discarded received frames due to: - Transmitted Frames are larger than the size of the PDU - Packets overflow.
Tx FECN	No. of FECN = 1 frames transmitted.
Tx BECN	No. of BECN = 1 frames transmitted.
Tx DE	No. of DE = 1 frame transmitted
Tx Excess	No. of frames transmitted within excess info rate
Tx Committed	No. of frames transmitted within committed info rate

## Display ATM PVC Statistics

To display the PVC Statistics Reports, type "A" on the Interface Statistics menu as shown in Figure 5.5. This option is displayed only when ATM is selected as the data link protocol.

The reports below are available, depending on the specification of the PVC:

### *AAL2 Statistics Report*

This PVC Report displays when an AAL2/LES PVC is configured.

Parameter	Description
Transmit overflows	Discarded packets due to the internal queue reached its maximum size.
Receive STF parity errors	No. of STF (Start Field) parity error received.
Receive sequence errors	Sequence number in header is incorrect for cells received.
Bad rx OSF sequence errors	Value of OSF sequence in header is incorrect for cells received.
Bad OSF value errors	Value of OSF in the header is incorrect.
Receive HEC errors	Value of HEC (Header Error Compression) in the header is incorrect.
Receive overlap HEC errors	HEC (Header Error Compression) value overlapped.
Receive CID errors	Value of CID (Channel ID) in header received is incorrect.
Transmit CID errors	Value of CID (Channel ID) in header sent is incorrect.

### ***Cumulative CPCS-2 Statistics Report***

This report displays when the AAL2/LES PVC is configured.

<b>Parameter</b>	<b>Description</b>
Maximum PDU Size	Maximum CP-5 Rx frame length (in bytes, without CPCS trailer)
Transmit bytes counter	Total AAL2 Cells sent in bytes.
Transmit microcell counter	Total AAL2 Cells sent.
Tx discarded microcells errors	No. of transmitting cell discarded due to: - Invalid Microcell Channel - The Microcell is empty - Length of the cell is larger than the PDU size - Transmitted cell overflow - Cell Allocation Problem
Tx too long microcell errors	Length of transmitting cells is larger than PDU size.
Tx reserved UUI errors	Value of UUI (User-to-User information) in the header of the cells transmitted is incorrect.
Receive bytes counter	Total AAL2 Cells received in bytes.
Receive microcell counter	Total AAL2 Cells received.
Rx discarded microcells errors	No. of receiving cells discarded because: - Invalid Microcell Channel - The microcell is empty - The cell length is larger than the PDU size - Transmitted cell overflow - Cell Allocation Problem
Rx too long microcells errors	The length of the cells received is larger than the PDU size.
Rx reserved UUI errors	Value of UUI (User-to-User information) in the header of the cells received is incorrect.
Rx reassembly errors	No. of errors of reassembling AAL2 cells: -Could not allocate an internal Cell buffer -Value of STF (Start Field) in the header is incorrect. -Value of the Sequence Number in the header is incorrect (out of sequence).

### ***Common AAL Statistics Report***

This report displays when ATM protocol is configured.

<b>Parameter</b>	<b>Description</b>
Vcc	Number the VCC (VPI/VCI value)
Status	Current status of this AAL connection. The status is the addition of the values: Connection Active: 1 Connection Confirm: 16 Connection Created: 32 Connection Congestion: 2 For example, if status is 33, the connection is Active and Created.
Max PDU	Max. PDU size limitation for this AAL connection.
Rx Frames	No. of frames received.
Rx Cells	No. of AAL cells received.
Rx Bytes	Total data in bytes received.
Rx Error Cells	No. of received cells are dropped due to: -Connection is not established/closed. -Could not allocation internal cell buffer -Value of STF (Start Field) in header is incorrect. -Cells Overflow (the internal queue for storing the cell reaches it maximum size). -Cells Re-Assembly Errors -CRC checksum errors.
Rx Error Frames	No. of received frames are dropped due: -Could not allocation internal cell buffer -Cells Overflow (the internal queue for storing the cell reaches it maximum size) -Frames re-assembly errors -Re-assembly timeout -CRC checksum errors.
Tx Frames	Total frames transmitted.
Tx Cells	Total cells transmitted.
Tx Bytes	Total data transmitted in bytes.
Tx Discarded	No. of discarded transmitting cells due to: -Could not allocation internal cell buffer -Cells Overflow (the internal queue for storing the cell reaches it maximum size) -Connection is not established/closed -Transmitting frame is empty -size of frame is larger than the PDU size.

Parameter	Description
Tx OverFlow	Transmitted Cells Overflow. The internal SAR transmitting queue for storing the cell reached its maximum size (64), so it can not hold more outgoing cell.
Tx UnderFlow	Out of cells for transmit. Internal cell buffer could not be allocated for transmitting cells.
Tx Inactive	Discarded Transmitted Cells because the connection is not established   disconnected   closed.
Rx Inactive	Discarded Received Cells because connection not established   disconnected   closed.
CRC 32 Errors The size	AAL5 only. CRC-32 header checksum in is wrong.
Reassembly Timeouts	No. of SAR reassembly timeouts. Frames could not be reassembling and discarded.
Frames too Long	Frame size is larger than the max. size of PDU.

### ***IP Header Compression Statistics Report***

This report is available when ATM PVC Encapsulation Type RFC 1483 is selected, an IP address is assigned and IP Header Compression is enabled on the ATM Interface.

Parameter	Description
Missed TCP contexts	No. of times search didn't find a TCP stream.
Missed RTP context	No. of times search didn't find an RTP stream.
<b>Sent Packet Information</b>	
Compressed TCP packets sent	No. of compressed TCP packets sent.
Compressed UDP packets Sent	No. of compressed UDP packets sent.
Compressed RTP packets Sent	No. of compressed RTP packets sent.
FULL_HEADER packets Sent	No. of FULL_HEADER packets sent.
CONTEXT_STATE packets sent	No. of CONTEXT TATE packets sent.
<b>Received Packet Information</b>	
Compressed TCP packets received	No. of compressed TCP packets received.
Compressed UDP packets received	No. of compressed UDP packets received.
Compressed RTP packets received	No. of compressed RTP packets received.
FULL_HEADER packets received	No. of FULL_HEADER packets received.

Parameter	Description
CONTEXT_STATE packets Received	No. of CONTEXT_STATE packets received.
<b>Incorrect Sequence Numbers by Packet Type</b>	
TCP packets with wrong sequence number	No. of compressed TCP packets received with bad sequence number.
UDP packets with wrong sequence number	No. of compressed UDP packets received with bad sequence number.
RTP packets with wrong sequence number	No. of compressed RTP packets received with bad Sequence Number.
<b>Average Header Sizes</b>	
Ave. sent TCP header	The average size of the TCP header sent.
Ave. sent UDP header	The average size of the UDP header sent.
Ave. sent RTP header	The average size of the TCP header sent.
Ave. received TCP header	The average size of the TCP header received.
Ave. received UDP header	The average size of the UDP header received.
Ave. received RTP header	The average size of the RTP header received.

### ***PPP Statistics Report***

This report is available when ATM PVC Encapsulation Type RFC 2364 is selected.

Parameter	Description
<b>Received Packet Information</b>	
packets received	Total PPP packets received.
discarded for various reasons	Discard received packets due to: - Could not allocate PPP packet from internal queue. - Discarded all non-LCP packets until link is opened. - Discarded all non-AP packets until link is authenticated - Value of Length field in the header is zero
LCP rejects	No. of LCP Rejects messages received.
- echoes	No. of LCP Echoes messages received.
- replies	No. of LCP Replies messages received.
- discards	No. of LCP Discards messages received.
<b>Sent Packet Information</b>	
packets sent	Total PPP packets sent.
discarded (link not open)	Discarded transmitted packets because links are not opened.
LCP rejects	No. of LCP Rejects messages sent.
- echoes	No. of LCP Echoes messages sent.



Parameter	Description
- replies	No. of LCP Replies messages sent.
- discards	No. of LCP Discards messages sent.

## Display Bridge Statistics

To display the Bridge Statistics report, type "B" on the Interface Statistics menu. This report provides details about all packets sent and received on the IAD bridge.

Parameter	Description
<b>Received Packet Information</b>	
bridge packets received	Total of bridge packet received from interface.
bridge octets received	Total bridge octets/bytes received from interface.
discarded for lack of resources	Discarded received packets due to lack of resources: kernel memory or packet buffers.
bridge packets received and discarded	Discarded received packets due to lack of packet buffers or Spanning Tree packets arrived on an interface, when Spanning Tree is not enabled.
bridge packets sent to one other port	No. of bridge packets sent to a proper low-level output port.
bridge packets sent to all other ports	No. of bridge packets sent to all other bridge ports.
<b>Sent Packet Information</b>	
bridge packets sent	Total bridge packets sent.
bridge octets sent	Total octets/bytes of bridge packets sent.
discarded for lack of resources	Discarded transmitted packets due to lack of resources (kernel memory, packet buffers, etc.)
<b>Packets Received by Type</b>	
spanning tree config packets received	No. of Spanning Tree Configuration packets received.
spanning tree topology change packets received	No. of Spanning Tree Topology Change packets received.
spanning tree invalid packets received	No. of invalid Spanning Tree packets, such as Wrong LSAP, Control, Protocol ID, Version, Length, and Message Type value.
spanning tree config packets sent	No. of Spanning Tree Configuration packets sent.
spanning tree topology change packets sent	No. of Spanning Tree Topology Change packets sent.

## Clear Interface Statistics

To clear interface statistics, type "Z" on the Interface Statistics menu. The IAD displays the Clear Statistics menu:

**Figure 5.6** *Clear Interface Statistics Menu*

```
*****  
*                               Clear Statistics                               *  
*****  
  
  I. Clear Interface Statistics  
  B. Clear Bridge Statistics  
  A. Clear ATM PVC Statistics
```

To reset statistics for a specific interface, type the option.

The IAD immediately resets the statistics for the specified interface, and displays the menu. Continue resetting statistics, or press Escape to return to the Interface Statistics menu.



---

**NOTICE:** *You must enable bridging for the Clear Bridge Statistics option to display. For more information on enabling bridging, refer to Bridge Configuration Menu on page 4-54.*

---

## Media Statistics Reports

Media statistics reports display statistical information about the total packets handled (Layer 2) on a per-port basis. Reports on physical connections vary, based on the type of connection. To display specific media statistics, select an interface to display the statistics as shown in the steps below:

- 1 Type "M" on the Reports menu to display Media statistics reports. The IAD displays the interfaces on this IAD.

```
Available Interfaces :  
  1. G7070 ADSL ATU-R  
  2. 10/100BaseT Ethernet  
  3. 8-Line POTS  
  0. (Abort)
```

- 2 Type the number of the interface. With the interface chosen, the IAD displays the Media Statistics menu.



---

**NOTICE:** *The commands that display on the Media Statistics menu vary, based on the WAN module and configuration of the IAD. In the sample below, the IAD is configured for ATM.*

---



Parameter	Description
Tx Frames	No. of frames transmitted
Tx Bytes	No. of total bytes transmitted
Tx Frames discarded	No. of Frame Relay packets discarded due to: - Transmitted frames are larger than PDU size. - Packets overflow.
DE set on Tx	Indicates Discard Eligibility is allowed on transmitted frames, based on congestion, to maintain committed information rate.
FECN set on Tx	Forward Explicit Congestion Notification status set to notify DTE that congestion avoidance should be initiated by IAD.
BECN set on Tx	Backward Explicit Congestion Notification status set to notify DTE that congestion avoidance should be initiated by the sending device.
Tx congestion counter	No. of frames dropped due to congestion to maintain committed information rate.
CLLM frames Tx	No. of CLLM frames received
LMI frames Tx	No. of LMI frames received
ANSI frames Tx	No. of ANSI frames received
Last error:	Description of last recorded error since reset.

## Display ATM Statistics

This report displays basic ATM transport statistics at the cell level for all ports and PVCs.

Field	Description
The link has been up for X hours X minutes X seconds	Total time for the current time has been established.
Cells Rx	No. of valid ATM cells received.
CLPI Rx	No. of cells received with CLPI (Cell Loss Priority Indication) bit is on.
OAM Rx	No. of OAM (Operation And Maintenance) cells received.
EFCI Rx	No. of cells received with EFCI (Explicit Forward Congestion Indication) bit is on.
RM Rx	No. of RM (Resource Management) cells received.
Rx Cells Discarded	No. of received packets discarded due to: - Unknown VPI/VCI numbers - Bad Cell headers - Size of cells received is larger than PDU size - other reasons as required.

<b>Field</b>	<b>Description</b>
Cells Tx	No. of valid ATM cell sent.
OAM Tx	No. of cells transmitted with CLPI (Cell Loss Priority Indication) bit is on.
CLPI Tx	No. of OAM (Operation And Maintenance) cells transmitted.
EFCI Tx	No. of cells transmitted with EFCI (Explicit Forward Congestion Indication) bit is on.
RM Tx	No. of RM (Resource Management) cells transmitted.
Rx HEC Errors	No. of cells receives with HEC errors in the header.
Lost Cell Delineation (OCD)	No. of times cell delineation was lost.
Time in OCD	Amount of time in OCD condition
ATM Sync	Current ATM Synchronization status—Established or Lost.

## Display G7070 ADSL Statistics (81xx)

This report displays ADSL statistics.

<b>Parameter</b>	<b>Description</b>
Operational Seconds	Total kernel time (in seconds) link was operational.
Downstream SNR Margin	Current rate of downstream signal-to-noise ratio margin.
Downstream Attenuation	Current rate of downstream attenuation.
Upstream Attenuation	Current rate of upstream attenuation.
Near-End FEC	Count of near-end forward error correction.
Near-End CRC	Count of the near-end interleaved symbols with cyclic redundancy check errors.
Near-End SEF	Count of near-end severely errored frames.
Near-End LOS	Count of near-end loss of signal frames.
Far-End FEC	Count of far-end forward error correction.
Far-End CRC	Count of far-end cyclic redundancy check.
Far-End SEF	Count of far-end severely errored frames.
Far-End LOS	Count of far-end loss of signal frames.
Near-End CRC Last	Number of seconds of cyclic redundancy check error counts.
Near-End CRC Last	Number of minutes of cyclic redundancy check error counts.
Failure Counters Overall	Total overall failure frames.
Local SEF	Count of local (near-end) severely errored frames.

Parameter	Description
Local LOS	Count of local (near-end) loss of signal frames.
Remote SEF	Count of remote (far-end) severely errored frames.
Remote LOS	Count of remote (far-end) loss of signal frames.
ADSL Standard	Current status of the ADSL standard in use.

## Display G2237 xDSL Statistics (85xx)

This report shows xDSL status indicators.

Parameter	Description
Operational State	Current operation state.
Start Progress	Current start progress.
Operational Seconds	Total Operation Time in Seconds
Up/Down Counter	No. of times modem has come up.
Received SNR	No. of SNR (Signal-to-Noise Ration) received.
Mean SQ Error	No. of mean SQ error used to compute received signal to noise ratio.
Initial Received SNR	No. of the Initial Received SNR (Signal-to-Noise Ration)
Loop Attenuation	Current level of Loop Attenuation
Actual PSD Mask	Actual PSD mask is used for the line code comparison. It is acknowledged that an optimized PSD mask can be decided only after line code decision is made. The transmit power back-off of remote HTU
Framer Sync	Current framer synchronization status: In-Sync / Out of Sync
LOSW Status	Current status of LOSW (Loss of Sync Defect): ON / OFF
Total Seconds	Total seconds of statistics gathering.
Errored Seconds	Total errored seconds received of CRC and LOSW errors found.
CRC Count	No. of CRC errors (near end) received.
LOSW Defect Count	No. of LOSW Defect (Loss of Sync Defect) errors received.
FEBE Count	No. of Far End Block Error Count (far end).

Parameter	Description
Tip/Ring	Current status of Tip/Ring: Normal / Reserved.
Transmit Power	Nominal transmit power.
Receiver Gain	Current no. of total receiver gain.
SHDSL	
Remote Country Code	Current Remote Country Code.
Remote Provider Code	Current Provider Code.
H.DSL2	
Remote HDSL2 Version	Current version of the Remote HDSL2.
Remote Country Code	Current Remote Country Code.
Provider Code	Current Provider Code.
Remote Vendor Data Low	Remote vendor provided data (the low 4 bytes)
Remote Vendor Data Hi	Remote vendor provided data (the high 4 bytes)
Data Mode Heartbeat	Total Data Mode Heartbeat received. (Handle Modem Data state)
Framer Sync Lost Tick	No. of time that framer synchronization was lost

### Display Serial (USI) Statistics (8216s/8224s/8316s/8324s/8512s/8516s/8524s)

Type "S" to display the Serial Statistics report. This report displays basic serial (HDLC) transport statistics on the Universal Serial Interlace port.

Parameter	Description
bytes rcvd	Total data received in bytes.
packets rcvd	No. of Serial packets received.
discarded, RX Busy	No. of discarded received packets due to packets Overrun.
Available Buffers (PCB Entries)	Current available internal PCB (Packets Buffers) entries.
discarded, RX error:	No. of discarded due to the following reasons:- Could not allocate packet buffers.
Rx Clock glitch	Total frames discarded on this port due to receives clock glitch errors.
PLL error	Total frames discarded on this port due to receives phase lock loop errors.
Frame too long	Total frames discarded on this port because the received frame was too long.

Parameter	Description
Non octet aligned	Total frames discarded on this port because the received frame was not an integral no. of octets.
Abort seq	No. of frames aborted on the port due to receiving an abort sequence since system re-initialization and the port state was 'up' or 'test'.
CRC error	Total frames discarded on this port due to received CRC errors.
Rx overrun	Total frames discarded on this port due to receiver overruns errors.
CD lost	Total frames discarded on this port due to lost Carrier Detect.
Out Of Buffers (PCBs)	No. of times that could not allocate a packet buffer for received packets.
Lack of resources	Discarded received packets because a PCB for Transmitted/Received Pool Buffers could not be allocated.
bytes sent	No. of Data sent in bytes.
packets sent	No. of packets sent.
discarded, TX ring full	No. of packets discarded because Transmitted Ring Pool is full.
discarded, bad pkt or link not ready	Discarded received packets due to: - The status of the interface is not Online - Transmitted packet length is larger than interface.
discarded, TX error	No. of outgoing packet being discarded due to Clock glitch, and other transmission errors.
Tx Clk glitch	Total frames discarded on this port due to transmitter clock glitch errors.
Tx underrun	No. of times that there are no packets waiting in the Transmitted Ring Buffer.
CTS lost	Total frames discarded on this port due to transmitter CTS lost errors.

## Display Ethernet Statistics

This report displays Ethernet statistics.]

Parameter	Description
<b>Received Packet Information</b>	
packets rcvd	Total Ethernet packets received.
discarded, RX ring empty	Discarded received packets because the internal Received Packet Ring Pool Buffers are empty; therefore no incoming packets could be processed.
discarded, unrecognized protocol	Protocol Type field value in Ethernet header does not correspond to IP.



<b>Parameter</b>	<b>Description</b>
discarded, RX error	No. of discarded received packets due to the following reasons:
alignment errors	Frames containing a no. of bits not divisible by eight is received and discarded.
bad fcs	Received frame contains CRC errors in the header.
runt	Received frame is smaller than the minimum defined for this interface.
giant	Received frame lengths are greater than maximum defined for this interface.
late collision	Discarded frames because a collision occurred during frame reception. No. of times that a collision is detected on a particular interface later than 512 bit-times into the transmission of a packet.
overrun	Discarded received packets due to the internal Received Packet Ring Pool are full; therefore no incoming packets could be processed.
<b>Sent Packet Information</b>	
packets sent	Total Ethernet packets sent.
discarded, TX ring full	Discarded outgoing packets due to internal Transmitted Packet Ring Pool Buffers are full. Could not process any outgoing packets.
discarded, bad pkt	Length of outgoing packets is larger than the maximum length of this interface.
discarded, TX error	No. of discarded transmitted packets due to:
heartbeat lost	No. of transmitting Heartbeat (signal-quality error) packets lost/errors.
deferred	A count of frames for which the first transmission attempts on a particular interface is delayed because the medium is busy. The count represented by an instance of this object does not include frames involved in collisions.
late collision	Discarded transmitted frames because a collision occurred. No. of times that a collision is detected on a particular interface later than 512 bit-times into the transmission of a packet.
excessive collision	A count of frames for which transmission on a particular interface fails due to excessive collision
carrier sense lost	No. of times that the carrier sense condition was lost or never asserted when attempting to transmit a frame on a particular interface. The count represented by an instance of this object is incremented at most once per transmission attempt, even if the carrier sense condition fluctuates during a transmission attempt.

Parameter	Description
underrun	DMA underrun. Discarded outgoing packets because there are no packets waiting in the buffer.
transmitter resets	No. of transmitted packets after an error occurred

## Display POTS Statistics

This report displays POTS statistics.

Parameter	Description
Line X Active/Inactive	Current status of line X. Active: Phone line connection is up. Inactive: Phone line connection is down.
Buffers Rcvd	No. of packets received from this POTS line.
Buffers Sent	No. of packets sent to this POTS line.
Discarded	Discarded packets due to Jitter Buffer Overrun. The internal Jitter Buffer is full and could not allocate a new free packet buffer.
Underrun	Discarded packets due to there are no packets waiting in the Jitter buffer.

## Clear Media Statistics

To clear network statistics, type "Z" on the Network Statistics menu. The IAD displays the Clear Network Statistics menu, giving you the option of clearing the statistics related to the IAD's specific datalink protocol and WAN configuration (i.e., ATM Statistics, Frame Relay DLCI Statistics, etc.).

To permanently reset statistics for a specific protocol, type the option. The IAD immediately resets all statistics for the specified protocol.

Continue resetting network statistics, or press Escape to return to the Network Statistics menu.

## Route Table Report

Type "R" in the Reports menu to display the Route Table report. The IAD lists each route by IP address, and displays the information listed in the table below regarding statically configured routes and dynamically learned ones.

Parameter	Description
Network Destination	network destination address
Netmask	IP subnet mask; no. of bits reserved for the host ID
Gateway Address	IP address of packets sent to destination
Interface	IP address of outgoing interface

Parameter	Description
Metric	no. of hops (routers) required to reach the specified gateway
Type	static   dynamic   RIP   local

## ARP Table Report

Address Resolution Protocol (ARP) obtains the Ethernet Media Access Control (MAC) address for a known IP address.

Type "A" on the Reports menu to display the information shown in the table below about mappings between Ethernet Media Access Control (MAC) addresses (hardware addresses) and IP addresses.

Parameter	Description
IP Address	IP address that corresponds to the MAC address
Ethernet Address	Ethernet address of the device; assigned by the manufacturer
Interface	The interface for the Ethernet address

## Bridge Forwarding Database Report

To display information about mappings between Ethernet addresses and devices connected to the LAN, type "B" on the Reports Menu. The IAD displays the shown in the table below.

Parameter	Description
Ethernet Address	Ethernet address of the device; assigned by the manufacturer
Interface	Interface for the Ethernet address
Port	Port for the Ethernet interface
Timer	No. of seconds until this entry deletes from the database. The time counts down from the bridge database aging time value, in one-second intervals; at zero, the entry deletes from the database.

You must enable bridging for this information to display. For more information on enabling bridging, refer to *Bridge Configuration Menu* on page 4-54.

## Bridge Status Report

To display information about bridging, type "S" on the Reports Menu. The IAD displays a record for each interface as shown in the table below.

Parameter	Description
Interface	interface for the active slot for bridging
Port	port for the preceding interface
Spanning Tree Protocol (STP)	enabled   disabled
State	Spanning tree state: disabled   blocking   listening   learning   forwarding
Root	root port for the bridge—yes   no
Designated	designated port for the bridge—yes   no
Timers	current values of the spanning state timer (first value) and the hello timer (second value)

The spanning state timer value is for listening or learning states and counts down from the forward delay time to zero.

The hello timer value is valid only if the active port is the Root Bridge of the network. It counts down from the hello time to zero.

- Root priority – priority of the root bridge on the network.
- ID – Ethernet MAC address of the root bridge on the network.

Press any key to return to the Reports menu.

## PPP Authorization Entries Report

Type "P" on the Reports menu to display information about PPP authorization entries. If no PPP authorization entries have been created, the IAD displays a message to confirm this.

Otherwise, the information shown in the table below is displayed for each entry.

Parameter	Description
Authorization type	None   Password Authentication Protocol (PAP) Client   PAP Server   Challenge Handshake Authentication Protocol (CHAP) Client   CHAP Server
Slot #/Interface #/Port #	active slot for the PPP interface
Userid/Password/Peer Name	values for the PPP interface

Press any key to return to the Reports menu.

## System Uptime Report

Type "U" on the Reports menu to display the amount of time elapsed since the IAD was reset.

Press any key to return to the Reports menu.

## Memory Statistics Reports

Type "O" on the Reports menu to display the Memory Statistics menu. The Memory Statistics menu (1-O) contains two memory display commands:

**Figure 5.8** *System Memory Statistics Menu*

```
*****
*                               Memory Statistic Menu                               *
*****
M. Display System Memory Statistic
T. Display Kernel Tasks Memory Statistic
```

To display a specific memory statistic report, type the option. For details, refer to the appropriate section below.

### Display System Memory Statistics

Type "M" on the Memory Statistics menu to display the System Memory Statistics report. The System Memory Statistics report displays the following details about system memory.

**Figure 5.9** *Memory Statistics Menu*

```
Total Memory Size:                8192 KB (8388608 Bytes)
Total Allocated Memory:            6214 KB (6363416 Bytes)
Total Free Memory:                 1977 KB (2025192 Bytes)

Kernel Memory Size:               1280 KB (1310720 Bytes)
  Kernel Memory Allocated:         847 KB ( 868256 Bytes)
    Allocated Blocks:              331 Blocks
    Largest Allocated Block Size:  159 KB ( 163248 Bytes)
    Highest Memory Used:           939 KB ( 962319 Bytes)
  Kernel Free Memory:              377 KB ( 386792 Bytes)
    Free Blocks                     6 Blocks
    Largest Free Block Size         372 KB ( 381720 Bytes)
Reserved Area Size:               1024 KB (1048576 Bytes)
```

When you have finished reviewing the report, press any key to return to the System Memory Statistics menu (Figure 5.8).

### Display Kernel Tasks Memory Statistics

Type "T" on the Memory Statistics menu to display the Kernel Tasks Memory Statistics report. The System Memory Statistics report displays

details about the kernel tasks. Six are shown in this sample report; usually 24 or more run concurrently.

**Figure 5.10** *Kernel Tasks Memory Statistics Menu*

**Total Running Kernel Tasks: 30**

**Kernel memory allocated by each tasks**

TASK 0	Allocated Size:	106 KB ( 109456 Bytes)
TASK 1	Allocated Size:	493 KB ( 504848 Bytes)
TASK 2	Allocated Size:	0 KB ( 208 Bytes)
TASK 3	Allocated Size:	10 KB ( 10832 Bytes)
TASK 4	Allocated Size:	96 KB ( 99280 Bytes)
TASK 5	Allocated Size:	5 KB ( 5728 Bytes)
TASK 6	Allocated Size:	62 KB ( 64416 Bytes)
TASK 7	Allocated Size:	9 KB ( 9488 Bytes)
TASK 8	Allocated Size:	2 KB ( 2112 Bytes)
TASK 9	Allocated Size:	3 KB ( 3536 Bytes)
TASK 10	Allocated Size:	4 KB ( 4112 Bytes)
TASK 11	Allocated Size:	2 KB ( 2080 Bytes)
TASK 12	Allocated Size:	4 KB ( 4128 Bytes)
TASK 13	Allocated Size:	4 KB ( 4128 Bytes)
TASK 14	Allocated Size:	4 KB ( 4128 Bytes)
TASK 15	Allocated Size:	2 KB ( 2080 Bytes)
TASK 16	Allocated Size:	11 KB ( 11696 Bytes)
TASK 17	Allocated Size:	17 KB ( 18128 Bytes)

## Tasks Run Time

Type "E" on the Reports menu to display the Performance Reports menu (). These reports show CPU utilization and run time for the software tasks.

**Figure 5.11** *Performance Reports Menu*

```
*****
*           Performance Reports Menu           *
*****
  1. Display CPU utilization 10s
  2. Display CPU utilization 100s
  3. Display Tasks Run Time
```

Option 1 displays the time the CPU is in the idle loop. You may view option 2 in either 1-second or 10-second granularity. Option 3 displays the percent of time used for individual tasks.

## Zero All Statistics

Type "Z" on the Reports menu to reset all statistics and redisplay the menu. This command allows you to reset all statistics using one command. To reset specific statistics, use the clear statistics command in each report.

Press any key to return to the Reports menu (Figure 5.1).

# COMMAND LINE INTERFACE

## Introduction

---

The command line interface (CLI) is often more convenient to use than the menu interface. Many of the tasks you normally perform using the menu interface are also available in the command line interface.

To enter CLI mode, type "C" on the Main menu (Figure 2.2). The IAD enters command mode and allows you to enter IAD commands (described below) until you type the `exit` or `quit` command to return to the menu interface.

Any time you use the menu or CLI to make setting changes, or change any of the physical characteristics of the IAD (such as changing the MAC address of the Ethernet port), you must reset (or restart) the IAD for the new settings to take effect. An alternative to issuing the reset command is to simply turn off (or unplug) the IAD, and power it back on, forcing it to reboot.

## CLI Help

Display a list of all commands in the CLI by typing `help` at the prompt. To display the parameters for a specific command, type `command`, followed by a question mark (?). For example, `set wan ip address?`.

### Command Line Syntax

The CLI supports the following syntax:

```
command <required parameters> (optional parameters)
```

For example:

```
set wan ip address 192.3.4.5 255.255.255.0 2 0 0 1
```

The required parameters are IP address <192.3.4.5> and netmask <255.255.255.0>. The optional parameters are the slot (2), interface (0), port (0) and connection (1).

The command and its parameters are NOT case sensitive.

For the commands listed below, the following will apply:

**Slot** will always be 0 to 3, where 0 is the WAN port, 1 is the Ethernet port, 2 is the USI port and 3 is the POTS port.

**Interface** will always be 0.

**Port** will always be from 0 to 7 except for the POTS CLI command where the values can range between 0 to 23 (the upper-level number is dependant on the number of POTS ports associated with the specific IAD).

**Connection** will always be 0 to 7.

**exit** Quits the command line interface and returns to the menu system.

`exit`

**update entire system** Updates all the software in the IAD. This command is typically used to install a new software release. It does *not* affect the configuration file.

`update entire system <IPaddress>`

**IPaddress**

IP address of the TFTP server.

**rename file** Changes the name of a file.

`rename file <old name> <new name>`

**old name**

File name of existing file

**new name**

New name of file.

**tftp receive** Receives a file from the TFTP server identified by the IP address. The file must exist in the default directory of the TFTP server.

`tftp receive <IP address> <file name>`

**IP address**

IP address of TFTP server.

**file name**

name of file to receive.

**ping** Pings an IP address. The IP address must be on the same subnet. Press Escape to premature halt the test. Upon termination, displays a summary table.

`ping <IP address> (size) (tries)`

**IP address**

IP address of destination in decimal format (999.999.999.999)

**size**

Packet size, in number of bytes (0-1450, default 32)

**tries**

Number of attempts (0-1000, 0 is continuous; default 4 tries)

**tracerte** Used to trace the route of an IP address.



tracerte (IPaddress)  
**IPaddress**  
 Displays ping times between hops.

**reset system** Performs a soft system reset.  
 reset system

**set system defaults** Sets the system to the default parameters.  
 set system defaults

**set password** Sets the password for the IAD.  
 set password <user | netman | supervisor> <password>  
**user | netman | supervisor**  
 Password level.  
**password**  
 Password for the IAD

**set hostname** Sets the hostname of the IAD.  
 Set hostname <name>

**set domain** Sets the domain name of the network to which the IAD is connected.  
 Set domain name <name>

**set time offset** Sets the offset from Greenwich Mean Time (GMT). For example, for Pacific Standard time, you would type in an offset of -8.  
 set time offset <hours (-12 -14)> (minutes (0-59))

**set time string** Defines the time zone.  
 Set time string <time zone name>  
**time zone name**  
 Text field for any description

**set radius server** Programs the address of the RADIUS Server. (Use to determine the validity of unknown user ID/password pairs in the IAD. Verilink does not provide a RADIUS Server; user must provide a RADIUS Server to use this feature.)  
 Set radius server <1 or 2> <server address>  
**1 or 2**  
 Allows primary for 1 or secondary for 2.  
**server address**  
 IP address of RADIUS Server

**set radius secret** Changes the primary or secondary RADIUS encryption key.  
 Set radius secret <1 or 2> <secret>  
**1 or 2**

Allows primary for 1 or secondary for 2.

**secret**

RADIUS encryption key

**set voice gateway** Configures which voice gateway to use.

```
set voice gateway <name>
```

Name	Gateway Name
callctrl	Jetstream
cucomcpe	CopperCom
sip_rg	SIP 1.0
mg_rg	MGCP 1.0
les_elcp	AAL2/LES CCS-ELCP
aal2les	AAL2/LES CAS
tbcpe	TollBridge
tdsoft	TdSoft

**set ip route** Sets a static IP route.

```
set ip route <IP Route> <netmask> <Gateway IP Address>
```

**IP Route**

IP address in decimal format (999.999.999.999)

**netmask**

Subnet mask in decimal format (255.255.255.255)

**Gateway IP address**

IP address in decimal format (999.999.999.999)

**set ip default** Sets the default IP address.

```
route set ip default route <IP address>
```

**IP address**

IP address in decimal format (999.999.999.999)

**set bridge global** Enable or disables bridging globally.

```
set bridge global <on | off>
```

**on | off**

Keyword to enable (on) or disable (off) bridging globally.

**set bridge stp** Enables or disables Spanning Tree Protocol globally.

```
global set bridge stp global <on | off>
```

**on | off**

Keyword to enable (on) or disable (off) STP globally.

**set wan bridge** Enables and disables bridging on a WAN port.

- `set wan bridge <on | off> (slot) (interface) (port)`  
**on | off**  
 Keyword to enable (on) or disable (off) bridging on the specified port.
- set wan stp bridge** Enables and disables Spanning Tree Protocol on the specified WAN port.  
`set wan stp bridge <on | off> (slot) (interface) (port)`  
**status**  
 on | off. on enables STP; off disables STP.
- set wan ip address** Sets the WAN IP address. If you do not enter any optional parameters, it finds the first available slot, interface, port and connection.  
`set wan ip address <IPaddress> <netmask> (slot) (interface) (port) (connection)`
- set wan rip** Enables and disables RIP on a WAN IP port. If you do not enter any optional parameters, it will find the first available slot, interface and port.  
`set wan rip <on | off> <version (1, 2Bcst, | 2Mlti)> (slot) (interface) (port)`  
**on | off**  
 Keyword to enable (on) or disable (off) RIP on the specified port.  
**version 1 | 2Bcst | 2Mlti**  
 Keyword identifying version to implement. (Must be preceded by keyword *version*)
- set wan datalink** Sets the datalink protocol to Frame Relay or ATM. If you don't enter optional parameters, it finds the first available slot, interface and port.  
`set wan datalink <framerelay | atm> (slot) (interface) (port)`  
**framerelay | atm**  
 Keyword identifying datalink protocol.
- set wan framerelay dlci** Sets the Frame Relay DLCI number and encapsulation type to RFC1490 or RFC1483. If you do not enter any optional parameters, it finds the first available slot, interface, and port.  
`set wan framerelay dlci <dlci number> <1490 | 1483> (slot) (interface) (port)`  
**dlci number**  
 DLCI value (16 - 1023—default is 32 for data and 33 for voice)  
**1490 | 1483**  
 Encapsulation keyword
- set wan atm vc** Sets an ATM VC on a given WAN port—RFC 1483 and RFC 2364 VC Muxing PVCs, as well as LLC Encapsulation PVCs. You must specify VPI

number, VCI number and RFC encapsulation type. If you do not enter any optional parameters, it will find the first WAN slot, interface and port.

```
set wan atm vc <vpi> <vci> <1483 | 2364> (slot)
(interface) (port)
```

**vpi**

Virtual Port Identifier (0 - 255)

**vci**

Virtual Circuit Identifier (32 - 65535—default is 38 for data and 39 for voice)

**1483 | 2364**

Encapsulation keyword

**set wan atm ppp auth** Sets the PPPoATM options—RFC 2364 VC muxing PVCs, as well as LLC Encapsulation PVCs. If authorization is PAP or CHAP, you must specify an authentication type, UserID and password.

```
set wan atm ppp auth <NONE | PAP | CHAP> <ID>
<password> (slot) (interface) (port)
```

**NONE | PAP | CHAP**

Keyword to select authorization type.

**ID**

PPP user ID

**password**

PPP password

**set lan bridge** Enables or disables bridging on a LAN port.

```
set lan bridge <on | off> (slot) (interface) (port)
```

**on | off**

Keyword to enable (on) or disable (off) bridging on the specified port.

**netmask**

Subnet mask in decimal format (255.255.255.255)

**set lan stp bridge** Enables or disables Spanning Tree Protocol on a LAN port.

```
set lan stp bridge <on | off> (slot) (interface)
(port)
```

**on | off**

Keyword to enable (on) or disable (off) STP on the specified port.

**set lan ip address** Sets the LAN IP address. If you do not enter any optional parameters, the IAD sets the address on the first available slot, interface, port and connection. If connection is omitted, the first is used.

```
set lan ip address <IPaddress> <netmask> (slot)
(interface) (port) (connection)
```

**IP address**

- IP address in decimal format (999.999.999.999)
- netmask**  
Subnet mask in decimal format (255.255.255.255)
- remove lan ip address** Removes the LAN IP address. If you do not enter any optional parameters, the IAD locates and removes the first available slot, interface, port, and connection.
- ```
remove lan ip address <IP address> <netmask> (slot)
(interface) (port) (connection)
```
- IP address**  
IP address to remove, in decimal format (999.999.999.999)
- netmask**  
Subnet mask in decimal format (255.255.255.255)
- set lan rip** Enables or disables RIP on a LAN IP port. If you do not enter any optional parameters, the IAD performs the command against the first available slot, interface and port.
- ```
set lan rip <on | off> <version (1 | 2Bcst | 2Mlti)>
(slot) (interface) (port)
```
- on | off**  
Keyword to enable (on) or disable (off) RIP on the specified port.
- version 1 | 2Bcst | 2Mlti**  
Keyword identifying version to implement. (Must be preceded by keyword *version*)
- set nat** Enables or disables NAT on the specified port. If you do not enter any optional parameters, it finds the first available slot, interface and port.
- ```
set nat <on | off> (slot) (interface) (port)
```
- on | off**  
Keyword to enable (on) or disable (off) NAT on the specified port.
- set nat alias** Each NAT alias entry allows a device on the LAN (inside of NAT) to be accessible from the Internet via a unique IP address. The IAD only translates IP addresses for alias entries – port numbers are not changed.
- ```
set nat alias <add|remove> <index> <local IP>
<Network IP>
```
- add|remove**  
This commands adds or removes the nat alias.
- index**  
Index used on the NAT alias table
- local IP**  
Local IP address

**network IP**

Public IP address that is translated

**set nat server** Configures the NAT local server.

```
set nat server <add|remove> <index> <local IP>
<TCP|UDP|ESP|AH> <Translated Port> <Standard Port>
```

**add|remove**

Adds or removes the nat server.

**index**

Index used on the NAT server table

**local IP**

Local IP address

**TCP|UDP|ESP|AH**

Protocol used for traffic across the NAT port.

**Translated Port**

Local IP port

**Standard Port**

Port on the server that defines which TCP or UDP port is used

**set dhcp relay enable** Allows the IAD to forward DHCP requests from the LAN to a separate DHCP Server.

```
set dhcp relay enable <on or off>
```

**on or off**

On enables and off disables

**set dhcp relay sever** Provides IP address of DHCP server.

```
set dhcp relay enable <IP address>
```

**IP address**

IP address of DHCP server

**show dhcp relay configuration** Displays DHCP relay configuration

**set dhcp server enable** Enables or disables DHCP server on the IAD.

```
set dhcp server enable <on | off>
```

**on | off**

Keyword to enable (on) or disable (off) DHCP server.

**set dhcp server gateway** Sets the DHCP server default IP address.

```
set dhcp server gateway <IP address>
```

**IP address**

IP address of the DHCP server, in decimal format (999.999.999.999)

**set dhcp server subnet** Sets the DHCP server default subnet mask.  
 set dhcp server subnet <subnet mask>  
**subnet mask**  
 Subnet mask in decimal format (255.255.255.255)

**set dhcp server dns** Sets the DHCP DNS server IP address.  
 set dhcp server dns <IP address>  
**IP address**  
 IP address in decimal format (999.999.999.999)

**set dhcp server dns2** Sets the DHCP DNS secondary server IP address.  
 set dhcp server dns2 <IP address>  
**IP address**  
 IP address in decimal format (999.999.999.999)

**set dhcp server netbios** Sets the DHCP NetBIOS server IP address.  
 set dhcp server netbios <IP address>  
**IP address**  
 IP address in decimal format (999.999.999.999)

**set dhcp server domain** Sets the DHCP server domain name.  
 set dhcp server domain <domain name>  
**domain name**  
 Fully-qualified domain name

**set dhcp server range** Sets the DHCP server low and high IP address range.  
 set dhcp server range <low IP address> <high IP address>  
**Low IP address**  
 IP address in decimal format (999.999.999.999)  
**High IP address**  
 IP address in decimal format (999.999.999.999)

**set dhcp server lease** Determines how long the lease is valid.  
 set dhcp server lease <time in sec>

**set dns server address** Sets the DNS server IP address.  
 set dns server address <IP address>  
**IP address**  
 IP address in decimal format (999.999.999.999)

**set dns server address2** Sets the DNS secondary server IP address.  
 set dns server address <IP address>  
**IP address**  
 IP address in decimal format (999.999.999.999)

**set mgcp notified entity** Specifies the DNS name or IP address of the notified entity (call agent). You can specify one notified entity in the CLI. Use the menu interface to set up a maximum of four call agents.  
 set mgcp notified entity <domain name | IP address>  
**domain name | IP address**  
 Fully-qualified domain name or IP address of the call agent.

**set mgcp listening port** Specifies the UDP port the Notified Entity (call agent) is listening on.  
 set mgcp listening port <port>  
**port**  
 UDP Port number (any valid port number; usually 2427 or 2727)

**set mgcp signaling port** Specifies the UDP port the IAD uses for incoming MGCP messages.  
 set mgcp signaling connection <port>  
**port**  
 UDP Port number (any valid port number; usually 2427)

**set mgcp bracketing** When communicating with the notified entity (call agent), indicates whether the UDP port number should be wrapped in brackets for compatibility.  
 set mgcp bracketing <on | off>  
**on | off**  
 Keyword to enable (on) or disable (off) MGCP bracketing.

**set mgcp fqdn** Sets the fully qualified domain name.  
 set mgcp fqdn <on | off>

**set mgcp lcs** Sets the line control service.  
 set mgcp lcs <on | off>

**set voip rtp connection** Configures IP address that will be used to send and receive voice RTP traffic.  
 set voip rtp connection (slot) (interface) (port)  
 (connection)

**set voip signaling connection** Configures IP address used for SIP signaling and is used to identify a user to a SIP proxy.  
 set voip signaling connection (slot) (interface)  
 (port) (connection)



**set voip server** Configures FQDN or IP address of a SIP proxy.  
 set voip server <server name or IP address>  
**server name or IP address**  
 Defines a SIP proxy

**set voip line prefix** Configures a name (phone number) or a phone line on an IAD.  
 set voip line prefix <line number> <prefix>  
**line number**  
 Defines a line: values are from one to a maximum number of lines.  
**prefix**  
 Identifier for a line (phone number)

**set voip line password** Enables a password for POTS line used for VoIP.  
 set voip line password <line number> <password>  
**line number**  
 Determines which POTS line is used.  
**password**  
 Passwords are case-sensitive.

**set voip rtp port start** Configures a starting RTP port on which voice data is sent and received. First phone line on an IAD will use it. Each following line will use a port number two higher.  
 set voip port start <port number>  
**port number**  
 Defines starting RTP port

**set voip signaling tos** Configures value of the TOS byte of IP header for SIP signaling messages.  
 set voip signaling tos <0-7>

**set voip voice tos** Configures value of the TOS byte of IP header for RTP voice packets.  
 set voip voice tos <0-7>

**set voip buffer size** Configures size of RTP voice packets in milliseconds.  
 set voip buffer size <5-40>

**set voip password** Configures SIP authentication passwords.  
 set voip password <line> <password>  
**line**  
 Defines phone line  
**password**  
 Defines password

**set voip codec** Sets up which codecs are advertised.

- `set voip codec <add|remove>  
<G729a|G726|uLAW|ALAW|2833|NSE|ALL>`  
**add | remove**  
 Determines if you are adding or removing from the codec advertised list.  
**G729a | G726 | uLAW | ALAW | 2833 | NSE | ALL**  
 List of possible codec selections. ALL selects every available codec.
- register port** Used to register the VoIP port with the Proxy.  
`register port <port|all>`
- set jitter** Sets inter-arrival jitter delay.  
`set jitter <5-60>`  
**5-60**  
 Values are in milliseconds.
- set pots gain** Changes the gain on the POTS port.  
`set pots gain <port|all> <tx|rx> <gain>`  
**tx | rx**  
 Sets transmit or receive gain for the POTS port  
**gain**  
 Gain value in decibels. The values range from -9 to +3 dB
- set pots admin** Displays administration status of the POTS ports as set in the SIP configuration menu.  
`set pots admin <port|all> <on|off>`  
**on | off**  
 Enables or disables the port.
- set sds1 speed** Sets the SDSL speed. This command sets the speed to manual framed (Nokia) or Auto Cycle (Nokia).  
`set sds1 speed <speed> <auto|manual>`  
**speed**  
 Keyword identifying speed: 2320 | 1744 | 1536 | 1152 | 768 | 384 | 192  
**auto | manual**  
 Keyword identifying manual or auto cycle for Nokia
- set encoding** Sets the type of zero suppression used on the T1 network port.  
`set encoding <ami|b8zs> (slot)`  
**ami | b8zs**  
 Type of zero suppression
- set framing** Sets type of framing for the T1 network.  
`set framing <esf|d4> (slot)`

**esf | d4**  
Allows ESF or D4 framing

**set clocking** Sets clock source for the T1 network port.  
set Clocking <internal|external> (slot)  
**internal | external**  
Allows T1 network port timing to be internal or received from network

**set loopback** Sets up a loopback for test for T1 Network Port only.  
set loopback <line|payload|local|clear|far line|far payload> (slot)  
**line | payload | local | clear | far line | far payload**  
Determines which loopback is used. Clear is used to remove the loop.

**set channels** Sets which channels on the T1 network port are enabled or disabled.  
set channels <on|off> <low\_chan> <high\_chan> (slot)  
**on | off**  
Keyword to enable (on) or disable (off) the DS0 channels for the network port  
**low\_chan**  
Lowest channel number you are changing  
**high\_chan**  
Highest channel number that you are changing

**set buildout** Determines the buildout level for the T1 network port only.  
set buildout <133|266|399|533|655> (slot)  
**133 | 266 | 399 | 533 | 655**  
These values are for a DSX-1 short haul and values are in feet.

**show nat configuration** Displays NAT configuration

**show dhcp server configuration** Displays the DHCP server configuration.

**Show lan status** Displays LAN status

**show wan ppp configuration** Displays WAN PPP configuration.

**show wan status** Displays WAN status.

**show mgcp config** Displays MGCP configuration.

<b>show sip config</b>	Displays SIP parameters.
<b>show time</b>	Displays time.
<b>show snmp configuration</b>	Displays SNMP parameters.
<b>show configuration</b>	Displays the current configuration.
<b>show config file</b>	Displays IAD configuration.
<b>show statistics</b>	Displays IAD statistics.
<b>show ip routes table</b>	Displays the IP route table.
<b>show dns configuration</b>	Displays DNS configuration.
<b>quit</b>	Quits the command line interface and returns to the menu interface.

# TROUBLESHOOTING AND DIAGNOSTICS

This chapter describes procedures for troubleshooting and diagnosing problems that may be associated with the IAD.

Diagnostics are destructive, and may result in loss of connection to network or voice gateway. After running diagnostics, reset the IAD to return to normal working order.




---

**NOTICE:** *When the IAD prompts you for input, the current value is displayed in parentheses. To conveniently accept the current value, just press Enter.*

---

## Using the Diagnostics Menu

---

All diagnostic tasks are displayed and accessed on the Diagnostics menu, which is displayed by typing "z" on the Main menu.

**Figure 7.1** *Diagnostics Menu (Except SDSL Units)*

```
*****
*           Diagnostics           *
*****
P. POTS Diagnostics
```

**Figure 7.2** *Diagnostics Menu (SDSL Units Only)*

```
*****
*           Diagnostics           *
*****
P. POTS Diagnostics
S. SDSL Diagnostics
```

You may sign on as Supervisor or Network Manager to perform diagnostics tasks. Options that display in the Diagnostics menu are the same for both security levels. Type the option and proceed to the appropriate section below.

## POTS Diagnostics

A WAN uplink is not required to perform POTS testing. To perform POTS diagnostics, type "P" on the Diagnostics Menu. The IAD loads and configures the DSP software module, and displays the following menu:

**Figure 7.3** *POTS Diagnostics Menu*

```
*****
*           POTS Diagnostics           *
*****
D. Dialup Test
H. Hotline Test
R. Ring Test
O. On/Off Hook Test
I. Infineon Codec Test
T. Test External DSP Memory
```



---

**CAUTION:** *Pots diagnostics are intrusive tests. Any active calls will be terminated. You should terminate all voice gateway activity prior to employing POTS diagnostic testing. The Infineon CODEC test is reserved for Verilink use only.*

---

To perform a specific test, type the option and proceed to the appropriate section below.

### Dialup Test

The dialup test verifies the operational status of each telephone station by allowing the user to dial another POTS phone on the IAD by dialing the port number. To perform a dialup test, follow the steps below.

- 1 Type "D" on the POTS Diagnostics menu to select Dialup Test. The IAD displays this prompt:  
**Dialup test mode...**  
**Pick up any handset and dial the number of the line you want to test**
- 2 Take the selected handset offhook, listen for dial tone, and dial the port number. Hang up after a successful connection. The IAD reports the status of each action:  
**Line 1 off-hook**  
**Line 1 hung up**  
**Line 5 off-hook**  
**Line 5 hung up**
- 3 Press Escape to terminate the test. The IAD terminates the test and displays the menu.

## Hotline Test

The hotline test allows line-to-line telephone connections on a single IAD without requiring a gateway connection on the WAN port. To perform a hotline test, follow the steps below.

- 1 Type "H" on the POTS Diagnostics menu to select Hotline Test. The IAD displays the following prompt:  
**Perform an all-lines test? (Y or N):**
- 2 Type "Y" to enable automatic line connection. The IAD informs you the test has started. Proceed to step 6.  
– or –  
Type "N" to connect two specific ports. The IAD prompts you for the first port.
- 3 Type the port and press Enter. The IAD prompts for the second port.
- 4 Type the port and press Enter. The IAD informs you that the lines are connected and the test is started:  
**Lines 1 and 2 are connected together**  
**Lines 3 and 4 are connected together**  
**Lines 5 and 6 are connected together**  
**Lines 7 and 8 are connected together**  
**Hotline test started**
- 5 Press Escape to terminate the test. The IAD terminates the test and displays the POTS Diagnostics menu.

## Ring Test

The ring test verifies that the POTS device attached may be rung by the IAD. To perform a ring test, follow the steps below.

- 1 Type "R" on the POTS Diagnostics menu to select Ring Test. The IAD displays this prompt:  
**Ring all lines? (YN or ESC):**
- 2 Enter "Y" to proceed, or "N" or Escape to abort and return to the menu. The IAD displays this prompt:  
**Ring lines concurrently or sequentially? (CS or ESC):**
- 3 Enter "C" (concurrent), "S" (sequential), or Escape.
- 4 Listen for the rings to occur, and press Escape to terminate the test. The IAD terminates the test and displays the menu.

## Ring Test

The ring test rings all voice port lines either simultaneously or individually, in sequence. To perform a ring test, follow the steps below.

- 1 Type "R" on the POTS Diagnostics menu to select Ring Test. The IAD displays the following prompt:

Ring all lines? (YN or ESC): y

- 2 Type "Y" to test all lines.  
– or –  
Type "N" to test a specific line. The IAD prompts you for the port number and prompts you to perform the test sequentially or concurrently:

Ring lines concurrently or sequentially? (CS or ESC): s

- 3 Type "S" to perform the test sequentially, or type "C" to perform the test concurrently. The IAD displays information about the test progress:

```
Press a key to end ring test...
Ringing onhook lines...
Line 1 2 3 4 5
      6 7 8
top ringing all lines...
Line 1 2 3 4 5 6 7 8
Ring test complete
```

- 4 Press any key to terminate the test. The IAD displays the POTS Diagnostics menu.
- 5 Continue with other tests, or press Escape twice to return to the Main menu.

## On/Off Hook Test

The On/Off Hook test reports the hook state of each voice port line. To perform an On/Off Hook test, follow the steps below.

- 1 Type "O" on the POTS Diagnostics menu to select On/Off Hook Test. The IAD displays the status of the test as it runs in real time:

```
->o
Display hook state
Legend: .=onhook, ^=offhook, #=ring ground, &=no ring ground, *=flash hook
Press a key to exit...
 1 2 3 4 5 6 7 8
- . . . . .
```

- 2 Press Enter to terminate the test. The IAD displays the POTS Diagnostics menu.

The following tests listed on the POTS Diagnostics menu (Figure 7.3) are reserved for Verilink engineers:

- I. Infineon Codec Test
- C. Select Voice Loop Back Test Channel (8208 Only)
- V. Send/Receive Voice
- M. Quick Voice Loop Back Test (8208 Only)
- N. Burning Voice Loop Back Test (8208 Only)
- T. Test External DSP Memory



## SDSL Diagnostics

To perform SDSL diagnostics, type "S" on the Diagnostics menu. The IAD displays the SDSL Diagnostics menu:

Figure 7.4 SDSL Diagnostics Menu

```
*****
*           SDSL Diagnostics           *
*****

  Select Diagnostic

  P. Transmit Isolated Pulses
  2. Continuous 2-level transmission
  4. Continuous 4-level transmission
  L. Digital Far Loopback
```

To perform a type of transmission, type the specific option. For option "P", select the level to begin the transmission. Press any key to terminate the test.

## Troubleshooting the IAD

This section provides information for troubleshooting symptoms associated with the operation of the IAD. The table below describes symptoms and probable causes, and suggests what action can be taken to correct the problem.

Symptom	Probable Cause	Corrective Action
<b>Power indicator is not lit</b>	Power is not available to the IAD	Ensure the power cord is securely connected.
		Ensure the power cord is plugged into a live outlet.
		Ensure the power switch is on.
		If powered by an adapter, ensure the correct adapter is used.
<b>LAN Link indicator is not lit</b>	Incorrect Ethernet connection	Ensure an Ethernet cable is properly connected to the IAD and its upstream connection.
<b>No dial tone is present</b>	Incorrect PVC/DLCI set for voice channel	Verify these settings: VPI: 0 to 255 VCI: 0 to 65535 DLCI: 16 to 1023 (default PVC 0/39; DLCI 33)

Symptom	Probable Cause	Corrective Action
	IAD is improperly provisioned at the voice gateway  Incorrect network provisioning  Incorrect directory number at the Class 5 switch	Verify and correct provisioning of IAD as required (refer to page 5-2).  Check and correct network provisioning at DSLAM, network switches, etc.  Check and correct as required
<b>Cannot receive or send data</b>	Incorrect PVC/DLCI set for data channel	Verify these settings: VPI: 0 to 255 VCI: 0 to 65535 DLCI: 16 to 1023 (default PVC 0/38; DLCI 32) View Interface (page 5-13) and Media statistics (page 5-22) to check the pack receive and send status.
	Incorrect network setup	Check and correct network setup as necessary.
<b>If IAD is configured as a router:</b>		
	Incorrect or missing LAN or WAN IP address	Ensure that both the LAN and WAN IP addresses are configured.
	Incorrect or missing default static route	Review the routing table and correct as necessary (page 5-30).
	Incompatible RIPv1	Check and correct subnet masks (255.255.255.0) Update RIPv1 to RIPv2.
<b>If IAD is configured as a bridge:</b>		
	Incorrect bridging parameters	Review IAD configuration (page 5-2) and current bridge status (page 5-32). Correct as necessary
	Incorrect connection	Ensure the IAD is connected to another bridge
	Missing peer or converter	Install a converter to convert 1483 cells to Ethernet packets.

The table below lists the IAD provisioning parameters on the voice gateway that identifies the IAD and affects its performance. Verify these parameters when troubleshooting the IAD.

<b>Parameter</b>	<b>Description</b>
<b>ID</b>	Identification number of the IAD (read only)
<b>Serial Number</b>	IAD serial number (read only). Same as MAC Address
<b>Profile Name</b>	IAD profile name
<b>Interface Group</b>	Interface Group that will deliver the subscriber's calls.
<b>ATM Protection Group</b>	ATM Protection Group to which the IAD is assigned.
<b>VPI</b>	Virtual Path Identifier that identifies the subscriber-specific logical path between the voice gateway and the ATM network.
<b>VCI</b>	Virtual Circuit Identifier that identifies the subscriber-specific virtual circuit between the voice gateway and the ATM network (VCI must be specific – between 32 and 1023).
<b>Transport</b>	ATM or Frame Relay
<b>Signaling</b>	Loop Start or Ground Start
<b>Compression</b>	No compression, 32k, or 16k
<b>Echo Cancellation</b>	On or off
<b>Admin</b>	Service state of IAD: locked or unlocked
<b>Operational</b>	State of IAD (read only)



## VERIFICATION

This chapter describes how to verify that the 8000 Series IADs operate properly after installation. It also covers maintenance and how to display the current configuration. Before you can test the voice capabilities of the IAD, you must first provision it at the voice gateway and configure the voice application and parameters as described beginning on page 4-61.

### Power-up Test

---

The IAD displays an indication of normal operation when you first power it up. When you power it up, verify that the POWER indicator on the front panel lights green.

### Operational Test

---

Follow the procedure below to verify that the IAD is operating properly after installation. This procedure assumes that

- You have configured Directory numbers (DNs) in the Class 5 switch for the associated Voice Ports.
- The IAD has been connected to a terminal emulator via the console port, displays the normal boot sequence and you can log in.
- You have configured PVCs at the DSLAM (default data = 0, 38; default voice is 0, 39) when using ATM.
- You have provisioned a data network.
- You connected and configured a WAN link at the associated DSLAM or voice gateway. For more information, see *WAN Configuration* on page 4-2.
- You have a PC with Telnet, and an Ethernet adapter running TCP/IP. For more information, see *Connecting via Telnet* on page 2-9.
- For testing, you and a counterpart logged on to the upstream voice gateway can communicate via telephone or cell phone.

## Testing the IAD

- 1** Verify the WAN link status:
  - SDSL Interface—the LINK indicator blinks while the IAD synchronizes with the DSLAM, and lights continuously when the link is established.
  - T1/E1 Interface—the LINK indicator blinks while the IAD synchronizes with the voice gateway, and lights continuously when the link is established.
- 2** Connect a POTS telephone to a provisioned line port on the IAD.
- 3** Lift the telephone receiver and check for dial tone. If no dial tone is present, troubleshoot as necessary. (See *Troubleshooting the IAD* on page 7-5.)
- 4** Repeat steps 2 and 3 for each provisioned line port.
- 5** Disconnect the telephone once you are through testing the line ports.
- 6** Use a crossover cable to connect the PC to the Ethernet LAN port on the IAD. Determine that the PC is configured with an IP address on the same subnet as the IAD.
- 7** Observe that the LINK indicator on the IAD front panel lights to verify that the IAD is connected to the LAN.
- 8** Run Ping on the PC to ping a known good address on the IAD and verify the acknowledgement. If a timeout occurs, troubleshoot the LAN path to the IAD.
- 9** Ping a known good address on the network and wait for acknowledgement. If a timeout occurs, troubleshoot the LAN path to the IAD.
- 10** Disconnect the Ethernet cable between the PC and the IAD.
- 11** Using a straight-through cable, connect the Ethernet LAN port on the IAD to your local LAN patch panel or hub|switch|router.
- 12** Connect the IAD telephone ports to the local distribution frame or patch panel.

The IAD is ready for service.

## Maintenance

The IAD menu interface contains utilities reserved for factory maintenance and development. Before running any System Utilities, call the Verilink Technical Support Center at 800-285-2755 (toll-free).

## Displaying the Current Configuration

To display the current configuration and data transmission status, follow the steps below.

- 1** On the Main menu, type "1" to display the Reports menu.

Figure 8.1 *Reports Menu*

```
*****  
*                Reports Menu                *  
*****  
C. Display Current Configuration  
N. Display Network Statistics  
I. Display Interface Statistics  
M. Display Media Statistics  
R. Display Route Table  
A. Display ARP Table  
B. Display Bridge Forwarding Database  
S. Display Bridge Status  
P. Display PPP Authorization Entries  
U. Display System Uptime  
O. Display Memory Statistic  
E. Display Task Run Time
```

**2** Type "C" to display the current configuration.

For more information, see *Current Configuration Report* on page 5-2.



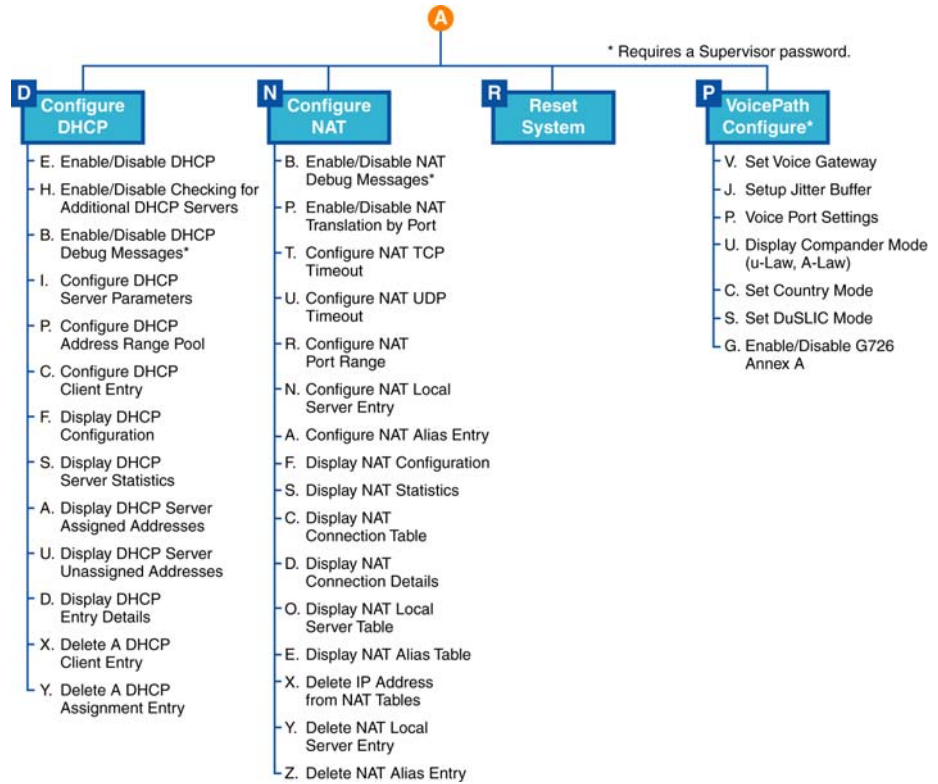




# MENU MAP

This appendix provides a map of the menu interface for the 8000 Series IADs.





## B

## SPECIFICATIONS

## T1/E1 (8208/8208s)

## Voice Features

**Analog Voice**

Voice Ports:	8 POTS ports (RJ-11)
Failover:	Analog input fail over to Line 1 (RJ-11)
Signaling:	Loop start, ground start
Dialing:	DTMF (tone), Pulse
Ring Source:	Internal
Impedance:	600 or 900 $\Omega$ or complex impedance
REN:	5 REN per port, 16 REN total
Loop Current:	20, 24 mA typical (country-specific)
Idle State Voltage:	-48 V typical
Ring Voltage:	Balanced 65 V rms $\pm$ 5% at 5 REN load
Ring Frequency:	20, 25, 50 Hz (country-specific)
Gain/System Loss:	Programmable, +3 to -9 dB

**Digital Voice**

Compression for non "s" Units:	G.711 (64 kbps PCM), G.726 (32 kbps ADPCM)
Compression for "s" Units (VoIP):	G.711 (64 kbps PCM), G.726 (32 kbps ADPCM), G.729a (8 kbps CS-ACELP)
Encoding:	A-law, $\mu$ -law
Echo Cancellation:	G.168 compliant (single reflector)
Protocol Support:	CopperCom, ELCP (af-vmoa=0145), Jetstream, LES (af-vmoa-0145), MGCP and SIP (s-version only)
DID/DOD Support	
Fax Support:	V.17, V.29 support

Modem Support:	V.34, V.90 support
Calling Features:	Caller ID, flash hook, distinctive ring, stutter dial tone, call forwarding, call waiting
Cell Delay Variation Buffer:	Configurable 0 – 30 ms

## Data Features

LAN Interface:	10/100Base-T (RJ-45)
Bridging:	IEEE 802.1d including spanning tree
Routing:	Default, Static, RIP1 (RFC 1058), RIP2 (RFC 2453), ICMP for IP Packet Processing
DHCP:	Server, Client (RFC 2131), Relay Agent (RFC 1542)
PPP:	PPoA, PPOE, PAP, CHAP, IPCP (RFC 1332)
HCLC Support Management:	SNMP via IP or EOC, MIB1, MIB2 (RFC 1213), Enterprise MIB, LES MIB
Configuration:	Console, Telnet (local, remote)

## WAN Features

Transport:	ATM and Frame Relay
Voice Gateways:	CopperCom, Jetstream, General Bandwidth, TdSoft, and any af-vmoa-0145-compliant gateway
Softswitches:	MGCP v1.0, SIP 1.0 (s-version only)
Protocols:	RFC 1483, RFC 1490, RFC 2364

## Network Interfaces

### T1

Network Interface:	RJ-48
Line Interface:	Balanced, 100 $\Omega$
Line Rate:	1.544 Mbps
Clock Source:	Line/local (s/w selectable)
Line Coding:	B8ZS or AM1 per T1.401
Framing:	D4 (SF)/ESF, AT&T 54016 or ANSI T1.403
Line Build Out:	0, -7.5, -15, or -22.5 dB
Receive Sensitivity:	Automatic
Input Jitter Tolerance:	Per ATT TR62411
Protection:	Over voltage/over current

## **E1**

Network Interface:	RJ-48
Line Rate:	2.048 Mbps ( $\pm 50$ bps) unframed
Line Framing:	CAS, CCS, or 2 Mbits unframed
Line Code:	AMI or HDB3
Input Signal:	E1, +1 to $-27$ dB
Connection:	RJ-48 jack at $120 \Omega$ ( $\pm 10\%$ )
Output Signal:	3.0 V ( $\pm 10\%$ ) base-peak into $120 \Omega$ with protection
Transient Voltage:	1000 V protection, fused input/output
Jitter Control:	per G.823 Sections 2.1 and 3.0
Ones Density:	HDB3, alternate fill; complies with G.701 and G.703

## **T1/E1 Provisioning (8208s Only)**

Provisioning:	Fractionally multiplexed voice and data (s-version only)
Programming:	On a DS0 basis

## **ATM**

Adaptation Layers:	AAL2 (voice), AAL5 (data), AAL5 (for layer 3 voice)
Encapsulation:	RFC 1483 multiprotocol encapsulation over ATM; RFC 2364 (PPP over ATM); ITU 366.1, ITU 366.2 (AAL2)
AAL2 Profiles (non-“s” Version):	ATM: 9, 10, 11, and ITU: 1
AAL2 Profiles (“s” Version):	ATM: 7, 8, 9, 10, 11, 12, and ITU: 1, 2
Voice:	Single AAL2 PVC
Data:	Up to 8 AAL5 PVCs
Security:	Software-configurable payload scrambling
Voice QoS:	CBR
Data QoS:	CBR, UBR
OAM Cell Handling:	F4/F5 segment and end-to-end loopbacks

## **Frame Relay**

Encapsulation:	RFC 1490 multiprotocol encapsulation over Frame Relay
Voice:	Single PVC
Data:	8 Data Link Identifiers (DLCIs)
Data Link Format:	Q.922
Data Link Control:	FRF.12 support, CMCP
Framing:	HDLC support

## Configuration and Management

### 10/100 Ethernet (Management or IP Gateway)

Connection:	8-pin modular
Network Protocol:	TCP/IP based networks
Data Rate:	10/100 Mbps
Compatibility:	10/100Base-T

### Supervisory Port

Connection:	DB-9 female
Data Rates:	1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200 bps (default: 19.2 kbps)

### Upgrades

- Trivial File Transfer Protocol (TFTP) server and client for software upgrades and configuration
- Software download via gateway (wherever supported)
- Automatic Upgrade via DHCP server
- Telnet (local and remote)

### Management

- SNMP 1.0, SNMP 3.0, Telnet, Console

## Security Features

### Integrated Firewall

NAT/PAT:	RFC 1631, Port translation, exported services, multiNAT (up to 8 public IP addresses)
Security:	Multi-level password protection
Other:	Radius client support RFC 2865

## Management Interfaces

### Alarms

Activation:	Programmable thresholds on all interfaces
Reporting:	SNMP traps

## Diagnostics

Network Loops:	Line loopback, payload loopback, or maintenance loopback
Fractional Loop:	Generates and responds to in-band V.54 loop code
DTE Port Loops:	V.54 and Local

## Environmental

Power Supply:	90 to 240 Vac, 60/50 Hz
Power:	20 W nominal, 50 W max operating
Operating Temperature:	0 to 40 °C
Storage Temperature:	-10 to -70 °C
Operating Humidity:	5 to 90% non-condensing
Safety:	UL 1950, CSA C22.2 No. 950-95, EN 60950:2000, IEC 60950:1999
EMC:	FCC Part 15, Class A; EN55022; EN55024; EN61000-3-2; EN61000-3-3
Industry Canada Registration Number:	2097B-NE8208
LEDs:	Power, LAN Link, LAN ACT, WAN Link, Voice
Dimensions:	11.8 in. x 8.3 in. x 1.8 in.
Weight:	1.8 lb
Mounting:	Stand-alone or Wall-mountable

## Connector Pin Assignments

### Console Port Pin Assignments (DB-9)

Pin	Signal
2	Tx Data
3	Rx Data
5	Ground

### POTS Port Pin Assignments (RJ-11)

Line	Pin Assignment		Line	Pin Assignment	
	Tip	Ring		Tip	Ring
1	3	4	5	3	4
2	3	4	6	3	4
3	3	4	7	3	4
4	3	4	8	3	4

### 10/100Base-T Connector Pin Assignments (RJ-45)

Pin	Signal	Pin	Signal
1	Tx+	3	Rx+
2	Tx-	6	Rx-

### T1/E1 Connector Pin Assignments (RJ-48)

Pin	Signal	Pin	Signal
1	Rx Ring	4	Tx Tip
2	Rx Tip	6	Tx Ring



# T1/E1 (8216s and 8224s)

## Voice Features

### Analog Voice

Voice Ports:	16 or 24 POTS ports (RJ-21)
Failover:	Analog input fail over to Line 1 (RJ-11)
Signaling:	Loop start, ground start
Dialing:	DTMF (tone), Pulse
Ring Source:	Internal
Impedance:	600 or 900 $\Omega$ or complex impedance
REN:	5 REN per port, 40 REN total
Loop Current:	20, 24 mA typical (country-specific)
Idle State Voltage:	-48 V typical
Ring Voltage:	Balanced 65 V rms $\pm$ 5% at 5 REN load
Ring Frequency:	20, 25, 50 Hz (country-specific)
Gain/System Loss:	Programmable, +3 to -9 dB

### Digital Voice

Compression:	G.711 (64 kbps PCM), G.726 (32 kbps ADPCM), G.729a (8 kbps CS-ACELP)
Encoding:	A-law, $\mu$ -law
Echo Cancellation:	G.168 compliant (single reflector)
Protocol Support:	CopperCom, ELCP (af-vmoa=0145), Jetstream, LES (af-vmoa-0145), MGCP and SIP
DID/DOD Support	
Fax Support:	V.17, V.29 support
Modem Support:	V.34, V.90 support
Calling Features:	Caller ID, flash hook, distinctive ring, stutter dial tone, call forwarding, call waiting
Cell Delay Variation Buffer:	Configurable 0 – 30 ms

## Data Features

LAN Interface:	10/100Base-T (RJ-45)
Bridging:	IEEE 802.1d including spanning tree
Routing:	Default, Static, RIP1 (RFC 1058), RIP2 (RFC 2453), ICMP for IP Packet Processing
DHCP:	Server, Client (RFC 2131), Relay Agent (RFC 1542)

PPP:	PPoA, PPOE, PAP, CHAP, IPCP (RFC 1332)
HCLC Support Management:	SNMP via IP or EOC, MIB1, MIB2 (RFC 1213), Enterprise MIB, LES MIB
Configuration:	Console, Telnet (local, remote)

## WAN Features

Transport:	ATM and Frame Relay
Voice Gateways:	CopperCom, Jetstream, General Bandwidth, TdSoft, and any af-vmoa-0145-compliant gateway
Softswitches:	MGCP v1.0, SIP 1.0
Protocols:	RFC 1483, RFC 1490, RFC 2364

## Network Interfaces

### T1

Network Interface:	RJ-48
Line Interface:	Balanced, 100 $\Omega$
Line Rate:	1.544 Mbps
Clock Source:	Line/local (s/w selectable)
Line Coding:	B8ZS or AM1 per T1.401
Framing:	D4 (SF)/ESF, AT&T 54016 or ANSI T1.403
Line Build Out:	0, -7.5, -15, or -22.5 dB
Receive Sensitivity:	Automatic
Input Jitter Tolerance:	Per ATT TR62411
Protection:	Over voltage/over current

### E1

Network Interface:	RJ-48
Line Rate:	2.048 Mbps ( $\pm 50$ bps) unframed
Line Framing:	CAS, CCS, or 2 Mbits unframed
Line Code:	AMI or HDB3
Input Signal:	E1, +1 to -27 dB
Connection:	RJ-48 jack at 120 $\Omega$ ( $\pm 10$ %)
Output Signal:	3.0 V ( $\pm 10$ %) base-peak into 120 $\Omega$ with protection
Transient Voltage:	1000 V protection, fused input/output
Jitter Control:	per G.823 Sections 2.1 and 3.0
Ones Density:	HDB3, alternate fill; complies with G.701 and G.703

## **T1/E1 Provisioning**

Provisioning: Fractionally multiplexed voice and data  
Programming: On a DS0 basis

## **ATM**

Adaptation Layers: AAL2 (voice), AAL5 (data), AAL5 (for layer 3 voice)  
Encapsulation: RFC 1483 multiprotocol encapsulation over ATM; RFC 2364 (PPP over ATM); ITU 366.1, ITU 366.2 (AAL2)  
AAL2 Profiles (non-“s” Version): ATM: 9, 10, 11, and ITU: 1  
AAL2 Profiles (“s” Version): ATM: 7, 8, 9, 10 11, 12, and ITU: 1, 2  
Voice: Single AAL2 PVC  
Data: Up to 8 AAL5 PVCs  
Security: Software-configurable payload scrambling  
Voice QoS: CBR  
Data QoS: CBR, UBR  
OAM Cell Handling: F4/F5 segment and end-to-end loopbacks

## **Frame Relay**

Encapsulation: RFC 1490 multiprotocol encapsulation over Frame Relay  
Voice: Single PVC  
Data: 8 Data Link Identifiers (DLCIs)  
Data Link Format: Q.922  
Data Link Control: FRF.12 support, CMCP  
Data Interworking: FRF.5, FRF.8 support  
Framing: HDLC support

## **Universal Serial Interface (DB-25)**

Interface: EIA-530, RS-449, V.35

## **Configuration and Management**

### **10/100 Ethernet (Management or IP Gateway)**

Connection: 8-pin modular  
Network Protocol: TCP/IP based networks  
Data Rate: 10/100 Mbps  
Compatibility: 10/100Base-T

## Supervisory Port

Connection:	DB-9 female
Data Rates:	1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200 bps (default: 19.2 kbps)

## Upgrades

- Trivial File Transfer Protocol (TFTP) server and client for software upgrades and configuration
- Software download via gateway (wherever supported)
- Automatic Upgrade via DHCP server
- Telnet (local and remote)

## Management

- SNMP 1.0, SNMP 3.0, Telnet, Console

## Security Features

### Integrated Firewall

NAT/PAT:	RFC 1631, Port translation, exported services, multiNAT (up to 8 public IP addresses)
Security:	Multi-level password protection
Other:	Radius client support RFC 2865

## Management Interfaces

### Alarms

Activation:	Programmable thresholds on all interfaces
Reporting:	SNMP traps

## Diagnostics

Network Loops:	Line loopback, payload loopback, or maintenance loopback
Fractional Loop:	Generates and responds to in-band V.54 loop code
DTE Port Loops:	V.54 and Local

## Environmental

Power Supply:	100 to 240 Vac, 60/50 Hz
Power:	
16 Port:	40 W nominal, 76 W max operating
24 Port:	40 W nominal, 110 W max operating
Operating Temperature:	0 to 40 °C

Storage Temperature:	-10 to -70 °C
Operating Humidity:	5 to 90% non-condensing
Safety:	ANSI/UL 60950-1:2002, CAN/CSA-C22.2 no. 60950-1-2003, EN 60950:2000, IEC60950:1999
EMC:	FCC Part 15, Class A; EN55022; EN55024; EN61000-3-2; EN61000-3-3
Industry Canada Registration Number:	2097B-82xx
LEDs:	Power, LAN Link, LAN ACT, WAN Link, Voice, DCE Link, DCE ACT
Dimensions:	10 in. x 17.5 in. x 1.75 in.
Weight:	5.6 lb (2.54 kg)
Mounting:	Stand-alone or rack-mountable

## Connector Pin Assignments

### Console Port Pin Assignments (DB-9)

Pin	Signal
2	Tx Data
3	Rx Data
5	Ground

### POTS Port Pin Assignments (RJ-21)

Line	Pin Assignment		Line	Pin Assignment	
	Tip	Ring		Tip	Ring
1	26	1	13	38	13
2	27	2	14	39	14
3	28	3	15	40	15
4	29	4	16	41	16
5	30	5	17	42	17
6	31	6	18	43	18
7	32	7	19	44	19
8	33	8	20	45	20
9	34	9	21	46	21
10	35	10	22	47	22
11	36	11	23	48	23
12	37	12	24	49	24

### 10/100Base-T Connector Pin Assignments (RJ-45)

Pin	Signal	Pin	Signal
1	Tx+	3	Rx+
2	Tx-	6	Rx-

### T1/E1 Connector Pin Assignments (RJ-48)

Pin	Signal	Pin	Signal
1	Rx Ring	4	Tx Tip
2	Rx Tip	5	Tx Ring

## USI Connector Pin Assignments (RS-530, V.35)

Signal	RS-530	V.35	RS-449
Shield Ground	1	A	1
Transmit Data (A)	2	P	4
Receive Data (A)	3	R	6
Request to Send (A)	4	C	7
Clear to Send (A)	5	D	9
DCE Ready (A)	6	E	13
Signal Ground	7	B	19
Receive Line Signal (A)	8	F	11
Receive DCE Clock (B)	9	X	26
Receive Line Signal (B)	10		29
Transmit DTE Clock (B)	11	W	35
Transmit DCE Clock (B)	12	AA	23
Clear to Send (B)	13		27
Transmit Data (B)	14	S	22
Transmit DCE Clock (A)	15	Y	5
Receive Data (B)	16	T	24
Receive DCE Clock (A)	17	V	8
	18		
Request to Send (B)	19		25
DTE Ready (A)	20	H	12
	21		
DCE Ready (B)	22		31
DTE Ready (B)	23		30
Transmit DTE Clock (A)	24	U	17
	25		

# SDSL (8304/8304s and 8308/8308s)

## Voice Features

### Analog Voice

Voice Ports:	4 or 8 POTS ports (RJ-11)
Failover:	Analog input fail over to Line 1 (RJ-11)
Signaling:	Loop start, ground start
Dialing:	DTMF (tone), Pulse
Ring Source:	Internal
Impedance:	600 or 900 $\Omega$ or complex impedance
REN:	5 REN per port, 16 REN total
Loop Current:	20, 24 mA typical (country-specific)
Idle State Voltage:	-48 V typical
Ring Voltage:	Balanced 65 V rms $\pm$ 5% at 5 REN load
Ring Frequency:	20, 25, 50 Hz (country-specific)
Gain/System Loss:	Programmable, +3 to -9 dB

### Digital Voice

Compression for non "s" Units:	G.711 (64 kbps PCM), G.726 (32 kbps ADPCM)
Compression for "s" Units (VoIP):	G.711 (64 kbps PCM), G.726 (32 kbps ADPCM), G.729a (8 kbps CS-ACELP)
Encoding:	A-law, $\mu$ -law
Echo Cancellation:	G.168 compliant (single reflector)
Protocol Support:	CopperCom, ELCP (af-vmoa=0145), Jetstream, LES (af-vmoa-0145), MGCP, SIP (s-version only)
DID/DOD Support	
Fax Support:	V.17, V.29 support
Modem Support:	V.34, V.90 support
Calling Features:	Caller ID, flash hook, distinctive ring, stutter dial tone, call forwarding, call waiting
Cell Delay Variation Buffer:	Configurable 0 – 30 ms

## Data Features

LAN Interface:	10/100Base-T (RJ-45)
Bridging:	IEEE 802.1d including spanning tree
Routing:	Default, Static, RIP1 (RFC 1058), RIP2 (RFC 2453), ICMP for IP Packet Processing



DHCP:	Server, Client (RFC 2131), Relay Agent (RFC 1542)
PPP:	PPoA, PPOE, PAP, CHAP, IPCP (RFC 1332)
HDLC Support Management:	SNMP via IP or EOC, MIB1, MIB2 (RFC 1213), Enterprise MIB, LES MIB
Configuration:	Console, Telnet (local, remote)

## WAN Features

### Interface

WAN:	RJ-11
Line Rate:	144 kbps to 2.3 mbps to 25,000 ft
Standards:	HDSL 2B1Q
Transport:	ATM and Frame Relay
Voice Gateways:	CopperCom, Jetstream, General Bandwidth, TdSoft, and any af-vmoa-0145-compliant gateway
Softswitches:	MGCP v1.0, SIP 1.0 (s-version only)

### ATM

Adaptation Layers:	AAL2 (voice), AAL5 (data), AAL5 (for layer 3 voice)
Encapsulation:	RFC 1483 multiprotocol encapsulation over ATM; RFC 2364 (PPP over ATM); ITU 366.1, ITU 366.2 (AAL2)
AAL2 Profiles (non-“s” Version):	ATM: 9, 10, 11 and ITU:1
AAL2 Profiles (“s” Version):	ATM: 7, 8, 9, 10 11, 12, and ITU: 1, 2
Voice:	Single AAL2 PVC
Data:	Up to 8 AAL5 PVCs
Security:	Software-configurable payload scrambling
Voice QoS:	CBR
Data QoS:	CBR, UBR
OAM Cell Handling:	F4/F5 segment and end-to-end loopbacks

### Frame Relay

Encapsulation:	RFC 1490 multiprotocol encapsulation over Frame Relay
Voice:	Single PVC
Data:	8 Data Link Identifiers (DLCIs)
Data Link Format:	Q.922
Data Link Control:	FRF.12 support, CMCP
Framing:	HDLC support

## Configuration and Management

### 10/100 Ethernet (Management or IP Gateway)

Connection:	8-pin modular
Network Protocol:	TCP/IP based networks
Data Rate:	10/100 Mbps
Compatibility:	10/100Base-T

### Supervisory Port

Connection:	DB-9 female
Data Rates:	1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200 bps (default: 19.2 kbps)

### Upgrades

- Trivial File Transfer Protocol (TFTP) server and client for software upgrades and configuration
- Software download via gateway (wherever supported)
- Automatic Upgrade via DHCP server
- Telnet (local and remote)

### Management

- SNMP 1.0, SNMP 3.0, Telnet, Console

## Security Features

### Integrated Firewall

NAT/PAT:	RFC 1631, Port translation, exported services, multiNAT (up to 8 public IP addresses)
Security:	Multi-level password protection
Other:	Radius client support RFC 2865

## Management Interfaces

### Alarms

Activation:	Programmable thresholds on all interfaces
Reporting:	SNMP traps

## Environmental

Power Supply:	90 to 240 Vac, 50/60 Hz
Power (8 Port):	20 W nominal, 50 W max operating
Power (4 Port):	15 W nominal, 30 W max operating
Operating Temperature:	0 to 40 °C

Storage Temperature:	-10 to -70 °C
Operating Humidity:	5 to 90% non-condensing
Safety:	UL 1950, CSA C22.2 No. 950-95, EN 60950:2000, IEC 60950:1999
EMC:	FCC Part 15, Class A; EN55022; EN55024; EN61000-3-2; EN61000-3-3
LEDs:	Power, LAN Link, LAN ACT, WAN Link, Voice
Dimensions:	11.8 in. x 8.3 in. x 1.8 in.
Weight:	1.8 lb
Mounting:	Stand-alone or Wall-mountable

## Connector Pin Assignments

### Console Port Pin Assignments (DB-9)

Pin	Signal
2	Tx Data
3	Rx Data
5	Ground

### POTS Port Pin Assignments (RJ-11)

Line	Pin Assignment		Line	Pin Assignment	
	Tip	Ring		Tip	Ring
1	3	4	5	3	4
2	3	4	6	3	4
3	3	4	7	3	4
4	3	4	8	3	4

### 10/100Base-T Connector Pin Assignments (RJ-45)

Pin	Signal	Pin	Signal
1	Tx+	3	Rx+
2	Tx-	6	Rx-

### SDSL Connector Pin Assignments (RJ-11)

Pin	Signal	Pin	Signal
2	Tip	3	Ring

# SDSL (8316s and 8324s)

## Voice Features

### Analog Voice

Voice Ports:	16 or 24 POTS ports (RJ-21)
Failover:	Analog input fail over to Line 1 (RJ-11)
Signaling:	Loop start, ground start
Dialing:	DTMF (tone), Pulse
Ring Source:	Internal
Impedance:	600 or 900 $\Omega$ or complex impedance
REN:	5 REN per port, 40 REN total
Loop Current:	20, 24 mA typical (country-specific)
Idle State Voltage:	-48 V typical
Ring Voltage:	Balanced 65 V rms $\pm$ 5% at 5 REN load
Ring Frequency:	20, 25, 50 Hz (country-specific)
Gain/System Loss:	Programmable, +3 to -9 dB

### Digital Voice

Compression:	G.711 (64 kbps PCM), G.726 (32 kbps ADPCM), G.729a (8 kbps CS-ACELP)
Encoding:	A-law, $\mu$ -law
Echo Cancellation:	G.168 compliant (single reflector)
Protocol Support:	CopperCom, ELCP (af-vmoa=0145), Jetstream, LES (af-vmoa-0145), MGCP, SIP
DID/DOD Support	
Fax Support:	V.17, V.29 support
Modem Support:	V.34, V.90 support
Calling Features:	Caller ID, flash hook, distinctive ring, stutter dial tone, call forwarding, call waiting
Cell Delay Variation Buffer:	Configurable 0 – 30 ms

## Data Features

LAN Interface:	10/100Base-T (RJ-45)
Bridging:	IEEE 802.1d including spanning tree
Routing:	Default, Static, RIP1 (RFC 1058), RIP2 (RFC 2453), ICMP for IP Packet Processing
DHCP:	Server, Client (RFC 2131), Relay Agent (RFC 1542)

PPP:	PPoA, PPOE, PAP, CHAP, IPCP (RFC 1332)
HDLC Support	
Management:	SNMP via IP or EOC, MIB1, MIB2 (RFC 1213), Enterprise MIB, LES MIB
Configuration:	Console, Telnet (local, remote)

## WAN Features

### Interface

WAN:	RJ-11
Line Rate:	144 kbps to 2.3 mbps to 25,000 ft
Standards:	HDSL 2B1Q
Transport:	ATM and Frame Relay
Voice Gateways:	CopperCom, Jetstream, General Bandwidth, TdSoft, and any af-vmoa-0145-compliant gateway
Softswitches:	MGCP v1.0, SIP 1.0

### ATM

Adaptation Layers:	AAL2 (voice), AAL5 (data), AAL5 (for layer 3 voice)
Encapsulation:	RFC 1483 multiprotocol encapsulation over ATM; RFC 2364 (PPP over ATM); ITU 366.1, ITU 366.2 (AAL2)
AAL2 Profiles:	ATM: 7, 8, 9, 10 11, 12, and ITU: 1, 2
Voice:	Single AAL2 PVC
Data:	Up to 8 AAL5 PVCs
Security:	Software-configurable payload scrambling
Voice QoS:	CBR
Data QoS:	CBR, UBR
OAM Cell Handling:	F4/F5 segment and end-to-end loopbacks

### Frame Relay

Encapsulation:	RFC 1490 multiprotocol encapsulation over Frame Relay
Voice:	Single PVC
Data:	8 Data Link Identifiers (DLCIs)
Data Link Format:	Q.922
Data Link Control:	FRF.12 support, CMCP
Data Interworking:	FRF.5, FRF.8 support
Framing:	HDLC support

## Universal Serial Interface (DB25)

Interface: EIA-530, RS-449, V.35

## Configuration and Management

### 10/100 Ethernet (Management or IP Gateway)

Connection: 8-pin modular  
Network Protocol: TCP/IP based networks  
Data Rate: 10/100 Mbps  
Compatibility: 10/100Base-T

### Supervisory Port

Connection: DB-9 female  
Data Rates: 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200 bps (default: 19.2 kbps)

### Upgrades

- Trivial File Transfer Protocol (TFTP) server and client for software upgrades and configuration
- Software download via gateway (wherever supported)
- Automatic Upgrade via DHCP server
- Telnet (local and remote)

### Management

- SNMP 1.0, SNMP 3.0, Telnet, Console

## Security Features

### Integrated Firewall

NAT/PAT: RFC 1631, Port translation, exported services, multiNAT (up to 8 public IP addresses)  
Security: Multi-level password protection  
Other: Radius client support RFC 2865

## Management Interfaces

### Alarms

Activation: Programmable thresholds on all interfaces  
Reporting: SNMP traps

## Environmental

Power Supply:	100 to 240 Vac, 50/60 Hz
Power:	
16 Port:	40 W nominal, 76 W max operating
24 Port:	40 W nominal, 110 W max operating
Operating Temperature:	0 to 40 °C
Storage Temperature:	-10 to -70 °C
Operating Humidity:	5 to 90% non-condensing
Safety:	ANSI/UL 60950-1:2002, CAN/CSA-C22.2 no. 60950-1-2003, EN 60950:2000, IEC60950:1999
EMC:	FCC Part 15, Class B; EN55022; EN55024; EN61000-3-2; EN61000-3-3
LEDs:	Power, LAN Link, LAN ACT, WAN Link, Voice, DCE Link, DCE ACT
Dimensions:	10 in. x 17.5 in. x 1.75 in.
Weight:	5.6 lb (2.54 kg)
Mounting:	Stand-alone or rack-mountable



## Connector Pin Assignments

### Console Port Pin Assignments (DB-9)

Pin	Signal
2	Tx Data
3	Rx Data
5	Ground

### POTS Port Pin Assignments (RJ-21)

Line	Pin Assignment		Line	Pin Assignment	
	Tip	Ring		Tip	Ring
1	26	1	13	38	13
2	27	2	14	39	14
3	28	3	15	40	15
4	29	4	16	41	16
5	30	5	17	42	17
6	31	6	18	43	18
7	32	7	19	44	19
8	33	8	20	45	20
9	34	9	21	46	21
10	35	10	22	47	22
11	36	11	23	48	23
12	37	12	24	49	24

### 10/100Base-T Connector Pin Assignments (RJ-45)

Pin	Signal	Pin	Signal
1	Tx+	3	Rx+
2	Tx-	6	Rx-

### SDSL Connector Pin Assignments (RJ-11)

Pin	Signal	Pin	Signal
2	Tip	3	Ring

### USI Connector Pin Assignments (RS-530, V.35)

Signal	RS-530	V.35	RS-449
Shield Ground	1	A	1
Transmit Data (A)	2	P	4

<b>Signal</b>	<b>RS-530</b>	<b>V.35</b>	<b>RS-449</b>
Receive Data (A)	3	R	6
Request to Send (A)	4	C	7
Clear to Send (A)	5	D	9
DCE Ready (A)	6	E	13
Signal Ground	7	B	19
Receive Line Signal (A)	8	F	11
Receive DCE Clock (B)	9	X	26
Receive Line Signal (B)	10		29
Transmit DTE Clock (B)	11	W	35
Transmit DCE Clock (B)	12	AA	23
Clear to Send (B)	13		27
Transmit Data (B)	14	S	22
Transmit DCE Clock (A)	15	Y	5
Receive Data (B)	16	T	24
Receive DCE Clock (A)	17	V	8
	18		
Request to Send (B)	19		25
DTE Ready (A)	20	H	12
	21		
DCE Ready (B)	22		31
DTE Ready (B)	23		30
Transmit DTE Clock (A)	24	U	17
	25		

# ADSL (8104/8104s and 8108/8108s)

---

## Voice Features

### Analog Voice

Voice Ports:	4 or 8 POTS ports (RJ-11)
Failover:	Analog input fail over to Line 1 (RJ-11)
Signaling:	Loop start, ground start
Dialing:	DTMF (tone), Pulse
Ring Source:	Internal
Impedance:	600 or 900 $\Omega$ or complex impedance
REN:	5 REN per port, 16 REN total
Loop Current:	20, 24 mA typical (country-specific)
Idle State Voltage:	-48 V typical
Ring Voltage:	Balanced 65 V rms $\pm$ 5% at 5 REN load
Ring Frequency:	20, 25, 50 Hz (country-specific)
Gain/System Loss:	Programmable, +3 to -9 dB

### Digital Voice

Compression for non "s" Units:	G.711 (64 kbps PCM), G.726 (32 kbps ADPCM)
Compression for "s" Units (VoIP):	G.711 (64 kbps PCM), G.726 (32 kbps ADPCM), G.729a (8 kbps CS-ACELP)
Encoding:	A-law, $\mu$ -law
Echo Cancellation:	G.168 compliant (single reflector)
Protocol Support:	CopperCom, ELCP (af-vmoa=0145), Jetstream, LES (af-vmoa-0145), MGCP and SIP (s-version only)
DID/DOD Support	
Fax Support:	V.17, V.29 support
Modem Support:	V.34, V.90 support
Calling Features:	Caller ID, flash hook, distinctive ring, stutter dial tone, call forwarding, call waiting
Cell Delay Variation Buffer:	Configurable 0-30 ms

## Data Features

LAN Interface:	10/100Base-T (RJ-45)
Bridging:	IEEE 802.1d including spanning tree
Routing:	Default, Static, RIP1 (RFC 1058), RIP2 (RFC 2453), ICMP for IP Packet Processing

DHCP:	Server, Client (RFC 2131), Relay Agent (RFC 1542)
PPP:	PPoA, PPOE, PAP, CHAP, IPCP (RFC 1332)
HCLC Support Management:	SNMP via IP or EOC, MIB1, MIB2 (RFC 1213), Enterprise MIB, LES MIB
Configuration:	Console, Telnet (local, remote)

## WAN Features

### Interface

WAN:	RJ-11
Standards:	ANSI T1.413 Issue 2; ITU-T G.992.2, G.992.1
Transport:	ATM
DSLAMs:	Cisco, Coppermountain, Innovia, Lucent, Nokia
Voice Gateways:	CopperCom, Jetstream, AAL2/LES: PSAX, TdSoft, Zhone, Tollbridge, General Bandwidth, Accelerated, Alcatel, and any af-vmoa-0145 complaint gateway
Softswitches:	MGCP v1.0, SIP 1.0 (s-version only)

### ATM

Adaptation Layers:	AAL2 (voice), AAL5 (data), AAL5 (for layer 3 voice)
Encapsulation:	RFC 1483 multiprotocol encapsulation over ATM; RFC 2364 (PPP over ATM); ITU 366.1, ITU 366.2 (AAL2)
AAL2 Profiles (non-“s” Version):	ATM: 9, 10, 11, and ITU: 1
AAL2 Profiles (“s” Version):	ATM: 7, 8, 9, 10 11, 12, and ITU: 1, 2
Voice:	Single AAL2 PVC
Data:	Up to 8 AAL5 PVCs
Security:	Software-configurable payload scrambling
Voice QoS:	CBR
Data QoS:	CBR, UBR
OAM Cell Handling:	F4/F5 segment and end-to-end loopbacks

## Configuration and Management

### 10/100 Ethernet (Management or IP Gateway)

Connection:	8-pin modular
Network Protocol:	TCP/IP based networks
Data Rate:	10/100 Mbps

Compatibility: 10/100Base-T

### **Supervisory Port**

Connection: DB-9 female

Data Rates: 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200 bps (default: 19.2 kbps)

### **Upgrades**

- Trivial File Transfer Protocol (TFTP) server and client for software upgrades and configuration
- Software download via gateway (wherever supported)
- Automatic Upgrade via DHCP server
- Telnet (local and remote)

### **Management**

- SNMP 1.0, SNMP 3.0, Telnet, Console

## **Security Features**

### **Integrated Firewall**

NAT/PAT: RFC 1631, Port translation, exported services, multiNAT (up to 8 public IP addresses)

Security: Multi-level password protection

Other: Radius client support RFC 2865

## **Management Interfaces**

### **Alarms**

Activation: Programmable thresholds on all interfaces

Reporting: SNMP traps

## **Environmental**

Power Supply: 90 to 240 Vac, 50/60 Hz

Power (8-Port): 20 W nominal, 50 W max operating

Power (4-Port): 15 W nominal, 30 W max operating

Operating Temperature: 0 to 40 °C

Storage Temperature: -10 to -70 °C

Operating Humidity: 5 to 90% non-condensing

Safety: UL 1950, CSA C22.2 No. 950-95, EN 60950:2000, IEC 60950:1999

EMC: FCC Part 15, Class A Digital Device; EN55022 Class A; EN55024; EN61000-3-2; EN61000-3-3

Industry Canada Registration Number: 2097B-NE8108

LEDs: Power, LAN Link, LAN ACT, WAN Link, Voice

Dimensions: 11.8 in. x 8.3 in. x 1.8 in.

Weight: 1.8 lb

Mounting: Stand-alone or wall-mountable

## Connector Pin Assignments

### Console Port Pin Assignments (DB-9)

Pin	Signal
2	Tx Data
3	Rx Data
5	Ground

### SHDSL Connector Pin Assignments (RJ-45)

Pin	Signal	Pin	Signal
1	Tx+	3	Rx+
2	Tx-	6	Rx-

### 10/100Base-T Connector Pin Assignments (RJ-48)

Pin	Signal	Pin	Signal
1	Tx+	3	Rx+
2	Tx-	6	Rx-

### ADSL Pin Assignments (RJ-11)

Pin	Signal	Pin	Signal
2	Tip	3	Ring

# SHDSL (8504/8504s and 8508/8508s)

---

## Voice Features

### Analog Voice

Voice Ports:	4 or 8 POTS ports (RJ-11)
Failover:	Analog input fail over to Line 1 (RJ-11)
Signaling:	Loop start, ground start
Dialing:	DTMF (tone), Pulse
Ring Source:	Internal
Impedance:	600 or 900 $\Omega$ or complex impedance
REN:	5 REN per port, 16 REN total
Loop Current:	20, 24 mA typical (country-specific)
Idle State Voltage:	-48 V typical
Ring Voltage:	Balanced 65 V rms $\pm$ 5% at 5 REN load
Ring Frequency:	20, 25, 50 Hz (country-specific)
Gain/System Loss:	Programmable, +3 to -9 dB

### Digital Voice

Compression for non “s” Units:	G.711 (64 kbps PCM), G.726 (32 kbps ADPCM)
Compression for “s” Units (VoIP):	G.711 (64 kbps PCM), G.726 (32 kbps ADPCM), G.729a (8 kbps CS-ACELP)
Encoding:	A-law, $\mu$ -law
Echo Cancellation:	G.168 compliant (single reflector)
Protocol Support:	CopperCom, ELCP (af-vmoa=0145), Jetstream, LES (af-vmoa-0145), MGCP, SIP (s-version only)
DID/DOD Support	
Fax Support:	V.17, V.29 support
Modem Support:	V.34, V.90 support
Calling Features:	Caller ID, flash hook, three-way calling, distinctive ring, stutter dial tone, call forwarding, call waiting
Cell Delay Variation Buffer:	Configurable 0 – 30 ms

## Data Features

LAN Interface:	10/100Base-T (RJ-45)
Bridging:	IEEE 802.1d including spanning tree
Routing:	Default, Static, RIP1 (RFC 1058), RIP2 (RFC 2453), ICMP for IP Packet Processing

DHCP:	Server, Client (RFC 2131), Relay Agent (RFC 1542)
PPP:	PPoA, PPOE, PAP, CHAP, IPCP (RFC 1332)
HCLC Support Management:	SNMP via IP or EOC, MIB1, MIB2 (RFC 1213), Enterprise MIB, LES MIB
Configuration:	Console, Telnet (local, remote)

## WAN Features

### Interface

WAN:	RJ-11
Standards:	ITU-T G.991.2
Transport:	ATM
DSLAMs:	Cisco, Coppermountain, Innovia, Lucent, Nokia
Voice Gateways:	CopperCom, Jetstream, AAL2/LES: PSAX, TdSoft, Zhone, Tollbridge, General Bandwidth, Accelerated, Alcatel, and any af-vmoa-0145 complaint gateway
Softswitches:	MGCP v1.0, SIP 1.0 (s-version only)

### ATM

Adaptation Layers:	AAL2 (voice), AAL5 (data), AAL5 (for layer 3 voice)
Encapsulation:	RFC 1483 multiprotocol encapsulation over ATM; RFC 2364 (PPP over ATM); ITU 366.1, ITU 366.2 (AAL2)
AAL2 Profiles (non-“s” Version):	ATM: 9, 10, 11, and ITU:1
AAL2 Profiles (“s” Version):	ATM: 7, 8, 9, 10 11, 12, and ITU: 1, 2
Voice:	Single AAL2 PVC
Data:	Up to 8 AAL5 PVCs
Security:	Software-configurable payload scrambling
Voice QoS:	CBR
Data QoS:	CBR, UBR
OAM Cell Handling:	F4/F5 segment and end-to-end loopbacks

## Configuration and Management

### 10/100 Ethernet (Management or IP Gateway)

Connection:	8-pin modular
Network Protocol:	TCP/IP based networks
Data Rate:	10/100 Mbps
Compatibility:	10/100Base-T



## Supervisory Port

Connection:	DB-9 female
Data Rates:	1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200 bps (default: 19.2 kbps)

## Upgrades

- Trivial File Transfer Protocol (TFTP) server and client for software upgrades and configuration
- Software download via gateway (wherever supported)
- Automatic Upgrade via DHCP server
- Telnet (local and remote)

## Management

- SNMP 1.0, SNMP 3.0, Telnet, Console

## Security Features

### Integrated Firewall

NAT/PAT:	RFC 1631, Port translation, exported services, multiNAT (up to 8 public IP addresses)
Security:	Multi-level password protection
Other:	Radius client support RFC 2865

## Management Interfaces

### Alarms

Activation:	Programmable thresholds on all interfaces
Reporting:	SNMP traps

## Environmental

Power Supply:	90 to 240 Vac, 50/60 Hz
Power (8-Port):	20 W nominal, 50 W max operating
Power (4-Port):	15 W nominal, 30 W max operating
Operating Temperature:	0 to 40 °C
Storage Temperature:	-10 to -70 °C
Operating Humidity:	5 to 90% non-condensing
Safety:	UL 1950, CSA C22.2 No. 950-95, EN 60950:2000, IEC 60950:1999
EMC:	FCC Part 15, Class A Digital Device; EN55022 Class A; EN55024; EN61000-3-2; EN61000-3-3
Industry Canada Registration Number:	2097B-NE8508

LEDs:	Power, LAN Link, LAN ACT, WAN Link, Voice
Dimensions:	11.8 in. x 8.3 in. x 1.8 in.
Weight:	1.8 lb
Mounting:	Stand-alone or wall-mountable

## Connector Pin Assignments

### Console Port Pin Assignments (DB-9)

Pin	Signal
2	Tx Data
3	Rx Data
5	Ground

### POTS Port Pin Assignments (RJ-11)

Line	Pin Assignment		Line	Pin Assignment	
	Tip	Ring		Tip	Ring
1	3	4	5	3	4
2	3	4	6	3	4
3	3	4	7	3	4
4	3	4	8	3	4

### 10/100Base-T Connector Pin Assignments (RJ-45)

Pin	Signal	Pin	Signal
1	Tx+	3	Rx+
2	Tx-	6	Rx-

### SHDSL Connector Pin Assignments (RJ-11)

Pin	Signal	Pin	Signal
1	Tx+	3	Rx+
2	Tx-	6	Rx-

# SHDSL (8512s, 8516s, and 8524s)

---

## Voice Features

### Analog Voice

Voice Ports:	12, 16 or 24 POTS ports (RJ-21)
Failover:	Analog input fail over to Line 1 (RJ-11)
Signaling:	Loop start, ground start
Dialing:	DTMF (tone), Pulse
Ring Source:	Internal
Impedance:	600 or 900 $\Omega$ or complex impedance
REN:	5 REN per port, 40 REN total
Loop Current:	20, 24 mA typical (country-specific)
Idle State Voltage:	-48 V typical
Ring Voltage:	Balanced 65 V rms $\pm$ 5% at 5 REN load
Ring Frequency:	20, 25, 50 Hz (country-specific)
Gain/System Loss:	Programmable, +3 to -9 dB

### Digital Voice

Compression:	G.711 (64 kbps PCM), G.726 (32 kbps ADPCM), G.729a (8 kbps CS-ACELP)
Encoding:	A-law, $\mu$ -law
Echo Cancellation:	G.168 compliant (single reflector)
Protocol Support:	CopperCom, ELCP (af-vmoa=0145), Jetstream, LES (af-vmoa-0145), MGCP, SIP
DID/DOD Support	
Fax Support:	V.17, V.29 support
Modem Support:	V.34, V.90 support
Calling Features:	Caller ID, flash hook, three-way calling, distinctive ring, stutter dial tone, call forwarding, call waiting
Cell Delay Variation Buffer:	Configurable 0 – 30 ms

## Data Features

LAN Interface:	10/100Base-T (RJ-45)
Bridging:	IEEE 802.1d including spanning tree
Routing:	Default, Static, RIP1 (RFC 1058), RIP2 (RFC 2453), ICMP for IP Packet Processing
DHCP:	Server, Client (RFC 2131), Relay Agent (RFC 1542)

PPP:	PPoA, PPOE, PAP, CHAP, IPCP (RFC 1332)
HCLC Support Management:	SNMP via IP or EOC, MIB1, MIB2 (RFC 1213), Enterprise MIB, LES MIB
Configuration:	Console, Telnet (local, remote)

## WAN Features

### Interface

WAN:	RJ-11
Standards:	ITU-T G.991.2
Transport:	ATM
DSLAMs:	Cisco, Coppermountain, Innovia, Lucent, Nokia
Voice Gateways:	CopperCom, Jetstream, AAL2/LES: PSAX, TdSoft, Zhone, Tollbridge, General Bandwidth, Accelerated, Alcatel, and any af-vmoa-0145 complaint gateway
Softswitches:	MGCP v1.0, SIP 1.0

### ATM

Adaptation Layers:	AAL2 (voice, AAL5 (data), AAL5 (for layer 3 voice)
Encapsulation:	RFC 1483 multiprotocol encapsulation over ATM; RFC 2364 (PPP over ATM); ITU 366.1, ITU 366.2 (AAL2)
AAL2 Profiles:	ATM: 7, 8, 9, 10 11, 12, and ITU: 1, 2
Voice:	Single AAL2 PVC
Data:	Up to 8 AAL5 PVCs
Security:	Software-configurable payload scrambling
Voice QoS:	CBR
Data QoS:	CBR, UBR
OAM Cell Handling:	F4/F5 segment and end-to-end loopbacks

### Universal Serial Interface (DB25)

Interface:	EIA-530, RS-449, V.35
------------	-----------------------

### Frame Relay (USI Interface Only)

Encapsulation:	RFC 1490 multiprotocol encapsulation over Frame Relay
Voice:	Single PVC
Data:	8 Data Link Identifiers (DLCIs)
Data Link Format:	Q.922

Data Link Control:	FRF.12 support, CMCP
Data Interworking:	FRF.5, FRF.8 support
Framing:	HDLC support

## Configuration and Management

### 10/100 Ethernet (Management or IP Gateway)

Connection:	8-pin modular
Network Protocol:	TCP/IP based networks
Data Rate:	10/100 Mbps
Compatibility:	10/100Base-T

### Supervisory Port

Connection:	DB-9 female
Data Rates:	1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200 bps (default: 19.2 kbps)

### Upgrades

- Trivial File Transfer Protocol (TFTP) server and client for software upgrades and configuration
- Software download via gateway (wherever supported)
- Automatic Upgrade via DHCP server
- Telnet (local and remote)

### Management

- SNMP 1.0, SNMP 3.0, Telnet, Console

## Security Features

### Integrated Firewall

NAT/PAT:	RFC 1631, Port translation, exported services, multiNAT (up to 8 public IP addresses)
Security:	Multi-level password protection
Other:	Radius client support RFC 2865

## Management Interfaces

### Alarms

Activation:	Programmable thresholds on all interfaces
Reporting:	SNMP traps

## Environmental

Power Supply:	100 to 240 Vac, 50/60 Hz
---------------	--------------------------

Power:	
12 Port:	40 W nominal, 65 W max operating
16 Port:	40 W nominal, 76 W max operating
24 Port:	40 W nominal, 110 W max operating
Operating Temperature:	0 to 40 °C
Storage Temperature:	-10 to -70 °C
Operating Humidity:	5 to 90% non-condensing
Safety:	ANSI/UL 60950-1:2002, CAN/CSA-C22.2 no. 60950-1-2003, EN 60950:2000, IEC60950:1999
EMC:	FCC Part 15, Class A Digital Device; EN55022 Class A; EN55024; EN61000-3-2; EN61000-3-3
Industry Canada Registration Number:	2097B-85xx
LEDs:	Power, LAN Link, LAN ACT, WAN Link, Voice, DCE Link, DCE ACT
Dimensions:	10 in. x 17.5 in. x 1.75 in.
Weight:	5.6 lb (2.54 kg)
Mounting:	Stand-alone or rack-mountable

## Connector Pin Assignments

### Console Port Pin Assignments (DB-9)

Pin	Signal
2	Tx Data
3	Rx Data
5	Ground

### POTS Port Pin Assignments (RJ-21)

Line	Pin Assignment		Line	Pin Assignment	
	Tip	Ring		Tip	Ring
1	26	1	13	38	13
2	27	2	14	39	14
3	28	3	15	40	15
4	29	4	16	41	16
5	30	5	17	42	17
6	31	6	18	43	18
7	32	7	19	44	19
8	33	8	20	45	20
9	34	9	21	46	21
10	35	10	22	47	22
11	36	11	23	48	23
12	37	12	24	49	24

### 10/100Base-T Connector Pin Assignments (RJ-45)

Pin	Signal	Pin	Signal
1	Tx+	3	Rx+
2	Tx-	6	Rx-

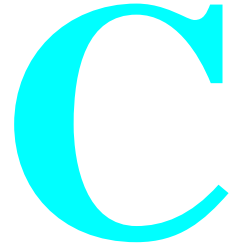
### SHDSL Connector Pin Assignments (RJ-11)

Pin	Signal	Pin	Signal
1	Tx+	3	Rx+
2	Tx-	6	Rx-

## USI Connector Pin Assignments (RS-530, V.35)

Signal	RS-530	V.35	RS-449
Shield Ground	1	A	1
Transmit Data (A)	2	P	4
Receive Data (A)	3	R	6
Request to Send (A)	4	C	7
Clear to Send (A)	5	D	9
DCE Ready (A)	6	E	13
Signal Ground	7	B	19
Receive Line Signal (A)	8	F	11
Receive DCE Clock (B)	9	X	26
Receive Line Signal (B)	10		29
Transmit DTE Clock (B)	11	W	35
Transmit DCE Clock (B)	12	AA	23
Clear to Send (B)	13		27
Transmit Data (B)	14	S	22
Transmit DCE Clock (A)	15	Y	5
Receive Data (B)	16	T	24
Receive DCE Clock (A)	17	V	8
	18		
Request to Send (B)	19		25
DTE Ready (A)	20	H	12
	21		
DCE Ready (B)	22		31
DTE Ready (B)	23		30
Transmit DTE Clock (A)	24	U	17
	25		





## APPLICATIONS NOTES

### Frame Relay

ATM was originally intended for multimedia applications and, therefore, is designed for delay-sensitive, real-time implementation. On the other hand, Frame Relay was originally intended for interactive data applications, which tend to be bursty and are delay tolerant since loss or errored frames can be detected and resent. To maximize line utilization, Frame Relay uses variable-sized frames that expand or contract based on traffic volume. For voice applications, this can be a fatal problem; large frames on a slow link can be addressed by constraining the frame size on voice DLCIs. The FRF.12 Agreement was formulated to address this problem. Fragmentation queueing reduces both delay and delay variation by dividing large packets into smaller packets for transmission and then reassembling them into original packets at their destination.

#### Setting the Fragment (Maximum Frame) Size

A good rule to follow when setting the fragment size is to set the size (in bytes) to the same value as the link rate (in kilobits). For example, if the link rate is 512 kbps, set the fragment size to 512 bytes. This ensures frame transmission (serialization) delay stays at less than 8 ms and allows a deterministic value when addressing network delay calculations. This rule works for *any* link rate as shown below.

If “X” is the link rate in kilobits per second, then:

Fragment size = X in bytes

so that

Transmission delay = X bytes x 8 bits/byte / (X x 1000 bits per second),  
which = 8/1000 s,

which = 8 ms for any X.

# Peak Cell Rate (PCR) Considerations and Recommendations

## Voice-only Applications

The primary requirement to ensure toll-quality voice is to keep packet loss as close to zero as possible and keep the round-trip-delay rate through the network below 150 ms. You must employ judicious network design engineering to control round-trip delay. To avoid packet loss, enforce timely delivery, and thereby maintain high voice quality, Verilink recommends that Voice be given the highest priority within the IAD (ATM Service Category “CBR” as shown on the “ATM Service Category Configuration Menu” on page 4-26). Verilink also recommends that the PCR value be adequate to support *all* configured ports at each port’s highest bit rate, and that the jitter delay parameter be set between 10 and 20 ms (refer to “Set Jitter Delay” on page 4-77). To establish the PCR, use the following approach for VoIP applications:

- Each ATM cell has (requires) 424 bits (53 bytes per cell x 8 bits per byte).
- Voice Payload is 160 bytes per packet for G.711 (derived by using 20 ms encoding option).
- Packet overhead is 49 bytes for PPP over ATM (includes RTP, UDP, IP header).
- A packet is generated every 20 ms (50 packets per second) to carry the Voice payload plus overhead at the encoding rate for each PCM channel.

With this approach, the bandwidth requirement for an attached POTS port is the following:

$$\begin{aligned} \text{BW} &= 50 \text{ packets per second} \times 1672 \text{ bits per packet} \\ &= 83,600 \text{ bps} \end{aligned}$$

For an IAD with eight attached POTS ports, allocate 8 x 83,600 bps of bandwidth on the link, or 668,800 bps. The PCR in this case would be the following:

$$668,800 \text{ bps} / 424 \text{ bits per cell} = 1577 \text{ cells per second}$$

## Voice and Data Applications

Set the PCR for the Voice PVC to the maximum for the link’s transmission rate and set the PCR for the data PVC to zero. This allows the IAD to dynamically allocate the bandwidth with Voice having the highest priority. For example, on an SDSL link running at 512 kbps, set the PCR at 1208 for the Voice PVC, and set the PCR for Data to 0 (zero).

## Network Address Translation (NAT)

In an IP network, all devices must have unique IP addresses. NAT allows multiple devices on the LAN port of an IAD to share Internet access via the IP address of the WAN port of the IAD. With this configuration, Verilink recommends that the LAN port of the IAD and all LAN devices use one of the private IP address ranges as defined in Section 3, Page 4 of RFC 1918:

10.0.0.0 through 10.255.255.255, 172.16.0.0 through 172.31.255.255, or 192.168.0.0 through 192.168.255.255.

## **Accessing the Internet from the LAN**

When you want to access the Internet from the LAN, but do not want to access any local LAN devices from the Internet, enable NAT translation on the WAN port that is connected to the Internet Service Provider (ISP). If two ATM PVCs are defined and one of these is connected to a voice gateway, the PVC connected to the ISP should have NAT enabled.

## **Configuring NAT Port Range**

When you access the internet from the LAN, the request uses the next unused port number in the configured NAT port range. For most applications, the default range of 30000 through 65535 will work, as these port numbers are not commonly used. If any port numbers in this range are used (i.e., multiplayer Internet games), the range must be adjusted. The number of concurrent requests through NAT is limited by the size of the range. For current port number assignments, please refer to <http://www.iana.org/assignments/port-numbers>.

## **Configuring NAT TCP Timeout**

When a TCP connection is made through NAT, a context block is allocated from the IAD's memory. This context block is freed when either the TERM bit is seen in the TCP header, or when the timeout period has been exceeded with no data. In most applications, the default value of 5 min (300 s) will be sufficient. If the application features a large number of aborted TCP connections, this value may need to be lowered. If the application features connections with longer idle times, this value may need to be increased.

## **Configuring NAT UDP Timeout**

When a non-TCP connection is made through NAT, a context block is allocated from the IAD's memory. This context block is freed when the timeout period has been exceeded with no data. In most applications, the default value of 2 min (120 s) will be sufficient. If the application features a large number of very short UDP, AH, or ESP connections, this value may need to be lowered. If the application features connections with longer idle times, this value may need to be increased.

## **Accessing LAN Devices from the Internet**

If you want to access a LAN device from the Internet (i.e., Web server, FTP server, etc.), the device must be configured in NAT to allow access from the Internet. There are two ways to do this: through a NAT Local Server entry or through a NAT Alias entry.

## NAT Local Server Configuration

A NAT Local Server entry is used when the local device shares its IP address with the WAN port of the IAD. Only the configured protocol and port will be visible from the Internet. When the Local Server is configured, the following information must be entered:

- Translated IP address – local IP address, as seen from the LAN.
- Protocol – TCP, UDP, AH, ESP, or both UDP and TCP.
- Translated Port Number – port number on which the local server sees the service (UDP and TCP only).
- Standard Port Number – port number on which the Internet sees the service (UDP and TCP only).

For current port number assignments, please see <http://www.iana.org/assignments/port-numbers>.

Note that TCP port 1723 is used to select Point-to-Point Tunneling Protocol (PPTP) and TCP port 1720 is used to select ViaVideo. When using ViaVideo units through NAT, the following limitations apply.

- Only one Via Video inside of NAT may accept calls.
- All ViaVideo units in the network must be configured to use fixed ports 3230 – 3235.
- All ViaVideo units inside of NAT must be configured to use NAT and must have the IAD's WAN address configured.

If Internet access of a local Telnet server at TCP port 23 is desired, it will be necessary to reconfigure the Telnet server port of the IAD. Refer to “*Configure Port IP Address*” on page 4-40 for further information.

## NAT Alias Configuration

A NAT Alias entry is used when the local device is assigned a unique IP address from the WAN port of the IAD. The local device will be *totally* accessible from the Internet. When the Alias entry is configured, the following information must be entered:

- Local IP Address – the local IP address as seen from the LAN.
- Internet IP Address – the IP address of the device as seen from the Internet.

When configuring a NAT Alias entry, the alias's Internet IP address *must* also be configured on the WAN port. This must be configured with an IP mask of 255.255.255.255 if the alias's Internet IP address is on the same subnet as the IAD's WAN IP address. If the alias's Internet IP address is on a subnet different from the IAD's WAN IP address, the proper subnet mask should be used. Refer to “*Configure Port IP Address*” on page 4-40 for further information.

## IP Filtering

IP Filtering controls IP traffic traveling through an interface by selectively passing or discarding IP packets based on criteria expressed in the form of a

“filter.” A filter is simply a set of rules that determine whether a packet should be passed or discarded as it crosses an interface. An interface is any port that carries IP traffic. On the IAD, it can be one of the following: Ethernet port, PPP connection, ATM PVC, or FR DLCI. IP filtering can selectively pass or discard IP packets based on one or more of the following properties:

- Protocol (IP, ICMP, TCP, and UDP)
- Protocol flags (for TCP and ICMP only)
- Source and/or Destination IP address
- Source and/or Destination port number

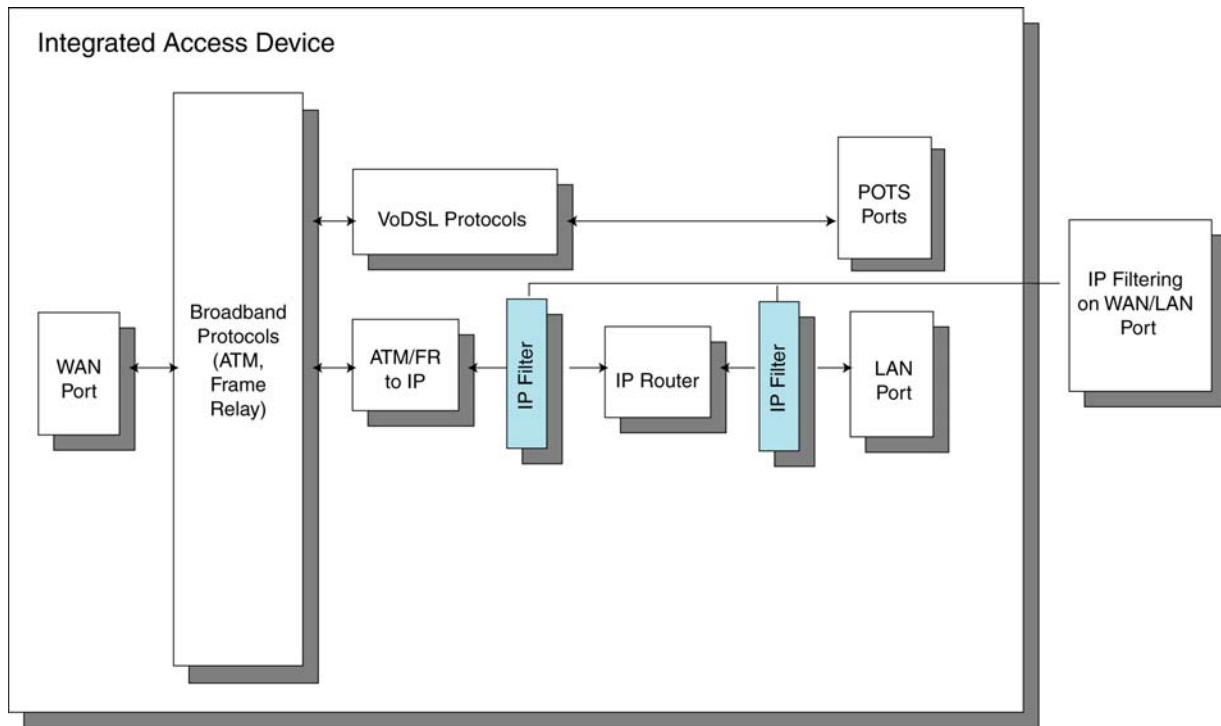
## **Information Policy**

Before you define a filtering rule set, you must determine what information you will permit to enter or exit the network and who should have access to that information. This “information policy” can be divided into two broad groups: open and closed. An open information policy, by default, allows access to everything; filters are put in place to block access only to a small number of sensitive addresses and/or protocols. This type of policy is typically used in a trusted network situation that places a premium on openness rather than security. Any filters applied are intended to deny access to sensitive information not intended for public viewing, such as financial data. A closed information policy, by default, blocks access to everything; filters are put in place to allow access only to approved addresses and/or protocols. A closed information policy is used when security and network integrity are more important than ease of access. If your network is connected to the Internet, a closed information policy will make your system less vulnerable to attack.

## **Filtering Interface**

You may apply IP Filtering to any interface that carries IP traffic. Rule sets can be defined for both inbound and outbound traffic through each interface. The block diagram below shows where IP Filtering is performed on the IAD.

Figure C-1. IAD Block Diagram With IP Filtering Shown



IP Filtering can be applied to either WAN or LAN ports; these are the only two that can carry IP traffic. For connections to the Internet, the WAN port is the best choice. All examples provided below assume the WAN port is the selected port. Although you may select the LAN port as well, it is not recommended, as this would make your network vulnerable if support protocols such as Telnet or TFTP are targeted. Port selection is also important because it establishes a point of view for defining filters. An input filter on the WAN port will block or pass packets entering the WAN port. An input filter on the LAN port will block or pass packets entering the LAN port.

IP Filtering on a WAN port for inbound traffic is performed after NAT has occurred. IP Filtering on a WAN port for outbound traffic is performed prior to NAT.

IP Filtering rule sets are defined using the *ifname* for each interface. The *ifname* for a particular interface can be viewed from Current Configuration. In general, the *ifname* is an abbreviated interface name with the port number. For example, the Ethernet interface *ifname* is *eth0*. ATM PVC interface names would be *atm0*, *atm1*, *atm2*, etc. Other *ifnames* include *ppp0*, *fr0*, *ppp0a0*, *hdlc0*. Please note that when creating and deleting PVCs and FR DLCIs, *ifnames* can change. Please review the IP Filtering rule set after modifying WAN connections to ensure that the rule set is still valid.

## IP Packet Filtering Syntax and Grammar

Each packet is compared to all the rules in the list for the interface and direction, with the last matching rule being applied (exception: see “quick” command below). Therefore, the most restrictive rules (block) should be placed first in the list, with pass rules following. This will allow only certain packet types to traverse the IAD.



---

**NOTICE:** *When modifying or deleting PVCs, the interface names can change. Verify the interface names match the desired interfaces after modifying or deleting PVCs.*

---

The rules are stored on the IAD in the file, *filter.st*, and can be viewed through the user interface. You may edit the *filter.st* file external to the IAD and then download it to the IAD.

### Grammar

The format used for construction of filtering rules can be described using the following grammar in BNF:

filter-rule = action in-out [ options ] [ match ] [ keep ]

action = "block" | "pass" | "count"

in-out = "in" | "out"

options = [ "quick" ] [ "on" interface-name ]

match = [ tos ] [ ttl ] [ proto ] [ ip ]

keep = "keep state"

tos = "tos" decnumber | "tos" hexnumber

ttl = "ttl" decnumber

proto = "proto" protocol

ip = srcdst [ flags ] [ with withopt ] [ icmp ] [ keep ]

protocol = "tcp/udp" | "udp" | "tcp" | "icmp" | decnumber

srcdst = "all" | fromto

fromto = "from" object "to" object

object = ["!"] addr [ port-comp | port-range ]

addr = "any" | nummask | host-name [ "mask" ipaddr | "mask" hexnumber ]

port-comp = "port" compare port-num

port-range = "port" port-num range port-num

flags = "flags" flag { flag } [ "/" flag { flag } ]

with = "with" | "and"

icmp = "icmp-type" icmp-type [ "code" decnumber ]

nummask = host-name [ "/" decnumber ]

host-num = digit [ digit [ digit ] ]

port-num = service-name | decnumber

withopt = [ "not" | "no" ] opttype [ withopt ] .

```

opttype   = "ipopts" | "short" | "frag" | "opt" ipopts .
optname   = ipopts [ ",", optname ] .
ipopts    = optlist | "sec-class" [ secname ] .
secname   = seclvl [ ",", secname ] .
seclvl    = "unclass" | "confid" | "reserv-1" | "reserv-2" | "reserv-3" | "reserv-4" |
           "secret" | "topsecret" .
icmp-type = "unreach" | "echo" | "echorep" | "squench" | "redir" | "timex" |
           "paramprob" | "timest" | "timestrep" | "inforeq" | "inforep" | "maskreq"
           | "maskrep" | decnumber
icmp-code = decumber | "net-unr" | "host-unr" | "proto-unr" | "port-unr" | "need-
           frag" | "srcfail" | "net-unk" | "host-unk" | "isolate" | "net-prohib" |
           "host-prohib" | "net-tos" | "host-tos" .
optlist   = "nop" | "rr" | "zsu" | "mtup" | "mtur" | "encode" | "ts" | "tr" | "sec" |
           "lsrr" | "e-sec" | "cipso" | "satid" | "ssrr" | "addext" | "visa" | "imitd" |
           "eip" | "finn"

hexnumber = "0" "x" hexstring
hexstring = hexdigit [ hexstring ]
decnumber = digit [ decnumber ]

compare   = "=" | "!=" | "<" | ">" | "<=" | ">=" | "eq" | "ne" | "lt" | "gt" | "le" | "ge" .
range     = "<>" | "><"
hexdigit  = digit | "a" | "b" | "c" | "d" | "e" | "f"
digit     = "0" | "1" | "2" | "3" | "4" | "5" | "6" | "7" | "8" | "9"
flag      = "F" | "S" | "R" | "P" | "A" | "U"

```

This syntax is somewhat simplified for readability, some combinations that match this grammar are disallowed by the software because they do not make sense (such as tcp **flags** for non-TCP packets).

## Filter Rules

The "briefest" valid rules are (currently) no-ops and are of the form:

```

block in all
pass in all

```

Filter rules are checked in order, with the last matching rule determining the fate of the packet (exception, see the quick option below).

## Actions

The action indicates what to do with the packet if it matches the rest of the filter rule. Each rule **MUST** have an action. The following actions are recognized:

**block** indicates that the packet should be flagged to be dropped.

**pass** will flag the packet to be let through the filter.

The next word must be either **in** or **out**. Each packet moving through the system is either inbound (just been received on an interface) or outbound (transmitted or forwarded by the stack, and on its way to an interface). There



is a requirement that each filter rule explicitly state which side of the I/O it is to be used on.

## Options

The list of options is brief. Where options are used, they must be present in the order shown here. These are currently supported options:

- quick** allows "short-cut" rules in order to speed up the filter or override later rules. If a packet matches a filter rule which is marked as **quick**, this rule will be the last rule checked, allowing a "short-circuit" path to avoid processing later rules for this packet. The current status of the packet (after any effects of the current rule) will determine whether it is passed or blocked. If this option is missing, the rule is taken to be a "fall-through" rule, meaning that the result of the match (block/pass) is saved and that processing will continue to see if there are any more matches.
- on** allows an interface name to be incorporated into the matching procedure. If this option is used, the rule will only match if the packet is going through that interface in the specified direction (in/out). If this option is absent, the rule is taken to be applied to a packet regardless of the interface it is present on (i.e. on all interfaces). Filter rulesets are common to all interfaces, rather than having a filter list for each interface.

This option is especially useful for simple IP-spoofing protection: packets should only be allowed to pass inbound on the interface from which the specified source address would be expected, others may be logged and/or dropped.

## Matching Parameters

The keywords described in this section are used to describe attributes of the packet to be used when determining whether rules match or don't match. The following general-purpose attributes are provided for matching, and must be used in this order:

- tos** packets with different Type-Of-Service values can be filtered. Individual service levels or combinations can be filtered upon. The value for the TOS mask can either be represented as a hex number or a decimal integer value.
- ttl** packets may also be selected by their Time-To-Live value. The value given in the filter rule must exactly match that in the packet for a match to occur. This value can only be given as a decimal integer value.
- proto** allows a specific protocol to be matched against. Protocol names may be used. However, the protocol may also be given as a DECIMAL number, allowing for rules to match your own protocols, or new ones which would out-date any attempted listing.

The special protocol keyword **tcp/udp** may be used to match either a TCP or a UDP packet, and has been added as a convenience to save duplication of otherwise-identical rules.

The **from** and **to** keywords are used to match against IP addresses (and optionally port numbers). Rules must specify BOTH source and destination parameters.

IP addresses may be specified in one of two ways: as a numerical address/mask, or as a hostname **mask** netmask. The hostname is of the dotted numeric form.

There is a special case for the hostname **any** which is taken to be 0.0.0.0/0 (see below for mask syntax) and matches all IP addresses. Only the presence of "any" has an implied mask, in all other situations, a hostname **MUST** be accompanied by a mask. It is possible to give "any" a hostmask, but in the context of this language, it is nonsensical.

The numerical format "x/y" indicates that a mask of y consecutive 1 bits set is generated, starting with the MSB, or a hexadecimal number of the form 0x12345678. Note that all the bits of the IP address indicated by the bitmask must match the address on the packet exactly; there isn't currently a way to invert the sense of the match, or to match ranges of IP addresses which do not express themselves easily as bitmasks.

If a **port** match is included, for either or both of source and destination, then it is only applied to TCP and UDP packets. If there is no **proto** match parameter, packets from both protocols are compared. This is equivalent to "proto tcp/udp". When composing **port** comparisons, either the service name or an integer port number may be used. Port comparisons may be done in a number of forms, with a number of comparison operators, or port ranges may be specified. See the examples for more information.

The **all** keyword is essentially a synonym for "from any to any" with no other match parameters.

Following the source and destination matching parameters, the following additional parameters may be used:

The **with** keyword is used to match irregular attributes that some packets may have associated with them. To match the presence of IP options in general, use **with ipopts**. To match packets that are too short to contain a complete header, use **with short**. To match fragmented packets, use **with frag**. For more specific filtering on IP options, individual options can be listed.

Before any parameter used after the **with** keyword, the word **not** or **no** may be inserted to cause the filter rule to only match if the option(s) is not present.

Multiple consecutive **with** clauses are allowed. Alternatively, the keyword **and** may be used in place of **with**, this is provided purely to make the rules more readable ("with ... and ..."). When multiple clauses are listed, all those must match to cause a match of the rule.

**flags** is only effective for TCP filtering. Each of the letters possible repre-

sents one of the possible flags that can be set in the TCP header. The association is as follows:

F - FIN  
S - SYN  
R - RST  
P - PUSH  
A - ACK  
U - URG

The various flag symbols may be used in combination, so that "SA" would represent a SYN-ACK combination present in a packet. There is nothing preventing the specification of combinations, such as "SFR", that would not normally be generated by law-abiding TCP implementations. However, to guard against weird aberrations, it is necessary to state which flags you are filtering against. To allow this, it is possible to set a mask indicating which TCP flags you wish to compare (i.e., those you deem significant). This is done by appending "<flags>" to the set of TCP flags you wish to match against, e.g.:

**flags S**

becomes "flags S/AUPRFS" and will match packets with ONLY the SYN flag set.

**flags SA**

becomes "flags SA/AUPRFS" and will match any packet with only the SYN and ACK flags set.

**flags S/SA**

will match any packet with just the SYN flag set out of the SYN-ACK pair; the common "establish" keyword action. "S/SA" will NOT match a packet with BOTH SYN and ACK set, but WILL match "SFP".

**icmp-type** is only effective when used with **proto icmp** and must NOT be used in conjunction with **flags**. There are a number of types, which can be referred to by an abbreviation recognized by this language, or the numbers with which they are associated can be used. The most important from a security point of view is the ICMP redirect.

## Keep History

The last parameter which can be set for a filter rule is whether or not to record historical information for that packet, and what sort to keep. The following information can be kept:

- state** keeps information about the flow of a communication session. State can be kept for TCP, UDP, and ICMP packets.
- frags** keeps information on fragmented packets, to be applied to later fragments.

## Examples

The **quick** option is good for rules such as

```
block in quick from any to any with ipopts
```

which will match any packet with a non-standard header length (IP options present) and abort further processing of later rules, recording a match and also that the packet should be blocked.

The "fall-through" rule parsing allows for effects such as this:

```
block in from any to any port < 6000
pass in from any to any port >= 6000
block in from any to port > 6003
```

which sets up the range 6000-6003 as being permitted and all others being denied. Note that the effect of the first rule is overridden by subsequent rules. Another (easier) way to do the same is:

```
block in from any to any port 6000 <> 6003
pass in from any to any port 5999 >> 6004
```

Note that both the "block" and "pass" are needed here to effect a result as a failed match on the "block" action

```
pass in quick from any to any port < 1024
```

would be needed before the first block.

## Dial Plan

The Call Agent can ask the gateway to collect digits dialed by the user. This facility is intended to be used with residential gateways to collect the numbers that a user dials; it can also be used with trunking gateways and access gateways alike, to collect access codes, credit card numbers and other numbers requested by call control services.

One procedure is for the gateway to notify the Call Agent of each individual dialed digit, as soon as they are dialed. However, such a procedure generates a large number of interactions. It is preferable to accumulate the dialed numbers in a buffer, and to transmit them in a single message.

The problem with this accumulation approach, however, is that it is hard for the gateway to predict how many numbers it needs to accumulate before transmission. For example, using the phone on our desk, we can dial the following numbers:

```

-----
| 0 | Local operator |
| 00 | Long distance operator |
| xxxx | Local extension number |
| 8xxxxxxx | Local number |
| #xxxxxxx | Shortcut to local number at|
| | other corporate sites |
| *xx | Star services |
| 91xxxxxxxxxxx | Long distance number |
| 9011 + up to 15 digits| International number |
-----

```

The solution to this problem is to have the Call Agent load the gateway with a digit map that may correspond to the dial plan. This digit map is expressed using a syntax derived from the Unix system command, *egrep*. For example, the dial plan described above results in the following digit map:

```
(0T|00T|[1-7]xxx|8xxxxxxx|#xxxxxxx|*xx|91xxxxxxxxxxx|9011x.T)
```

The formal syntax of the digit map is described by the DigitMap rule in the formal syntax description of the protocol – support for basic digit map letters is **REQUIRED** while support for extension digit map letters is **OPTIONAL**. A gateway receiving a digit map with an extension digit map letter not supported **SHOULD** return error code 537 (unknown digit map extension).

A digit map, according to this syntax, is defined either by a (case insensitive) "string" or by a list of strings. Each string in the list is an alternative numbering scheme, specified either as a set of digits or timers, or as an expression over which the gateway will attempt to find a shortest possible match. The following constructs can be used in each numbering scheme:

- \* Digit: A digit from "0" to "9".
- \* Timer: The symbol "T" matching a timer expiry.
- \* DTMF: A digit, a timer, or one of the symbols "A", "B", "C", "D", "#", or "\*". Extensions may be defined.
- \* Wildcard: The symbol "x" which matches any digit ("0" to "9").
- \* Range: One or more DTMF symbols enclosed between square brackets "[" and "]").
- \* Subrange: Two digits separated by hyphen ("-") which matches any digit between and including the two. The subrange construct can only be used inside a range construct, i.e., between "[" and "]".
- \* Position: A period (".") which matches an arbitrary number, including zero, of occurrences of the preceding construct.

A gateway that detects events to be matched against a digit map **MUST** do the following:

- 1** Add the event code as a token to the end of an internal state variable for the endpoint called the "current dial string".
- 2** Apply the current dial string to the digit map table, attempting a match to each expression in the digit map.

- 3** If the result is under-qualified (partially matches at least one entry in the digit map and doesn't completely match another entry), do nothing further.

If the result matches an entry, or is over-qualified (i.e., no further digits could possibly produce a match), send the list of accumulated events to the Call Agent. A match, in this specification, can be either a "perfect match," exactly matching one of the specified alternatives, or an impossible match, which occurs when the dial string does not match any of the alternatives. Unexpected timers, for example, can cause "impossible matches". Both perfect matches and impossible matches trigger notification of the accumulated digits (which may include other events).

The following example illustrates the above. Assume we have the digit map:

```
(xxxxxxx|x11)
```

and a current dial string of "41". Given the input "1" the current dial string becomes "411". We have a partial match with "xxxxxxx", but a complete match with "x11", and hence we send "411" to the Call Agent.

The following digit map example is more subtle:

```
(0[12].|00|1[12].1|2x.#)
```

Given the input "0", a match will occur immediately since position (".") allows for zero occurrences of the preceding construct. The input "00" can thus never be produced in this digit map.

Given the input "1", only a partial match exists. The input "12" is also only a partial match, however both "11" and "121" are a match. Given the input "2", a partial match exists. A partial match also exists for the input "23", "234", "2345", etc. A full match does not occur here until a "#" is generated, e.g., "2345#". The input "2#" would also have been a match.

Note that digit maps simply define a way of matching sequences of event codes against a grammar. Although digit maps as defined here are for DTMF input, extension packages can also be defined so that digit maps can be used for other types of input represented by event codes that adhere to the digit map syntax already defined for these event codes (e.g., "1" or "T"). Where such usage is envisioned, the definition of the particular event(s) SHOULD explicitly state that in the package definition.

This is the formal syntax definition:

```
DigitMap = DigitString / "(" DigitStringList ")"
DigitStringList = DigitString 0*( "|" DigitString )
DigitString = 1*(DigitStringElement)
DigitStringElement = DigitPosition ["."]
DigitPosition = DigitMapLetter / DigitMapRange; NOTE "X"
is now included
DigitMapLetter = DIGIT / "#" / "*" / "A" / "B" / "C" /
"D" / "T" / "X"; NOTE "[x]" is now allowed
DigitMapRange = "[" 1*DigitLetter "]"
DigitLetter = *((DIGIT "-" DIGIT) / DigitMapLetter)
```

# D

## GLOSSARY

**10/100BaseT.** 10-Mbps baseband Ethernet specification that uses two pairs of twisted-pair cabling: one pair for transmitting data and the other for receiving data. 10/100BaseT has a distance limit of approximately 100 meters per segment.

**100BaseT.** 100-Mbps baseband Fast Ethernet specification that uses UTP wiring. Like 10/100BaseT, 100BaseT sends link pulses over the network segment when no traffic is present. These link pulses contain more information than those used in 10/100BaseT.

**ADSL.** Asymmetric Digital Subscriber Line.

**ARP.** Address Resolution Protocol. Enables routers to obtain the Ethernet address for a known IP address. See also Inverse ARP.

**ATM.** Asynchronous Transfer Mode.

**BOOTP.** Bootstrap Protocol. Used during network booting by a network node to determine the IP address of its Ethernet interfaces.

**DLCI.** Data-Link Connection Identifier. Value that specifies a PVC or SVC in a Frame Relay network. In the basic Frame Relay specification, DLCIs are locally significant (connected devices might use different values to specify the same connection). In the LMI extended specification, DLCIs are globally significant (DLCIs specify individual end devices).

**E1.** Network connection with a capacity of 2.048, divided into 32 separate channels (or DS0s).

**EEPROM.** Electrically Erasable Programmable read only Memory. Nonvolatile memory chips that can be erased using electrical signals and reprogrammed.

**Ethernet.** Physical connection commonly used for LANs. Runs over a variety of cable types and provides theoretical bandwidth of 10 or 100 Mbps. Invented by Xerox Corporation and developed jointly with Intel and Digital Equipment Corporation.

**Fast Ethernet.** Any of a number of 100 Mbps Ethernet specifications.

**Frame Relay.** A network interface providing high-speed packet transmission with minimum delay. Uses variable-length packets called frames. Contrast with packet.

**Full Duplex.** Capable of handling simultaneous data transmission between a sending station and a receiving station.

**ICMP.** Internet Control Message Protocol. Internet protocol that reports errors and provides other information relevant to IP packet processing, such as routing information.

**IGMP.** Internet Group Management Protocol. Transport layer multicasting protocol used by IP hosts to register their dynamic multicast group membership. It is also used by connected routers to discover these group members.

**Inverse ARP.** Inverse Address Resolution Protocol. Enables routers to obtain the IP address of a known Ethernet address of a device associated with a virtual circuit. Method of building dynamic routes in a network.

**IP.** Internet Protocol. Part of the TCP/IP protocol. IP networks are connectionless, packet switching networks.

**IP address.** 32-bit address assigned to hosts using TCP/IP. An IP address contains four octets separated by periods, also known as a dotted quad address. Each address consists of a network number, an optional sub-network number and a host number. The network and sub-network numbers together are used for routing, while the host number is used to address an individual host within the network or sub-network.

**IP SNAP.** Sub-network Access Protocol. Internet protocol that operates between a network entity in the sub-network and a network entity in the end system. SNAP specifies a standard method of encapsulating IP datagrams and ARP messages on IEEE networks. The SNAP entity in the end system makes use of the services of the sub-network and performs three essential functions: data transfer, connection management and QOS selection.

**LAN.** Local Area Network. Privately owned network-connecting devices over a limited geographic area—usually limited to an office or office complex. Often connected to the Internet via IADs, with firewall software to limit access to the LAN by authorized users. May use TCP/IP or one of several other protocols.

**LMI.** Local Management Interface. A set of the following enhancements to the basic Frame Relay specification. Called LMT in ANSI terminology.

- a keep-alive mechanism that verifies that data is flowing.
- a multi-cast mechanism, which provides the network server with its local DLCI and the multi-cast DLCI.
- Global addressing; this gives DLCIs global rather than local significance in Frame Relay networks.
- a mechanism that provides an on-going status report on the DLCIs known to the switch.



**MAC.** Media Access Control. Lower of the two sub-layers of the data link layer defined by the IEEE.

**MAC address.** Standardized data link layer address that is required for every port or device that connects to a LAN. Other devices in the network use these addresses to locate specific ports in the network and to create and update routing tables and data structures. MAC addresses are six bytes long and are IEEE-controlled. Also known as a hardware address, a MAC-layer address, or a physical address.

**MPEG.** Moving Pictures Expert Group.

**Notified Entry.** IP address of the MGCP Call Agent; controls the call setup and teardown for all call features under MGCP.

**OSI Reference Model.** Network architectural model developed by ISO and ITU-T. The model consists of the following seven layers, each of which specifies particular network functions.

The lowest layer is closest to the media technology and the highest layer is closest to the user. The hardware and software implement the lower two layers, while only the software implements the upper five layers.

- Physical layer – the actual wires and connections in the network.
- Data link layer – responsible for physical addressing, network topology, error notification and ordered delivery.
- Network layer – responsible for connectivity, path selection and routing.
- Transport layer – responsible for network communication, virtual circuit management, fault detection and flow control.
- Session layer – manages sessions between applications.
- Presentation layer – responsible for data structures used by networked applications.
- Application layer – networked software applications such as e-mail, Telnet and FTP.

**Packet.** Logical grouping of information that includes a header containing control information and (usually) user data. Packets refer to network layer units of data, with messages divided into several packets. Some networks use fixed packet sizes; others use variable packet sizes. Packets typically have standard header information that identifies the packet. In contrast, frames contain only data; information about the frames transmits on the control plane.

The terms datagram, frame, message and segment describe logical information groupings at various layers of the OSI reference model and in various technology circles.

**PPP.** Point-to-Point Protocol. a successor to SLIP that provides router-to-router and host-to-network connections over synchronous and asynchronous circuits.

**Poisoned Reverse RIP.** Feature to set routes learned on the same port as the transmitted RIP message an infinite distance. Prevents the propagation of routes from crashed routers through the network.

**PVC.** Permanent Virtual Circuit. PVCs save bandwidth associated with circuit establishment and tear down in situations where certain virtual circuits must exist all the time.

**RFC.** Request for Comments. Documents that detail operation of the Internet. To obtain these document, go to [www.rfc-editor.org](http://www.rfc-editor.org).

**RIP.** Routing Information Protocol. Internet protocol used to exchange routing information within a system. RIP uses hop count as a routing metric.

**Router.** Network layer device that uses one or more metrics to determine the optimal path to forward network traffic. Routers forward packets from one network to another based on network layer information. a router may connect networks using various protocols by encapsulating data within another network's packet format or by removing layers of packet formatting.

**SNMP.** Simple Network Management Protocol. Network management protocol used in TCP/IP networks. SNMP provides a way to monitor and control network devices and to manage configurations, Statistics collection, performance and security.

**Subnet Mask.** 32-bit address mask that indicates the bits of an IP address used for the subnet address.

**SVC.** Switched Virtual Circuit. Virtual circuit that is dynamically established on demand and is torn down when transmission is complete.

**T1.** Network connection with a capacity of 1.544 Mbps, divided into 24 separate channels (or DS0s).

**TCP/IP.** Protocols used for IP networks, such as the Internet, Intranets and many LANs. IP networks are connectionless, packet switching networks.

**TFTP.** Trivial File Transfer Protocol. Simplified version of FTP that transfers files from one computer to another over a network.

**WAN.** Wide Area Network. Data communications network that serves users across a broad geographic area and often uses transmission devices provided by common carriers. Frame Relay is an example of a WAN.



## Five-Year Hardware Limited Warranty

- I. **Limited Warranty.** Subject to the limitations and disclaimers set forth in this Hardware Limited Warranty, Verilink warrants to the original purchaser ("Buyer") that the Verilink equipment and component parts ("Goods") purchased by Buyer shall be free from defects in material and workmanship under normal use and service for a period of five years from the date of shipment of the Goods to Buyer ("Limited Warranty"). Verilink's sole obligation and Buyer's sole remedy under this Limited Warranty shall be to repair or replace any Verilink Goods that Verilink determines to be so defective. Any claim by Buyer under this Limited Warranty must be presented to Verilink in writing within five years and fifteen (15) days of the date of shipment of the Goods to Buyer, as evidenced by Verilink's packing slip or similar shipment documentation from a Verilink authorized reseller. Any replacement Goods may be new or reconditioned. Verilink reserves the right to substitute equivalent Goods for defective Goods, in its sole discretion. As long as Verilink either so repairs or replaces the Goods, this Limited Warranty will not be found to have failed its essential purpose. If the defect has been caused by accident, misuse or abnormal operating conditions (including lightning damage) occurring after delivery to Buyer, repairs and/or replacement will be made at Buyer's expense. In such event, an estimate of cost will be submitted to Buyer before repair work is started. The Limited Warranty will continue to apply to replaced or repaired Goods for whichever is longer: the 90-day period after the shipment of such Goods to Buyer or the remainder of the original Limited Warranty period.
- II. **EXCLUSION OF IMPLIED WARRANTIES OR OTHER REPRESENTATION.** THE GOODS ARE SOLD BY VERILINK "AS IS" WITHOUT ANY WARRANTY OR GUARANTEE OF ANY KIND OTHER THAN THE LIMITED WARRANTY SET FORTH ABOVE, WHICH IS MADE EXPRESSLY IN LIEU OF ALL OTHER WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AND VERILINK HEREBY DISCLAIMS ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT, AND ALL OTHER IMPLIED WARRANTIES ON THE PART OF VERILINK. VERILINK DOES NOT WARRANT THAT THE BUYER'S USE OF THE GOODS WILL BE UNINTERRUPTED, SECURE, OR ERROR-FREE. Buyer agrees that no oral or written representation, advice, advertisement or other statement by Verilink, its reseller, agent, employee, or representative constitutes any warranty, guarantee or modification of the foregoing disclaimer and Limited Warranty, and Buyer acknowledges that no person, including resellers, agents, employees, or representatives of Verilink, is authorized to assume for Verilink any other liability on its behalf except as set forth in this paragraph.
- III. **LIMITATION ON LIABILITY.** IN NO EVENT SHALL VERILINK, ITS OFFICERS, DIRECTORS, EMPLOYEES, OR SUPPLIERS BE LIABLE FOR SPECIAL, CONSEQUENTIAL, EXEMPLARY, INCIDENTAL, OR PUNITIVE DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION, DATA LOSS, DAMAGE TO EQUIPMENT, OR THE LIKE), REGARDLESS OF WHETHER THE CLAIM IS BASED ON BREACH OF WARRANTY, BREACH OF CONTRACT, STRICT LIABILITY, OR OTHER LEGAL THEORY, EVEN IF VERILINK OR ITS AGENT WAS ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT WILL VERILINK'S LIABILITY TO BUYER OR ANY SUCCESSOR TO BUYER EXCEED THE PRICE PAID FOR THE APPLICABLE GOODS.
- IV. **LIMITED WARRANTY CONDITIONS.** The Limited Warranty shall be void (i) with respect to any Goods that have been repaired or altered outside Verilink's factory, unless Verilink specifically authorized such repairs or alterations; (ii) in the event parts not made or recommended by Verilink are used by Buyer in the Goods; or (iii) if the Goods are used by Buyer other than in the manner intended by Verilink or other than in conformance with operating instructions and specifications provided by Verilink.
- V. **MODIFICATIONS BY VERILINK.** Minor deviations from specifications that do not materially affect performance of the Goods covered hereby, as mutually agreed upon by Verilink and Buyer, shall not be deemed to constitute a breach of the Limited Warranty. Verilink also reserves the right to discontinue Goods and change specifications for Goods without notice, provided such changes do not adversely affect the performance of the Goods manufactured by Verilink or do not reduce performance below any applicable contract specifications between Verilink and the Buyer. Verilink also reserves the right to make product improvements without incurring any obligations or liability to make the same changes in Goods previously manufactured or purchased. Non-payment of any invoice rendered within the stated payment terms automatically suspends the application of, but not the running of, the Limited Warranty for the duration of the non-payment.
- VI. **AMENDMENT OF WARRANTY TERMS.** These terms and conditions of this Hardware Limited Warranty may be revised by Verilink from time to time in its sole discretion. The terms and conditions in effect at the time of purchase will apply to such Goods.
- VII. **RETURN OF GOODS.** If for any reason the Buyer must return a Verilink product, it must be returned to the factory, shipping prepaid, and packaged to the best commercial standard for electronic equipment. Verilink will pay shipping charges for delivery on return. The Buyer is responsible for mode and cost of shipment to Verilink. The Buyer must have a Return Material Authorization (RMA) number marked on the shipping package. Products sent to Verilink without RMA numbers will be returned to the sender, unopened, at the sender's expense. A product sent directly to Verilink for repair must first be assigned an RMA number. The Buyer may obtain an RMA number by calling the Verilink Customer Service Center at 1.800.926.0085, extension 2282 or 2322. When calling Verilink for an RMA, the Buyer should have the following information available:
  - Model number and serial number for each unit
  - Reason for return and symptoms of problem
  - Purchase order number to cover charges for out-of-warranty items
  - Name and phone number of person to contact if Verilink has questions about the unit(s).A return address will be provided at the time the RMA number is issued. The standard delivery method for return shipments is Standard Ground for domestic returns and International Economy for international returns (unless otherwise specified).
- VIII. **GOVERNING LAW.** This Agreement is governed by the laws of the State of Alabama, U.S.A., without reference to its conflicts of law provisions. The provisions of the UN Convention on Contracts for the International Sale of Goods shall not apply.