DSLPipe Reference Guide

Ascend Communications

Part Number 7820-0519-001 June 2, 1997

FCC Part 15

Warning: 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. 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. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

The authority to operate this equipment is conditioned by the requirement that no modifications will be made to the equipment unless the changes or modifications are expressly approved by Ascend.

Canadian Notice

Note: The Canadian Department of Communications label identifies certified equipment. This certification means that the equipment meets certain telecommunications network protective, operational and safety requirements. The Department does not guarantee the equipment will operate to the user's satisfaction.

Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. In some cases, the company's inside wiring associated with a single line individual service may be extended by means of a certified connector assembly (telephone extension cord). The customer should be aware that compliance with the above conditions may not prevent degradation of service in some situation.

Repairs to certified equipment should be made by an authorized Canadian main-

tenance facility designated by the supplier. Any repairs or alterations made by the user to this equipment, or equipment malfunctions, may give the telecommunications company cause to request the user to disconnect the equipment.

Users should ensure for their own protection that the electrical ground connections of the power utility, telephone lines and internal metallic water pipe system, if present, are connected together. This precaution may be particularly important in rural areas.

Caution: Users should not attempt to make such connections themselves, but should contact the appropriate electric inspection authority, or electrician, as appropriate.

The *Load Number (LN)* assigned to each terminal device denotes the percentage of the total load to be connected to a telephone loop which is used by the device, to prevent overloading. The termination on a loop may consist of any combination of devices subject only to the requirement that the total of the Load Numbers of all the devices does not exceed 100.

This equipment does not support line loopbacks.

Warning: THE 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 PRESENT APPAREIL NUMERIQUE N'EMET PAS DE BRUITS RADIOELECTRIQUES DEPASSANT LES LIMITES APPLICABLES AUX APPAREILS NUMERIQUES DE LA CLASSE A PRESCRITES DANS LE REGLEMENT SUR LE BROUILLAGE RADIOELECTRIQUE EDICTE PAR LE MINISTERE DES COMMUNICATIONS DU CANADA.

Parameter Reference

1

This chapter lists all of the parameters in the DSLPipe menus.

Note: Some of the parameters in this section do not apply to the DSLPipe or are not implemented at this time.

Parameters are listed in alphabetical order. Each listing provides information in this format:

Parameter Name

Description: The Description text explains the parameter.

Usage: The Usage text explains how to use the parameter.

Example: The Example text shows you an example entry or setting.

Dependencies: The Dependencies text tells you what other information you need to configure and use the parameter.

Parameter Location: The Parameter Location text shows you where to find the parameter.

See Also: The See Also text points you to related parameters.

Alphabetical parameter listing

2nd Adrs

Description: This parameter gives the DSLPipe an IP address on a remote subnet. When you set the 2nd Adrs parameter, the DSLPipe has a second IP address in addition to the IP Adrs value on its local Ethernet interface. Both IP addresses are treated equally, except that IP Adrs is the only one used for authentication over the WAN. Setting a second address doubles the number of entries in the DSLPipe routing table. The DSLPipe advertises a route from 2nd Adrs to IP Adrs and a route from IP Adrs to 2nd Adrs.

One use of 2nd Adrs is to advertise routes that would not otherwise be advertised. For example, suppose both the DSLPipe and Router2 have a route to the network 200.0.2.0. Both are on the same subnet. The device with the lower hop count to the destination network sends all the traffic destined for that network.

Now, suppose the DSLPipe has 2nd Adrs=200.0.2.9/28 and Router2 has 2nd Adrs=200.0.2.10/28 on the same subnet. The DSLPipe assumes that all subnets in the 200.0.2.0 network have the same subnet mask (/28). In addition, the DSLPipe has an address for a router at 200.0.2.129/28 and Router2 has an address for a router at 200.0.2.65/28. Because the DSLPipe and Router2 assume that /28 is the subnet mask, the DSLPipe routes traffic only to the 200.0.2.129/28 subnet and Router2 routes traffic only to the 200.0.2.65/28 subnet. The traffic to the 200.0.2.0 network is thereby shared.

Using the 2nd Adrs parameter also provides an easy way to change the IP address of the DSLPipe. When all routers know the DSLPipe by both its IP Adrs value and its 2nd Adrs value, you can safely turn off 2nd Adrs and put the new address in IP Adrs.

Usage: Press Enter to open a text field. Then, type the IP address of the DSLPipe on the remote subnet.

The address consists of four numbers between 0 and 255, separated by periods. Use a slash to separate the optional netmask from the address. The IP address must be a valid address on the remote subnet.

The default value is 0.0.0.0/0.

Press Enter to close the text field.

Dependencies: Keep this additional information in mind:

- If you do not know the right IP address to enter, you must obtain it from the network administrator.

  Do not attempt to configure an IP address by guesswork!
- Do not use 2nd Adrs to force interface-based routing; it is not designed as a second WAN address.

Parameter Location: Ethernet Profile, Mod Config/Ether options

See Also: IP Adrs

Active

Description: This parameter appears in a Connection Profile, a Frame Relay Profile, and a Static Rtes Profile. Its functionality differs depending on the profile:

- In a Connection Profile or a Frame Relay Profile, the Active parameter activates or deactivates the profile.

  If you activate a profile, it is available for use. If you deactivate a profile, it is not available for use.
- In a Static Rtes Profile, the Active parameter determines whether the route defined in the profile appears in the DSLPipe static routing table.

Usage: Press Enter to toggle between Yes and No.

- Yes activates the profile or specifies that the route can appear in the static routing table.

  Yes is the default.
- No deactivates the profile, keeps the route from appearing in the static routing table, or removes the route if it is already in the table.

  A dash appears before each deactivated profile or route.

Parameter Location: Connection Profile, Connections
Frame Relay Profile, Frame Relay
Static Rtes Profile, any profile

Adv Dialout Routes

Description: This parameter specifies whether the DSLPipe should continue to advertise dialout routes for which it is currently unable to establish a WAN connection. The default behavior of the DSLPipe is to advertise routes regardless of the condition of its lines.

Note: This parameter is intended for use when two or more Ascend units on the same network are configured with redundant profiles and routes. It is not necessary to use this feature if you have a single DSLPipe unit.

Usage: Press Enter to toggle between the choices.

- Always

  This setting causes the DSLPipe to always advertise its IP routes. Use this setting unless you have redundant Ascend units or don't use dialout routes.

  Always is the default.

- Trunks Up

  This setting causes the DSLPipe to stop advertising ("poison") its IP dialout routes if it temporarily loses the ability to dial out.

  This feature was developed in response to a problem that occurred when two or more Ascend units on the same network were configured with redundant profiles and routes. If one of the redundant DSLPipe units lost its dialout lines temporarily, it continued to receive outbound packets that should have been forwarded to the redundant DSLPipe.

Parameter Location: Ethernet Profile: Ethernet→Mod Config

Add Pers

Description: This parameter specifies the number of seconds that average line utilization (ALU) for transmitted data must exceed the threshold indicated by the Target Util parameter before the DSLPipe begins adding bandwidth to a session. The DSLPipe determines the ALU for a session by using the algorithm specified by the Dyn Alg parameter.

When utilization exceeds the threshold for a period of time greater than the value of the Add Pers parameter, the DSLPipe attempts to add a channel. Using the Add Pers and Sub Pers parameters prevents the system from continually adding

and subtracting bandwidth, and can slow down the process of allocating or removing bandwidth.

Usage: Press Enter to open a text field. Then, type a number between 1 and 300. Press Enter again to close the text field.

When the DSLPipe is using MP+ (Encaps=MPP), the default value is 5.

Dependencies: Keep this additional information in mind:

- Additional channels must be available, and the number of channels added cannot exceed the amount specified by the Max Ch Count parameter.
- Add Pers in the Answer Profile applies to incoming calls for which no Connection Profile exists; if a Connection Profile exists, the setting of its Add Pers parameter takes precedence.
- If Profile Reqd=Yes in the Answer Profile, Add Pers does not apply (Add Pers=N/A) in the Answer Profile.
- Add Pers and Sub Pers have little or no effect on a system with a high Sec History value.

  If the value of Sec History is low, the Add Pers and Sub Pers parameters provide an alternative way to ensure that spikes must persist for a certain period of time before the system responds.

Parameter Location: Answer Profile, Answer/PPP options
Connection Profile, Connections/Encaps options

See Also: Dyn Alg, Max Ch Count, Base Ch Count, Sec History, Sub Pers, Target Util

Alarm

Description: This parameter specifies whether the DSLPipe sends a traps-PDU (Protocol Data Unit) to the SNMP manager when an alarm event occurs.

SNMP (Simple Network Management Protocol) provides a way for computers to share networking information. In SNMP, two types of communicating devices exist: agents and managers. An agent (such as the DSLPipe) provides networking information to a manager application running on another computer. The agents

and managers share a database of information, called the Management Information Base (MIB).

A trap is a mechanism in SNMP for reporting system change in real time. To report system change, the DSLPipe sends a traps-PDU across the Ethernet interface to the SNMP manager.

Alarm events are defined in RFC 1215 and include the following:

- coldStart

  This event indicates that the DSLPipe started up from a power-off condition.
- warmStart

  This event indicates that the DSLPipe started up from a power-on condition, typically by a system reset.
- linkDown

  This event indicates that a WAN link or Ethernet interface has gone offline.
- linkUp

  This event indicates that a WAN link or Ethernet interface has come online.

Usage: Press Enter to toggle between Yes and No.

- Yes specifies that the DSLPipe traps alarm events.
- Yes is the default.
- No specifies that the DSLPipe does not trap alarm events.

Parameter Location: SNMP Traps Profile, SNMP Traps

AnsOrig

Description: This parameter specifies whether the DSLPipe can initiate calls, receive them, or both. The setting you choose affects calls to or from the destination specified by the Station and LAN Adrs parameters in the Connection Profile.

Usage: Press Enter to cycle through the choices.

- Both specifies that the DSLPipe can initiate calls to the destination specified in the Connection Profile, and that it can receive calls from that destination as well.

  Both is the default.

- Call Only specifies that the DSLPipe can dial out to the destination specified in the Connection Profile, but cannot answer calls from that destination.
- Ans Only specifies that the DSLPipe can receive calls from the destination specified in the Connection Profile, but cannot initiate calls to that destination.

Dependencies: The AnsOrig parameter does not apply (AnsOrig=N/A) when all channels of the link are nailed up (Call Type=Nailed).

Parameter Location: Connection Profile, Connection/Telco options

See Also: LAN Adrs, Station

APP Host

Description: This parameter specifies the IP address of the host that runs the APP Server Utility. Enigma Logic SafeWord AS and Security Dynamics ACE authentication servers are examples of APP servers.

Usage: Press Enter to open a text field. Then, type the IP address of the authentication server.

The address consists of four numbers between 0 and 255, separated by periods. Separate the optional netmask from the address using a slash. The default value is 0.0.0.0/0. The default setting specifies that no APP server is available.

Press Enter again to close the text field.

Example: `200.65.207.63/29`

Dependencies: Keep this additional information in mind:

- APP Host applies only to outgoing calls using security card authentication.
- You must set Send Auth=PAP-Token and APP Server=Yes for the APP Host parameter to have any effect.
- The APP Server utility must be running on a UNIX or Windows workstation on the local network.

Parameter Location: Ethernet Profile, Mod Config/Auth

See Also: APP Server, Send Auth

APP Port

Description: This parameter specifies the UDP port number monitored by the APP server identified in the APP Host parameter.

Usage: Press Enter to open a text field. Then, type a UDP port number. Valid port numbers range from 0 to 65535. The default value is 0, which indicates that no UDP port is being monitored by the APP server. Press Enter again to close the text field.

Example: 35

Dependencies: Keep this additional information in mind:

- The APP Port parameter applies only to outgoing calls using security card authentication.
- You must set Send Auth=PAP-Token and APP Server=Yes for the APP Port parameter to have any effect.
- The APP Server utility must be running on a UNIX or Windows workstation on the local network.

Parameter Location: Ethernet Profile, Mod Config/Auth

See Also: APP Server, Send Auth

APP Server

Description: This parameter lets you enable responses to security card password challenges by using the APP Server utility on a UNIX or Windows workstation.

Usage: Press Enter to toggle between Yes and No.

- Yes enables the DSLPipe to respond to password challenges by using the APP Server utility.
- No disables responses from the APP Server utility.
  Select No to authenticate calls through the terminal server. No is the default.

Dependencies: Keep this additional information in mind:

- You must set Send Auth=PAP-Token for the APP Server parameter to have any effect.
- The APP Server utility must be running on a UNIX or Windows workstation on the local network.

Parameter Location: Ethernet Profile, Mod Config/Auth

See Also: Send Auth

Auto Logout

Description: This parameter specifies whether the DSLPipe automatically logs out when a device disconnects from the its control port or when the DSLPipe loses power. The disconnected device can be a terminal, a VT-100, a terminal emulator, or a modem.

A terminal is a computer that does not have its own processor; it must connect to a computing device called a terminal server in order to use its CPU. VT100, ANSI, and TTY are all types of terminals.

A terminal emulator is a program that makes your computer act like a terminal so that you can connect to a terminal server. All processing takes place remotely.

A modem (MOdulator/DEModulator) is a device that takes digital data from a computer, translates (or modulates) the 1s and 0s into analog form, and sends the data over an analog communications channel. The receiving modem demodulates the analog signal into digital data and sends it to the computer to which it is attached.

Usage: Press Enter to toggle between Yes and No.

- Yes enables automatic logout.
- No disables automatic logout.
  No is the default.

Parameter Location: System Profile, Sys Config

Aux Send PW

Description: This parameter specifies the password that the DSLPipe sends when it adds channels to a security-card MP+ call that uses PAP-TOKEN-CHAP authentication. The DSLPipe obtains authentication of the first channel of this MP+ call from the hand-held security card.

Usage: Press Enter to open a text field. Then, type a password. This password must match the one set up for your DSLPipe in the RADIUS users file on the NAS (Network Access Server). Press Enter again to close the text field.

Dependencies: Aux Send PW applies only to outgoing MP+ calls in which Send Auth=PAP-TOKEN-CHAP.

Parameter Location: Configure Profile,
Connection Profile, Connections/Encaps options

See Also: Send Auth

Backup

Description: This parameter specifies the profile name of a backup connection.

If the primary connection is unavailable, the DSLPipe automatically diverts traffic to the backup connection. A connection can fail if, for example, a frame relay connection loses a Permanent Virtual Circuit, the physical link fails, or if a T1 line is in a red alarm condition. When the primary connection is restored, traffic again uses the primary connection.

When you use the backup connection, the DSLPipe does not move routes to the backup profile. Therefore, the IP routes shown in the terminal server display may be incorrect, although statistical counts reflect the change.

Usage: Press Enter to open a text field. Then, type the name of the profile that you want to act as the backup. The name you specify must match the value of the Name parameter in a local Connection Profile. The backup connection can be switched or nailed up.

Dependencies: Keep this additional information in mind:

- Do not create nested backup connections.

- The Backup parameter applies only to nailed-up connections (for which Call Type=Nailed or Nailed/MPP); otherwise, Backup=N/A.
- Parameters that you define in the primary Connection Profile do not automatically apply to the backup Connection Profile.

  For example, if you set the primary Connection Profile to filter Telnet packets, you must set the backup profile to filter Telnet packets as well. Outgoing Frame Relay packets are the only packets that follow the primary Connection Profile definitions. All other packets follow the backup Connection Profile definitions.
- Backup is intended for situations in which the remote device (such as a data center) goes out of service; the backup call is made to a backup data center.

  Backup is not intended to provide alternative lines for getting to a single destination.
- Do not confuse the Backup parameter with the Secondary parameter. A Backup Connection Profile is used to re-establish an existing connection that has terminated; a Secondary Connection Profile is used to establish a new connection if the primary Connection Profile cannot. That is, the Secondary Connection provides an alternative line for a single destination, which the Backup Connection Profile does not.

Parameter Location: Connection Profile: Ethernet, Connections, Any Connection Profile, Session Options

See Also: Name, Secondary

Base Ch Count

Description: This parameter specifies the initial number of channels the DSLPipe sets up when originating calls for a PPP, MP+, or MP multichannel link.

Usage: Press Enter to open a text field. Then, type a number.

The maximum value of the Base Ch Count parameter depends on the encapsulation method that both ends of the link use.

- For an PPP link (for which Encaps=PPP), the Base Ch Count is always 1.

- For an MP+ or MP link (for which Encaps=MPP), the amount you specify is limited by the number of channels available, but the device at the remote end of the link must also support MP+ or MP.

No matter what type of link you use, the amount you specify cannot exceed the maximum channel count set by the Max Ch Count parameter.

Press Enter to close the text field.

Dependencies: Keep this additional information in mind:

- You can determine the base bandwidth of a call by multiplying the value of the Base Ch Count parameter by the value of the Data Svc parameter.
- The Base Ch Count parameter does not apply (Base Ch Count=N/A) when all channels of the link are nailed up (Call Type=Nailed).
- For optimum MP+ performance, both sides of a connection must set these parameters to the same values:
  - Base Ch Count (in the Connection Profile)
  - Min Ch Count (in the Answer Profile and the Call Profile)
  - Max Ch Count (in the Answer Profile and the Connection Profile)

Parameter Location: Connection Profile, Connections/Encaps options

See Also: Data Svc, Max Ch Count, Min Ch Count

Bill

Description: This parameter specifies a billing number for charges incurred on the line. If you do not enter a billing number, the telephone company bills charges to the telephone number assigned to the line.

Your carrier determines the billing number, and uses it to sort your bill. If you have several departments, and each department has its own Bill #, your carrier can separate and tally each department's usage.

Usage: Press Enter to open a text field. Then, type a telephone number. You can specify up to ten characters, and you must limit those characters to the following:

```
1234567890()[]!z-*# |
```

The DSLPipe uses the Bill # parameter differently depending on the type of line you use:

- Bill # for outgoing calls on an ISDN BRI line applies only to installations in Australia.

Press Enter to close the text field.

Example: These specifications are valid for Bill #:

```
5105551972
```

```
510-555-1972
```

Parameter Location: Connection Profile, Connections/Telco options

See Also: Calling #, Clid Auth

Bridge

Description: This parameter enables or disables protocol-independent bridging for a call. If you disable bridging, you must enable routing by setting Route IP=Yes or Route IPX=Yes in the Connection Profile.

Usage: Press Enter to cycle through the choices.

- Yes enables bridging.
- No disables bridging.

  No is the default.

Dependencies: The effect of the Bridge parameter depends upon how you set the Route IP and Route IPX parameters.

Bridge and Route IP

- If Bridge=Yes and Route IP=Yes, the DSLPipe routes IP packets, and bridges all other packets.
- If Bridge=Yes and Route IP=No, the DSLPipe bridges all packets.
- If Bridge=No and Route IP=Yes, the DSLPipe routes only IP packets.
- If Bridge=No and Route IP=No, an error occurs and you cannot save the profile

You must enable bridging or routing, or both.

Bridge and Route IPX

- If Bridge=Yes and Route IPX=Yes, the DSLPipe routes IPX packets, and bridges all other packets.
- If Bridge=Yes and Route IPX=No, the DSLPipe bridges all packets.
- If Bridge=No and Route IPX=Yes, the DSLPipe routes only IPX packets.
- If Bridge=No and Route IPX=No, an error occurs and you cannot save the profile.

  You must enable bridging or routing, or both.

Additional Dependencies

- Bridging must be enabled on both the dialing and answering sides of the link.

  The Connection Profile on the dialing side and the Answer Profile on the answering side must both set the Bridge parameter to Yes. Otherwise, the DSLPipe does not bridge the packets.
- The Bridge parameter does not apply (Bridge=N/A) if you turn off bridging in the Ethernet Profile (Bridging=No).
- Bridge in the Answer Profile applies to incoming calls for which no Connection Profile exists; if a Connection Profile exists, the setting of its Bridge parameter takes precedence.
- If Profile Reqd=Yes in the Answer Profile, Bridge does not apply (Bridge=N/A) in the Answer Profile.
- If Profile Reqd=Yes in the Answer Profile, you must set Bridge=Yes in the answering Connection Profile.
- Do not confuse the Bridge parameter with the Bridging parameter.
  - The Bridge parameter in the Answer Profile applies only to connections that the DSLPipe answers.
  - The Bridge parameter in the Connection Profile applies only to a specific connection.
  - The Bridging parameter globally enables or disables bridging.

Parameter Location: Answer Profile, Answer/PPP options
Connection Profile, Connections

See Also: Bridging, Encaps, Route IP, Route IPX

Bridging

Description: This parameter allows you to globally enable or disable bridging for all connections that the DSLPipe answers or dials.

Usage: Press Enter to toggle between Yes and No.

- Yes globally enables bridging.

  When you choose this setting, the DSLPipe operates in promiscuous mode. The Ethernet controller in the DSLPipe accepts all packets and passes them up the protocol stack for a higher-level decision on whether to route, bridge, or reject them. This mode is appropriate if you are using the DSLPipe as a bridge.

- No globally disables bridging.

  When you choose this setting, the Ethernet controller filters out all packets except broadcast packets and those explicitly addressed to the DSLPipe. The Bridge parameter in the Connection and Answer Profiles, and all parameters exclusively associated with bridging, are set to N/A.

  This mode significantly reduces processor and memory overhead when the DSLPipe is routing, and can result in much better performance, especially in moderate to heavily loaded networks.

  No is the default.

Dependencies: Do not confuse the Bridge parameter in the Answer and Connection Profiles with the Bridging parameter in the Ethernet Profile.

- The Bridge parameter in the Answer Profile applies only to connections that the DSLPipe answers.
- The Bridge parameter in the Connection Profile applies only to a specific connection.
- The Bridging parameter in the Ethernet Profile globally enables or disables bridging.

Parameter Location: Ethernet Profile, Mod Config

See Also: Bridge

Callback

Description: This parameter enables or disables the callback feature.

When you enable the callback feature, the DSLPipe hangs up after receiving an incoming call that matches the one specified in the Connection Profile. The DSLPipe then calls back the device at the remote end of the link using the Dial # specified in the Connection Profile.

You can use this parameter to tighten security, as it ensures that the DSLPipe always makes a connection with a known destination.

Usage: Press Enter to toggle between Yes and No.

- Yes enables the callback feature.
- No disables the callback feature.
  No is the default.

Dependencies: Keep this additional information in mind:

- The Callback parameter does not apply (Callback=N/A) if all channels of the link are nailed up (Call Type=Nailed).
- If you set Callback=Yes, you must also set AnsOrig=Both, because the Connection Profile must both answer the call and call back the device requesting access.
  By the same token, any device calling into a Connection Profile set for callback must be configured to both dial calls and answer them.

Parameter Location: Connection Profile, Connections/Telco options

See Also: AnsOrig, Call Type, Dial #

Call Filter

Description: This parameter enables you to specify a call filter to plug into an Answer Profile or a Connection Profile.

By default, any packet destined for the WAN causes the DSLPipe to place a call. In addition, by default, every packet resets the idle timer, the indicator that the DSLPipe uses to know when to clear a call. When you set up a call filter, only

those packets that the call filter forwards can initiate a call or reset the Preempt or Idle parameters.

Usage: Press Enter to open a text field. Then, type a number between 0 and 16. The number corresponds to a call filter you created in the Filters menu. Press Enter again to close the text field.

When you set Call Filter to 0 (zero), the DSLPipe forwards all packets. Zero is the default.

Dependencies: Keep this additional information in mind:

- If all channels of a link are nailed up (Call Type=Nailed in the Connection Profile), the Call Filter parameter does not apply (Call Filter=N/A) in both the Answer and Connection Profiles.
- The DSLPipe applies a call filter after applying a data filter; only those packets that the data filter forwards can reach the call filter.
- If IPX client bridging is in use (Handle IPX=Client), set the Call Filter parameter to 0 (zero).
- Call Filter in the Answer Profile applies to incoming calls for which no Connection Profile exists; if a Connection Profile exists, the setting of its Call Filter parameter takes precedence.
- If Profile Reqd=Yes in the Answer Profile, Call Filter does not apply (Call Filter=N/A) in the Answer Profile.

Parameter Location: Connection Profile, Connections/Session options

See Also: Call Type, Data Filter, Filter menu, Forward, More, Profile Reqd

Calling

Description: This parameter specifies the calling party's phone number (also called CLID). If authentication by CLID is enabled by the Clid Auth parameter, the DSLPipe compares the CLID of incoming calls to the value of the Calling # parameter.

Usage: Press Enter to open a text field. Then, enter the calling party's phone number. You can enter up to 20 characters. Press Enter again to close the text field.

Parameter Location: Connection Profile, Connections

See Also: Clid Auth

Call Type

Description: This parameter appears in a Connection Profile, and a Frame Relay Profile. Its functionality differs depending on the profile:

- In a Connection Profile, the Call Type parameter specifies a type of link.
- In a Frame Relay Profile, the Call Type parameter specifies the type of connection to a frame relay switch

  Frame Relay is an HDLC-based packet protocol that enables you to send data to a destination using one or more frame relay switches within a private network or a public carrier's network. HDLC stands for High Level Data Link Control.

  From the viewpoint of the DSLPipe, a frame relay switch is an endpoint for all DLCIs (Data Link Connection Indicators) connecting to it. A DLCI identifies a Connection Profile as a logical link; because more than one Connection Profile can connect to a frame relay switch, a physical circuit can carry more than one logical link. The DLCI parameter enables the frame relay switch to identify each Connection Profile.

  The frame relay switch connects the endpoints of the DLCIs to each other to make a virtual permanent circuit to which users can connect. The circuit acts like a wire between two endpoints with a fixed maximum bandwidth.

Usage: The settings you can choose for the Call Type parameter differ depending on the profile.

Call Type Settings

In a Connection Profile or a Frame Relay Profile, you can specify any of these settings:

Nailed

This setting specifies a link that consists entirely of nailed-up channels.

- In a Connection Profile, you must use the Group parameter to specify which channels are in the connection.

- In a Frame Relay Profile, you must use the Nailed Grp parameter to specify which channels are in the connection.

  The Nailed setting is the default in a Frame Relay Profile.

Switched

This setting specifies a link that consists entirely of switched channels.

- In a Connection Profile, the Telco options parameters specify the bandwidth of the connection, as well as other features of the switched link.

  The maximum number of channels on the link is the number set by Max Ch Count.

  The Switched setting is the default in a Connection Profile.

- In a Frame Relay Profile, you must specify the Switched setting if the DSLPipe always initiates the connection to the frame relay switch; if a device at the remote end of the link initiates bridging or routing sessions, do not choose Switched.

  If you choose Switched, you must specify the bandwidth of the switched connection in the Data Svc parameter of the Frame Relay Profile.

Nailed/MPP (Connection Profile only)

This setting specifies a link that consists of both nailed-up and switched channels. The DSLPipe establishes this connection whenever any of its nailed-up or switched channels are connected end-to-end. If a Nailed/MPP link is down and the nailed-up channels are down, the link cannot re-establish itself until the DSLPipe brings up one or more of the nailed-up channels, or dials one or more switched channels.

Typically, the switched channels are dialed when the DSLPipe receives a packet whose destination is the unit at the remote end of the Nailed/MPP connection. The packet initiating the switched call must come from the caller side of the connection.

If a channel in a call fails for any reason, and the total number of channels in the Nailed/MPP connection falls below the value of the Min Ch Count parameter, the DSLPipe tries to add a switched channel to bring the connection back up to the minimum.

If a failed channel is in the group specified by the Group parameter, that channel is replaced with a switched channel, even if the call is online with more than the minimum number of channels. Failed nailed-up channels are replaced by

switched channels, regardless of the Min Ch Count setting.

Perm/Switched (Connection Profile only)

This setting specifies a permanent switched connection.

A permanent switched connection is an outbound call that attempts to remain up at all times. If the unit or central switch resets, or if the link is terminated, the permanent switched connection attempts to restore the link at ten-second intervals.

Use this setting if your telephone company charges for each incoming and outgoing connection attempt, but does not charge for connection time on local calls. Ascend's regular bandwidth-on-demand feature conserves connection time but causes many connection attempts. A permanent switched connection performs the opposite function—it conserves connection attempts but causes a long connection time.

For the answering device at the remote end of the permanent switched connection, we recommend that the Connection Profile be configured to answer calls but not originate them. If the remote device initiates a call, the DSLPipe simply does not answer it. This situation could result in repeated charges for calls that have no purpose. To keep the remote device from originating calls, set AnsOrig=Ans Only for that device.

Dependencies: Keep this additional information in mind:

- The DSLPipe determines the minimum number of channels by the value of the Min Ch Count parameter or the number of nailed-up channels in the group, whichever is greater.

  The DSLPipe does not count a nailed-up channel that is unused.
- The DSLPipe adds or subtracts switched channels on a Nailed/MPP connection as required by the parameters on either side of the connection.

  Each side makes its calculations based on the traffic received at that side. If the two sides of the connection disagree on the number of channels needed, the side requesting the greater number prevails.
- The DO Hangup parameter works only from the caller side of the connection when you choose Nailed/MPP.
- The Idle parameter works for both sides of the connection when you choose Nailed/MPP.

However, if the answering side of the connection brings the link down because of an Idle timeout, the calling side can bring it back up.

Dependencies: Keep this information in mind concerning the Call Type parameter in a Connection Profile or a Frame Relay Profile:

- If the link consists entirely of nailed channels (Call Type=Nailed), the Callback feature does not apply (Callback=N/A).
- If the link consists entirely of switched channels (Call Type=Switched), the Group parameter does not apply (Group=N/A).
- In a Connection Profile, the encapsulation must be MPP (Encaps=MPP) in order to select Call Type=Nailed/MPP.
- When you set Call Type=Perm/Switched in a Connection Profile, the following parameters do not apply and are set to N/A:
  - AnsOrig=N/A because permanent switched connections are always outbound.
  - Callback=N/A because the device will not answer calls for a permanent switched connection.
  - Idle=N/A because a permanent switched connection is up permanently.
  - Backup=N/A because permanent switched connections do not support backup calls.
- The Idle and Backup parameters in the Session Options submenu are also set to N/A when Call Type=Perm/Switched.

Parameter Location: Connection Profile, Connections/Telco options
Frame Relay Profile, Frame Relay

See Also: Callback, Call Mgm, Data Svc, DLCI, Group, Idle, Max Ch Count, Min Ch Count, and Nailed Grp.

Chan Usage

Description: This parameter specifies how the B channels are used on an ISDN line. Typically, both channels are switched. The first setting in each pair represents B1 channel usage, and the second represents the B2 channel usage.

Switched means that the channel uses dial-in switched service at either 64 kbps (the default) or 56 kbps per B channel. The B channels can be used singly or

together for one or more simultaneous dial-ups on the same line, depending on active sessions and bandwidth demands.

Unused means that the channel is not used for dial-in connections. The DSLPipe will have access only to the other channel, which limits the bandwidth to 64 kbps.

Leased means that the channel is leased (dedicated to a permanent “nailed” connection to one remote network).

Super Dig 128 is a feature added for ISDN connections in Japan. It concatenates the two B channels into a single 128 kbps pipe on a nailed-up connection, delivering unrestricted 128 kbps bandwidth. Only one dial-up phone number is assigned, and only one call can be supported at one time. The switch type must be set to JAPAN.

Usage: Press Enter to cycle through the choices.

- Switch/Switch (default)
- Super Dig 128
- Unused/Switch
- Switch/Unused
- Leased/Unused
- Unused/Leased
- Switch/Leased
- Leased/Switch

Location: Configure...

Clid Auth

Description: This parameter specifies whether the DSLPipe uses the calling party’s phone number to authenticate incoming calls. CLID stands for calling party ID.

Usage: Press Enter to cycle through the choices.

- Ignore indicates that calling party information is not required for authentication.
- Prefer specifies that whenever CLID is available, the calling party’s phone number must match the Calling # parameter before the DSLPipe answers the call.

If CLID is not available or if the DSLPipe cannot find a match to a calling number, the DSLPipe applies authentication using the Recv Auth or Password Reqd parameters.

- Required indicates that the calling party's phone number must match the value of the Calling # parameter before the DSLPipe can answer the call.

  If CLID is not available, the DSLPipe does not answer the call

Dependencies: Keep this additional information in mind:

- In some installations, the WAN provider might not be able deliver CLIDs, or individual callers might choose to keep their CLIDs private; in addition, CLID is not available without end-to-end ISDN service on the call and ANI (Automatic Number Identification) from your WAN provider.

  Ask your WAN provider whether the calling party number is conveyed by the network to the receiving party. In some cases, the network does not deliver the calling party number, such as when the DSLPipe is behind some PBXs.
- You cannot use a Connection Profile in which AnsOrig=Call Only to authenticate incoming calls.
- If a call is CLID authenticated, name-password authentication might also be required, but the parameters of the call are established only by the CLID authentication.

Parameter Location: Answer Profile, Answer

See Also: AnsOrig, Calling #

Comm

Description: This parameter specifies an SNMP (Simple Network Management Protocol) community name. The string you specify becomes a password that the DSLPipe sends to the SNMP manager when an SNMP trap event occurs. The password authenticates the sender identified by the IP address in the IP Adrs parameter.

SNMP provides a way for computers to share networking information. In SNMP, two types of communicating devices exist: agents and managers. An agent (such as the DSLPipe) provides networking information to a manager application

running on another computer. The agents and managers share a database of information, called the Management Information Base (MIB).

A trap is a mechanism in SNMP for reporting system change in real time. To report system change, the DSLPipe, sends a traps-PDU across the Ethernet interface to the SNMP manager. A complete list specifying the events that cause the DSLPipe to send a traps-PDU appears in the Ascend Enterprise Traps MIB.

Usage: Press Enter to open a text field. Then, type the community name. You can enter an alphanumeric string containing up to 31 characters. The default is [ ]. Press Enter again to close the text field.

Dependencies: To turn off SNMP traps, leave the Comm parameter blank and set Dest=0.0.0.0.

Parameter Location: SNMP Traps Profile, SNMP Traps

See Also: Dest

Compare

Description: This parameter specifies how a packet's contents are compared to the value specified in the filter.

After applying the Offset, Mask, and Length values to reach the appropriate location in a packet, the DSLPipe compares the packet's contents to the Value parameter. If Compare is set to Equals (the default), the DSLPipe applies the filter if the packet data is identical to the setting of the Value parameter. If Compare is set to NotEquals, the DSLPipe applies the filter if the packet data is not identical to the setting of the Value parameter.

Usage: Press Enter to cycle through the choices.

- Equals indicates that a match occurs when data in the packet equals the conditions specified in the filter.

  Equals is the default
- NotEquals indicates that a match occurs when data in the packet does not equal the conditions specified in the filter.

Dependencies: Keep this additional information in mind:

- Compare=N/A if the filter is not Valid or if the filter type is IP.

Parameter Location: Filter Profile, Filters

See Also: Length, Mask, Offset, Value

Connection #

Description: This parameter can appear in a Bridging Profile or an IPX Route Profile. Its functionality differs depending on the profile:

- In a Bridging Profile, this parameter specifies the number of a Connection Profile through which you can reach the node specified by the Enet Adrs parameter of the Bridging Profile.

  The IP address contained in the Connection Profile's LAN Adrs parameter corresponds to the MAC address contained in the Bridging Profile's Enet Adrs parameter. The DSLPipe dials the Connection Profile when a node on its LAN sends a packet whose destination matches the Enet Adrs value in the profile.
- In an IPX Route Profile, this required parameter identifies the number of the Connection Profile through which you can reach the NetWare server connected by the static route.

Usage: Press Enter to open a text field. Your usage depends on the profile.

Bridging Profile

Type the last two digits of the menu number of a Connection Profile in which Bridging=Yes. You can type a number from 1 to 31. Zero (0) is the default; this setting disables the profile.

Press Enter again to close the text field.

IPX Route Profile

Type the last two digits of the menu number of a Connection Profile. You can type a number from 1 to 31. Zero (0) is the default; this setting specifies that no Connection Profile can reach the destination.

You must enter a value in this parameter, because you should only advertise static routes that you can reach.

Press Enter again to close the text field.

Dependencies: Keep this additional information in mind for each type of profile.

Bridging Profile

You must set Dial Brdcast=No if you want the DSLPipe to use a static bridge entry. Any Connection Profile that dials on broadcast does not need a Bridging Profile.

IPX Route Profile

In an IPX Route Profile, you must carry out these tasks if you want static IPX routes to appear in the route table:

- Enable IPX routing in the Connection Profile by setting Route IPX=Yes.
- Configure IPX on the local Ethernet network by specifying a setting for one or more of these parameters: Active, Connection #, Hop Count, IPX Alias, IPX Frame, IPX Net#, Network, Node, Server Name, Server Type, Socket, and Tick Count.

Parameter Location: Bridging Profile, Bridge Adrs
IPX Route Profile, IPX Routes

See Also: Active, Connection #, Hop Count, IPX Alias, IPX Frame, IPX Net#, Network, Node, Route IPX, Server Name, Server Type, Socket, Tick Count

Console

Description: This parameter specifies the type of control interface established at the VT-100 port labeled Control on the back panel of the DSLPipe.

Usage: Standard enables you to use the standard set of menus. Standard is the default and cannot be changed on the DSLPipe.

The Control Monitor is a menu-based user interface for configuring, managing, and monitoring the DSLPipe. It consists of nine windows—eight status windows and a single edit window.

Parameter Location: System Profile, Sys Config

Contact

Description: This parameter specifies the person or department to contact if you experience problems using the DSLPipe.

Usage: Press Enter to open a text field. Then, type the name of the contact person or department. You can enter up to 60 characters. An SNMP management application can read this field, but the value you enter does not affect the operation of the DSLPipe.

Press Enter again to close the text field.

Parameter Location: System Profile, Sys Config

See Also: Location

Data Filter

Description: This parameter specifies a data filter to plug into an Answer Profile or a Connection Profile. This data filter examines each incoming or outgoing packet on a WAN, and either forwards or discards it.

Usage: Press Enter to open a text field. Then, type a number between 0 and 16. The number corresponds to a data filter you created in the Filters menu. Press Enter again to close the text field.

When you set Data Filter to 0 (zero), the DSLPipe forwards all data packets. Zero is the default.

Dependencies: Keep this additional information in mind:

- The DSLPipe applies a call filter after applying a data filter; only those packets that the data filter forwards can reach the call filter.

- If IPX client bridging is in use (Handle IPX=Client), set the Data Filter parameter to 0 (zero).
- Do not confuse the Filter parameter with the Data Filter parameter.

  The Filter parameter filters data packets on the DSLPipe unit's local LAN interface; the Data Filter parameter filters data packets on the DSLPipe unit's WAN interface. The WAN interface is the port on the DSLPipe that is connected to a WAN line.
- Data Filter in the Answer Profile applies to incoming calls for which no Connection Profile exists; if a Connection Profile exists, the setting of its Data Filter parameter takes precedence.
- If Profile Reqd=Yes in the Answer Profile, Data Filter does not apply (Data Filter=N/A) in the Answer Profile.

Parameter Location: Answer Profile, Answer/Session options
Connection Profile, Connections/Session options

See Also: Call Filter, Call Type, Filter menu, Forward, More, Profile Reqd

Data Svc

Description: This parameter specifies the type of data service the link uses for outgoing calls.

A data service is provided over a WAN line and is characterized by the unit measure of its bandwidth. A data service can transmit either data or digitized voice.

Usage: Press Enter to cycle through the choices. You can specify one of the settings listed in Table 1-1.

Table 1-1. Data Svc settings

Setting	Description
56K	The call contains any type of data and connects to the Switched-56 data service. The only services available to lines using inband signaling (such as Switched-56 lines) are 56K and 56KR.
56KR	The call connects to the Switched-56 data service. The only services available to lines using inband signaling (such as Switched-56 lines) are 56K and 56KR.
64K	The call contains any type of data and connects to the Switched-64 data service.
Voice	This value applies only to calls made over an ISDN BRI line. The voice setting enables the DSLPipe to instruct the network to place an end-to-end digital voice call for transporting data when a switched data service is not available. If you choose this setting, the data might become corrupted or unusable unless you meet these technical requirements: • Use only digital end-to-end connectivity; no analog signals should be present anywhere in the link. • Make sure that the phone company is not using any intervening loss plans to economize on voice calls. • Do not use echo cancellation; analog lines can echo, and the technology to take out the echoes can also scramble data in the link. • Do not make any modifications that can change the data in the link.

Dependencies: Keep this additional information in mind:

- The Voice setting only applies to switched channels.

- You can determine the base bandwidth of a call by multiplying the value of the Base Ch Count parameter by the value of the Data Svc parameter.
- Either party can request a data service that is unavailable; in this case, the DSLPipe cannot connect the call.

Parameter Location: Connection Profile, Connections/Telco options
Frame Relay Profile, Frame Relay

See Also: Call Type

DBA Monitor

Description: This parameter specifies how the DSLPipe monitors the traffic over a Multilink Protocol Plus (MPP) call.

Usage: Press Enter to cycle through the choices:

- Transmit
  This specifies that the Ascend unit will add or subtract bandwidth based on the amount of data it transmits.
- Transmit-Recv
  This specifies that the Ascend unit will add or subtract bandwidth based on the amount of data it transmits *or* receives.
- None
  This specifies that the Ascend unit will not monitor traffic over the link and will not use DBA.

Dependencies: DBA-Monitor is only supported on MPP calls (Encaps=MPP).

Parameter Location: Ethernet, Connections/Encaps options

See Also: Encaps, Dyn Alg, Target Util, Idle Pct

Dest

Description: This parameter appears in a Static Rtes Profile and in an SNMP Traps Profile. Its functionality differs depending on the profile:

- In a Static Rtes Profile, the Dest parameter specifies the IP address of the route's destination.
- In an SNMP Traps Profile, the Dest parameter specifies the IP address of the SNMP manager to which the DSLPipe sends traps-PDUs (Protocol Data Units).

  SNMP (Simple Network Management Protocol) provides a way for computers to share networking information. In SNMP, two types of communicating devices exist: agents and managers. An agent provides networking information to a manager application running on another computer. The agents and managers share a database of information, called the Management Information Base (MIB).

  A trap is a mechanism in SNMP for reporting system change in real time. To report system change, the DSLPipe sends a traps-PDU across the Ethernet interface to the SNMP manager. A complete list specifying the events that cause the DSLPipe to send a traps-PDU appears in the Ascend Enterprise Traps MIB.

Usage: Press Enter to open a text field. Then, type the IP address of the destination.

An IP address consists of four numbers between 0 and 255, separated by periods. If a netmask is in use, you must specify it. Separate a netmask from the IP address with a slash.

The DSLPipe ignores any digits in the IP address hidden by a netmask. For example, the address 200.207.23.1/24 becomes 200.207.23.0. To specify a route to a specific host, use a mask of 32.

The default value is 0.0.0.0/0. This value has a different meaning depending on the profile:

- In a Static Rtes Profile, the first route is the default route, and the Dest parameter is set to 0.0.0.0/0; this default specifies all destinations for which no other route exists.

- In an SNMP Traps Profile, you turn off traps by setting Dest=0.0.0.0 and deleting the value for the Comm parameter.

Press Enter to close the text field.

Example: `200.207.23.1`

Dependencies: Keep this additional information in mind:

- If you do not know the right IP address to enter, you must obtain it from the network administrator.
- Do not attempt to configure an IP address by guesswork!
- The Dest parameter does not apply (Dest=N/A) if the DSLPipe does not support IP (Route IP=No).

Parameter Location: Static Rtes Profile, Static Rtes
SNMP Traps Profile, SNMP Traps

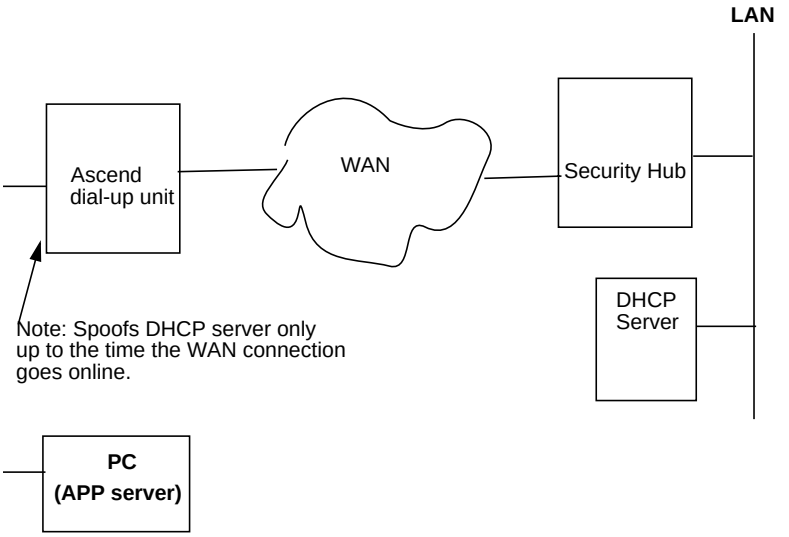
See Also: Comm, Encaps, Route IP

DHCP Spoofing

Description: This parameter enables or disables Dynamic Host Configuration Protocol (DHCP) spoofing. When DHCP spoofing is enabled, the DSLPipe can act as a DHCP server for one IP address.

When card-based security is used, the user must interact with the DSLPipe to provide the card-based password. This interaction must occur over IP. However,

the user doesn't have an IP address yet at the time when the password must be supplied.



To solve this "which came first" problem, the DSLPipe supports DHCP spoofing. DHCP spoofing works like this:

1 If there is no authenticated dial-up session and the DSLPipe receives a DHCP Discover packet, it responds with a DHCP Offer packet containing the configured IP address, netmask, and renewal time. This is quickly verified by an exchange between the client and the DSLPipe. The renewal time is limited to a few seconds to ensure that the computer gets its *real* address from the remote DHCP server as soon as possible.

2 The APP Server utility runs using only broadcast addresses (see the discussion on the APP Server Utility and DHCP Spoofing in the *DSLPipe User's Guide*), so that the DSLPipe does not need a real IP address and the temporary "spoofed" address is not relied upon.

3 As soon as an authenticated dial-up link exists, the DSLPipe refused to renew the spoofed address, forcing the computer to get its real address from the remote DHCP server.

Usage: Press Enter to toggle between Yes and No.

- Yes enables DHCP spoofing.
- No (default) disables this feature.

Parameter Location: Ethernet, Mod Config/DHCP Spoofing...

Dependencies: The Spoof Adr and Renewal Time parameters must be configured for this feature to work.

See Also: Spoof Adr, Renewal Time

Dial #

Description: This parameter appears in the Configure Profile, a Connection Profile, and a Frame Relay Profile. Its functionality differs depending on the profile:

- In the Configure or Connection Profile, the Dial # parameter specifies the phone number the DSLPipe dials to reach the bridge, router, or node at the remote end of the link.
- In a Frame Relay Profile, the Dial # parameter specifies the phone number that the DSLPipe dials to reach a frame relay switch.

  Frame Relay is an HDLC-based packet protocol that enables you to send data to a destination using one or more frame relay switches within a private network or a public carrier's network. HDLC stands for High Level Data Link Control.

  From the viewpoint of the DSLPipe, a frame relay switch is an endpoint for all DLCIs (Data Link Connection Indicators) connecting to it. A DLCI identifies a Connection Profile as a logical link. The frame relay switch connects the endpoints of the DLCIs to each other to make a virtual permanent circuit to which users can connect. The circuit acts like a wire between two endpoints with a fixed maximum bandwidth.

Usage: Press Enter to open a text field. Then, type a telephone number. You can enter up to 37 characters, and you must limit those characters to the following:

```
1234567890()[]!z-*#|
```

The DSLPipe sends only the numerical characters to place a call.

The default value is null.

Press Enter to close the text field.

Dependencies: Keep this additional information in mind:

- Dial # does not apply (Dial #=N/A) when all channels are nailed up (Call Type=Nailed) or if you are using frame relay encapsulation (Encaps=FR).
- If Sub-Adr=Termsel (in the System, Sys Config menu) include the ISDN subaddress in the Dial #, separating it from the phone number with a comma. The characters before the comma comprise the phone number; the one or two numeric characters after the comma comprise the subaddress. Consider this example:

  `555-1212,23`

  The DSLPipe dials the phone number 555-1212, and conveys the subaddress 23 to the answering party.

Parameter Location: Configure Profile
Connection Profile, Connections
Frame Relay Profile, Frame Relay

See Also: Call Type, Encaps, Group, Sub-Adr

Dial Brdcast

Description: This parameter specifies whether broadcast packets initiate dialing.

Usage: Press Enter to toggle between Yes and No.

- Yes specifies that the DSLPipe dials a link if (a) the link is not online and (b) the DSLPipe receives a frame whose MAC address is set to broadcast.

  When a device on the local Ethernet interface sends out broadcast packets that the DSLPipe must bridge to another network, the DSLPipe starts up a session for each Connection Profile in which Dial Brdcast=Yes. Gradually, it builds an internal bridge table based on experience; this table helps to limit the number of calls by recording the appropriate destination network for various addresses.
- No specifies that broadcast packets do not initiate dialing.

  If you choose this setting, the DSLPipe relies on its Bridging Profiles, which contain remote physical addresses you have manually entered.

No is the default.

Dependencies: The Dial Brdcast parameter applies only if the Connection Profile enables bridging (Bridge=Yes) and allows outgoing calls (AnsOrig=Call Only or AnsOrig=Both).

Parameter Location: Connection Profile, Connections

See Also: Connection #

Dial Query

Description: This parameter specifies whether the DSLPipe places a call to the location indicated in the Connection Profile when a workstation on the local IPX network looks for the nearest IPX server. More than one Connection Profile can have this parameter set to Yes. As a a result, several connections can occur at the same time.

Usage: Press Enter to toggle between Yes and No.

- Yes specifies that the DSLPipe places a call to the location specified in the Connection Profile when a workstation looks for the nearest server.

  Note that a workstation is likely to stop attempting to find a server before the DSLPipe establishes any connections with the Dial Query mechanism.
- No specifies that the DSLPipe does not place a call to the location specified in the Connection Profile when a workstation looks for the nearest server.

  No is the default.

Dependencies: If there is an entry in the DSLPipe unit's routing table for the location specified by the Connection Profile, Dial Query has no effect.

Parameter Location: Connection Profile: Ethernet→Connections→Any Connection Profile→IPX Options

DLCI

Description: This parameter specifies the Data Link Connection Indicator that identifies the Connection Profile to the frame relay switch as a logical link on a physical circuit.

Frame Relay is an HDLC-based packet protocol that enables you to send data to a destination using one or more frame relay switches within a private network or a public carrier's network. HDLC stands for High Level Data Link Control.

From the viewpoint of the DSLPipe, a frame relay switch is an endpoint for all DLCIs (Data Link Connection Indicators) connecting to it. A DLCI identifies a Connection Profile as a logical link. The frame relay switch connects the endpoints of the DLCIs to each other to make a virtual permanent circuit to which users can connect. The circuit acts like a wire between two endpoints with a fixed maximum bandwidth.

Usage: Press Enter to open a text field. Then, enter a number between 16 and 991. The default is 16. Ask you frame relay network administrator for the value you should enter. Press Enter to close the text field.

Dependencies: Keep this additional information in mind:

- DLCI only appears in a Connection Profile when Encaps=FR
- Each Connection Profile that contains the setting Encaps=FR represents a separate logical link; you must assign it a unique setting for DLCI.

Parameter Location: Connection Profile, Connections/Encaps

See Also: Encaps, FR Prof

Domain Name

Description: This parameter specifies the name of domain the DSLPipe is located in. This name is used by the Domain Name System (DNS) to associate IP addresses with symbolic names.

DNS is a TCP/IP service that enables you to specify a symbolic name instead of an IP address. A symbolic name consists of a username and a domain name in the format *username@domain name*. The *username* corresponds to the host number

in the IP address. The *domain name* corresponds to the network number in the IP address. A symbolic name might be steve@abc.com or joanne@xyz.edu.

DNS maintains a database of network numbers and corresponding domain names on a domain name server. When you use a symbolic name, DNS translates the domain name into an IP address, and sends it over the network. When the Internet service provider receives the message, it uses its own database to look up the username corresponding to the host number.

Usage: Press Enter to open a text field. Then, type the domain name of the DSLPipe. Press Enter again to close the text field.

Parameter Location: Ethernet Profile, Mod Config > DNS

See Also: Pri DNS, Sec DNS

Dst Adrs

Description: In a filter of type IP, this parameter specifies the destination address to which the DSLPipe compares a packet's destination address.

Usage: Press Enter to open a text field. Then, type the destination address the DSLPipe should use for comparison when filtering a packet. The address consists of four numbers between 0 and 255, separated by periods.

The null address 0.0.0.0 is the default. If you accept the default, the DSLPipe does not use the destination address as a filtering criterion.

Press Enter to close the text field.

Example: `200.62.201.56`

Dependencies: Dst Adrs does not apply (Dst Adrs=N/A) if you are using a generic filter (Type=Generic) or if you have not activated the IP filter (Valid=No).

Parameter Location: Filter Profile, Filters/IP

See Also: Dst Mask

Dst Mask

Description: In a filter of type IP, this parameter specifies the bits that the DSLPipe should mask when comparing a packet's destination address to the value of the Dst Adrs parameter. The masked part of an address is hidden; the DSLPipe does not use it for comparison with Dst Adrs. A mask hides the part of a number that appears behind each binary 0 (zero) in the mask; the DSLPipe uses only the part of a number that appears behind each binary 1 for comparison.

The DSLPipe applies the mask to the address using a logical AND after the mask and address are both translated into binary format.

Usage: Press Enter to open a text field. Then, type the IP mask in dotted decimal format. The value 0 (zero) hides all bits, because the decimal value 0 is the binary value 00000000; the value 255 does not mask any bits, because the decimal value 255 is the binary value 11111111.

The null address 0.0.0.0 is the default; this setting indicates that the DSLPipe masks all bits. To specify a single destination address, set Dst Mask=255.255.255.255 and set Dst Adrs to the IP address that the DSLPipe uses for comparison.

Press Enter to close the text field.

Example: Suppose a packet has the destination address 10.2.1.1. If Dst Adrs=10.2.1.3 and Dst Mask=255.255.255.0, the DSLPipe masks the last digit and uses only 10.2.1, which matches the packet.

Dependencies: Dst Mask does not apply (Dst Mask=N/A) if you are using a generic filter (Type=Generic) or if you have not activated the IP filter (Valid=No).

Parameter Location: Filter Profile, Filters/IP

See Also: Dst Adrs

Dst Port

Description: In a filter of type IP, this parameter specifies the destination port number to which the DSLPipe compares the packet's destination port number.

The destination port number specifies the port on the remote device that must be "listening" for packets.

The Dst Port Cmp criterion determines how the DSLPipe carries out the comparison.

Usage: Press Enter to open a text field. Then, type the number of the destination port the DSLPipe should use for comparison when filtering packets. You can enter a number between 0 and 65535.

The default setting is 0 (zero). If you accept the default, the DSLPipe does not use the destination port number as a filtering criterion.

Press Enter to close the text field.

Example: 25

Port 25 is reserved for SMTP; that socket is dedicated to receiving mail messages. Port 20 is reserved for FTP data messages, Port 21 for FTP control sessions, and Port 23 for Telnet sessions.

Parameter Location: Filter Profile, Filters/IP

See Also: Dst Port Cmp, Src Port Cmp, Src Port #

Dst Port Cmp

Description: In a filter of type IP, this parameter specifies the type of comparison the DSLPipe makes when using the Dst Port # parameter.

Usage: Press Enter to cycle through the choices.

- None specifies that the DSLPipe does not compare the packet's destination port to the value specified by Dst Port #.
  None is the default.
- Less specifies that port numbers with a value less than the value specified by Dst Port # match the filter.
- Eql specifies that port numbers equal to the value specified by Dst Port # match the filter.

- Gtr specifies that port numbers with a value greater than the value specified by Dst Port # match the filter.
- Neq specifies that port numbers not equal to the value specified by Dst Port # match the filter.

Dependencies: Keep this additional information in mind:

- This parameter works only for TCP and UDP packets.
  You must set Dst Port Cmp=None if the Protocol parameter is not set to 6 (TCP) or 17 (UDP).
- Dst Port Cmp does not apply (Dst Port Cmp=N/A) if you are using a generic filter (Type=Generic) or if you have not activated the IP filter (Valid=No).

Parameter Location: Filter Profile, Filters/IP

See Also: Dst Port #

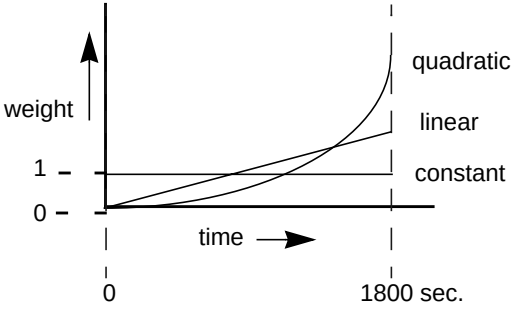
Dyn Alg

Description: This parameter specifies which Dynamic Bandwidth Allocation (DBA) algorithm to use for calculating average line utilization (ALU) of transmitted data. DBA enables you to specify that the DSLPipe uses ALU as the basis for automatically adding or subtracting bandwidth from a switched connection without terminating the link.

The DSLPipe uses the historical time period specified by the Sec History parameter as the basis for calculating ALU. It then compares ALU to the amount specified in the Target Util parameter. When ALU exceeds the threshold defined by Target Util for a period of time greater than the value of the Add Pers parameter, the DSLPipe attempts to add the number of channels specified by the Inc Ch Count parameter. When ALU falls below the threshold defined by Target Util for a period of time greater than the value of the Sub Pers parameter, the DSLPipe attempts to remove the number of channels specified by the Dec Ch Count parameter.

MP+ supports Dynamic Bandwidth Allocation.

Usage: Press Enter to cycle through the choices. This graph illustrates the algorithms you can choose:



- Linear gives more weight to recent samples of bandwidth usage than to older samples taken during the historical period specified by the Sec History parameter; the weighting grows at a linear rate.
- Quadratic gives more weight to recent samples of bandwidth usage than to older samples taken during the historical period specified by the Sec History parameter; the weighting grows at a quadratic rate.

  Quadratic is the default for MP+ calls (Encaps=MPP).
- Constant gives equal weight to all samples taken during the historical time period specified by the Sec History parameter.

  When you select this option, older historical samples have as much impact on the decision to change bandwidth allocation as do more recent samples.

Dependencies: Keep this additional information in mind:

- To dynamically allocate bandwidth by tracking line usage, you must specify the Add Pers, Dec Ch Count, Dyn Alg, Inc Ch Count, Max Ch Count, Sec History, Sub Pers, and Target Util parameters.
- Dyn Alg in the Answer Profile applies to incoming calls for which no Connection Profile exists; if a Connection Profile exists, the setting of its Dyn Alg parameter takes precedence.
- If Profile Reqd=Yes in the Answer Profile, Dyn Alg does not apply (Dyn Alg=N/A) in the Answer Profile.

Parameter Location: Answer Profile: Ethernet→Answer→PPP Options
Connection Profile: Ethernet→Connections→Any Connection Profile→Encaps Options

See Also: Add Pers, Dec Ch Count, Dyn Alg, Inc Ch Count, Max Ch Count, Sec History, Sub Pers, Target Util

---

Edit Security

Description: This parameter grants or restricts privileges to edit Security Profiles.

Usage: Press Enter to toggle between Yes and No.

- Yes grants privileges.

  Yes is the default. When you choose Yes, a user is permitted to edit Security Profiles, and can access all other operations by enabling them in his or her active Security Profile.
- No restricts privileges.

Dependencies: Keep this additional information in mind:

- The Edit Security parameter does not apply (Edit Security=N/A) if Operations=No.
- Do not set the Edit Security parameter to No on all nine Security Profiles; if you do, you will be unable to edit any of them.

Parameter Location: Security Profile, Security

Edit System

Description: This parameter grants or restricts privileges to edit the System Profile and the Ethernet Profile.

Usage: Press Enter to toggle between Yes and No.

- Yes grants privileges to edit the System Profile, and to edit the Read Comm and R/W Comm parameters in the Ethernet Profile.

  Yes is the default.
- No restricts privileges.

Dependencies: The Edit System parameter does not apply (Edit System=N/A) if Operations=No.

Parameter Location: Security Profile, Security

Encaps

Description: This parameter enables you to choose the encapsulation method to use when exchanging data with a remote network.

Usage: Press Enter to cycle through the choices. You can choose one of the settings listed below.

PPP

PPP (Point-to-Point Protocol) provides a standard means of encapsulating data packets over a single-channel WAN link that a Connection Profile sets up. It ensures basic compatibility with non-Ascend devices.

For this setting to work, both the dialing side and the answering side of the link must support PPP.

MPP

MP+ (Multilink Protocol Plus) extends the capabilities of MP (Multilink PPP) to support inverse multiplexing, session management, and bandwidth management. MP is an extension of PPP that supports the ordering of data packets across multiple channels.

MP+ consists of two components: a low-level channel identification, error monitoring, and error recovery mechanism, and a session management level for supporting bandwidth modifications and diagnostics. MP+ enables the DSLPipe to perform Dynamic Bandwidth Allocation (DBA)—that is, MP+ enables the DSLPipe to add or remove channels without disconnecting a link as the need for bandwidth increases or decreases.

Both the dialing side and the answering side of the link must support MP+. If only one side supports MP+, the connection then tries to use MP. If that fails, the connection uses standard single-channel PPP. Note that neither MP nor PPP support DBA.

FR

FR stands for Frame Relay.

Frame Relay is an HDLC-based packet protocol that enables you to send data to a destination using one or more frame relay switches within a private network or a public carrier's network. HDLC stands for High Level Data Link Control.

From the viewpoint of the DSLPipe, a frame relay switch is an endpoint for all From the viewpoint of the DSLPipe, a frame relay switch is an endpoint for all DLCIs (Data Link Connection Indicators) connecting to it. A DLCI identifies a Connection Profile as a logical link. The frame relay switch connects the endpoints of the DLCIs to each other to make a virtual permanent circuit to which users can connect. The circuit acts like a wire between two endpoints with a fixed maximum bandwidth.

If you set Encaps=FR and FR Direct=No, the Connection Profile provides a bridge or route across the WAN over frame relay circuits. You must configure the FR Prof parameter in the Encaps submenu to send this connection to the frame relay switch. The FR Prof name must exist in a Frame Relay Profile before you can save the Connection Profile.

Dependencies: Keep this additional information in mind:

- When you select an encapsulation method, the Encaps options submenu displays a group of parameters relevant to your selection; you must set the appropriate Encaps options parameters.
- The Encaps parameter does not apply (Encaps=N/A) when the DSLPipe answers a call, or if the link consists of only nailed-up channels (Call Type=Nailed).
- If Call Type=Nailed/MPP then Encaps must be set to MPP. In this case, or whenever Encaps=MPP, the DSLPipe adds or subtracts switched channels on the connection as required by the DBA parameters on either side of the connection.

  DBA, or Dynamic Bandwidth Allocation, enables the DSLPipe to use average line utilization (ALU) of transmitted data as the basis for adding or subtracting bandwidth from a switched connection without terminating the link. MP+ and AIM support Dynamic Bandwidth Allocation. Each side makes its calculations based on the traffic received at that side. If the two sides of the connection disagree on the number of channels needed, the side requesting the greater number prevails.

- If Encaps=MPP and Call Type=Nailed/MPP, the minimum number of channels in the link is the number set by Min Ch Count or the number of nailed-up channels in the group, whichever is greater.
- If Encaps=MPP and Call Type=Nailed/MPP, the maximum number of channels in the link is the number set by Max Ch Count or the number of nailed-up channels in the group, whichever is greater.

  The DSLPipe does not count a nailed-up channel that is not online.

Parameter Location: Connection Profile, Connections

See Also: Encaps options submenu

Enet Adrs

Description: In a Bridging Profile, this parameter specifies the physical Ethernet address (MAC address) of a device at the remote end of the link.

The DSLPipe uses the Bridging Profile to build a bridge table with corresponding MAC and IP addresses. The Enet Adrs parameter specifies the MAC address of each remote device; the Net Adrs parameter specifies the IP address of each remote device.

These parameters enable the DSLPipe to respond to local ARP (Address Resolution Protocol) requests on behalf of a device at the remote end of the link. Whenever the DSLPipe receives an ARP request for a MAC address corresponding to a specified IP address, it checks to see whether the IP address matches one in its bridge table. If it does, the DSLPipe returns the MAC address corresponding to the IP address.

Usage: Press Enter to open a text field. Then, type the physical address of the device on the remote network. An Ethernet address is a 12-digit hexadecimal number.

The default setting is 000000000000.

Press Enter to close the text field.

`Example:` `0180C2000000`

Parameter Location: Bridging Profile, Bridge Adrs

See Also: Net Adrs

Field Service

Description: This parameter grants or restricts privileges to perform Ascend-provided field service operations, such as uploading new system software.

Usage: Press Enter to toggle between Yes and No.

- Yes grants privileges.
  Yes is the default.
- No restricts privileges.
  Selecting No does not disable access to any DSLPipe operations. Field service operations are special diagnostic routines not available through DSLPipe menus.

Dependencies: The Field Service parameter does not apply (Field Service=N/A) if Operations=No.

Parameter Location: Security Profile, Security

Filter

Description: This parameter specifies the number of a data filter that plugs into the Ethernet Profile. The data filter manages data flow on the Ethernet interface. The filter examines each incoming or outgoing packet, and uses the Forward parameter to determine whether to forward or discard it.

Usage: Press Enter to open a text field. Then, type a number between 0 and 16. The number corresponds to a data filter you created in the Filters menu. When you set Filter to 0 (zero), the DSLPipe forwards all packets.

Zero is the default.

Press Enter again to close the text field.

Dependencies: Do not confuse the Filter parameter with the Data Filter parameter or the Call Filter parameter.

- The Filter parameter filters data packets on the DSLPipe's local LAN interface.
- The Data Filter parameter filters data packets on the DSLPipe's WAN interface.

  The WAN interface is the port on the DSLPipe that is connected to a WAN line.
- The Call Filter parameter determines which packets can initiate a call or reset the idle timer.

  By default, any packet destined for the WAN causes the DSLPipe to place a call. In addition, by default, every packet resets the idle timer, the indicator that the DSLPipe uses to know when to clear a call. The Call Filter parameter limits the packets that can cause these events.

  The DSLPipe applies the call filter specified by Call Filter only after applying the data filter specified by Filter or Data Filter. Only those packets that a data filter forwards reach a call filter.

Parameter Location: Ethernet Profile, Mod Config/Ether options

See Also: Forward, More

Force56

Description: This parameter specifies whether the DSLPipe uses only the 56-kbps portion of a channel, even when all 64 kbps appear to be available.

Use this feature when you place calls to European or Pacific Rim countries and the complete path cannot distinguish between the Switched-56 and Switched-64 data services. This feature is not required if you are placing calls only within North America.

Usage: Press Enter to toggle between Yes and No.

- Yes specifies that the DSLPipe uses only 56 kbps.
- No specifies that the DSLPipe can use 64 kbps, if available.

  No is the default.

Parameter Location: Connection Profile, Connections/Telco options

Forward

Description: In a data filter or a call filter, this parameter specifies whether the DSLPipe forwards or discards packets that match the filter. When you use Forward in a call filter, any forwarded data packet resets the idle timer and can initiate a call.

Usage: Press Enter to toggle between Yes and No.

- Yes specifies that the DSLPipe forwards all packets matching the filter. If you have not specified any filters, Yes is the default.
- No specifies that the DSLPipe does not forward packets matching the filter. If you have specified one or more filters, No is the default.

Example: If Forward=No in several filters, you must specify Forward=Yes in the last filter to allow data to pass. Consider this example:

```
In filter 01...Valid=Yes
In filter 01...Type=Generic
In filter 01...Generic...Forward=No
...
In filter 02...Valid=Yes
In filter 02...Type=Generic
In filter 02...Generic...Forward=No
...
In filter 03...Valid=Yes
In filter 03...Type=Generic
In filter 03...Generic...Forward=Yes
```

Parameter Location: Filter Profile, Filter/Generic and Filter/IP

See Also: Call Filter, Data Filter, Filter, More

FR Prof

Description: This parameter specifies the name of the Frame Relay Profile whose parameters the DSLPipe should use in building the connection.

Usage: Press Enter to open a text field. Then, type the profile name. You can enter up to 15 alphanumeric characters. The default is null. Make sure that you enter the name exactly as it appears in the Name parameter of the Frame Relay Profile. Press Enter again to close the text field.

Parameter Location: Connection Profile, Connections/Encaps

See Also: Name

FT1 Caller

Description: This parameter specifies whether the DSLPipe initiates a dial-up to add channels to an existing nailed-up or serial WAN connection. Whenever you have a mixture of nailed-up and switched channels in a connection, you need the FT1 Caller parameter. On purely switched calls, when the DSLPipe needs to send packets across the WAN to a destination which is not online, it dials to bring up the connection to that destination. If additional channels are needed, the original caller dials, never the original answering side.

However, if the connection is already online over nailed-up channels, which end should dial to add switched channels? The only way to determine who calls (and therefore who is billed for the call) is by using this parameter.

Usage: Press Enter to toggle between Yes and No.

- Yes specifies that the DSLPipe initiates the call.
  If you choose this setting, the DSLPipe dials to bring online any switched circuits that are part of the call.
- No specifies that the DSLPipe waits for the remote end to initiate the call.
  No is the default.

Dependencies: Keep this additional information in mind:

- If the remote end has FT1 Caller=No, set FT1 Caller=Yes on the local DSLPipe; by the same token, if the remote end has FT1 Caller=Yes, set FT1 Caller=No on the local DSLPipe.
- The FT1 Caller parameter applies only when Call Type=Nailed/MPP.

Parameter Location: Connection Profile, Connections/Telco options

See Also: Call Type

Gateway

Description: This parameter specifies the IP address of the router that a packet must go through to reach the destination station of the route.

Usage: Press Enter to open a text field. Then, type the IP address of the router.

An IP address consists of four numbers between 0 and 255, separated by periods. The default value is 0.0.0.0.

You must configure the network address of the destination station with the LAN Adrs parameter in the Connection Profile; otherwise, the DSLPipe assumes that the router is on the same Ethernet interface.

Press Enter to close the text field.

Example: `200.207.23.1`

Dependencies: Keep this additional information in mind:

- If you do not know the right IP address to enter, you must obtain it from the network administrator.

  Do not attempt to configure an IP address by guesswork!
- The Gateway parameter does not apply (Gateway=N/A) if the DSLPipe does not support IP (Route IP=No).

Parameter Location: Static Rtes

See Also: Encaps, LAN Adrs, Route IP

Group

Description: This parameter points to the nailed-up channels used by the WAN link.

Usage: Press Enter to open a text field. Enter a number between 1 and 3.

Example: If Call Type=Nailed/MPP in a Connection Profile, the setting Group=3 assigns one nailed-up group to the profile.

Dependencies: Keep this additional information in mind:

- The Group parameter does not apply (Group=N/A) if the link consists entirely of switched channels (Call Type=Switched).
- If you add channels to the Group parameter and save your changes, the DSLPipe adds the additional channels to any online connection that uses the group.
- Do not assign more than one active Connection Profile to a group.
- Do not assign a Connection Profile to a group that a Frame Relay Profile uses.
- If you are using an ISDN BRI line the DSLPipe assigns the B channels to the following groups:

  1 represents the B1 channel

  2 represents the B2 channel

Parameter Location: Connection Profile, Connections/Telco options

See Also: Call Type, Nailed Group

Handle IPX

Description: This parameter enables you to configure a connection that bridges IPX.

Usage: Press Enter to cycle through the choices.

- None specifies that special IPX behavior does not take place.

  Choose this setting when the LAN on each side of the bridge has one or more IPX servers.

None is the default.

- Client specifies that the DSLPipe discards RIP (Routing Information Protocol) and SAP (Service Advertising Protocol) periodic broadcasts at its WAN interface, but forwards RIP and SAP queries.

  The WAN interface is the port on the DSLPipe that is connected to a WAN line. RIP and SAP queries enable a client workstation to locate a NetWare server across the network. Choose this setting when both these conditions are true:

  - The local LAN has IPX clients but no servers.
  - The DSLPipe is acting as a bridge to another LAN containing only IPX servers or a combination of IPX servers and clients.

- Server specifies that the DSLPipe discards all RIP (Routing Information Protocol) and SAP (Service Advertising Protocol) periodic broadcasts and queries at its WAN interface.

  Server mode allows the DSLPipe to bring down calls during idle periods without breaking client-server or peer-to-peer connections.

  Ordinarily, when a NetWare server does not receive a reply to the watchdog session *keepalive* packets it sends to a client, it closes the connection. When you select Server mode, however, the DSLPipe replies to NCP watchdog requests on behalf of clients on the other side of the bridge; in other words, the DSLPipe tricks the server watchdog process into believing that the link is still active. This process is called watchdog spoofing.

  Choose this setting when both these conditions are true:

  - The DSLPipe is acting as a bridge to a remote LAN with IPX clients, but no servers.
  - The local LAN contains only IPX servers, or a combination of IPX clients and servers.

Dependencies: Keep this additional information in mind:

- If you select the Server setting, you must also specify a value for the NetWare t/o parameter, indicating the maximum length of idle time during which the DSLPipe performs watchdog spoofing for NetWare connections.
- If the connection does not bridge (Bridge=No), the Handle IPX parameter does not apply (Handle IPX= N/A).
- If the encapsulation for the connection is Frame Relay (Encaps=FR), the Handle IPX parameter does not apply (Handle IPX= N/A).

- If you have not specified an IPX frame type (IPX Frame=None), the Handle IPX parameter does not apply (Handle IPX=N/A).
- We highly recommend that you set Dial Brdcast=Yes when Handle IPX=Client, and Dial Brdcast=No when Handle IPX=Server.

  When a client on the local Ethernet interface sends out broadcast packets to locate a server, and the DSLPipe must bridge these packets to another network, the DSLPipe starts up a session for each Connection Profile in which Dial Brdcast=Yes. The server need not broadcast and then dial, so set Dial Brdcast=No to keep broadcast packets from causing the DSLPipe to dial automatically.
- If the DSLPipe on one LAN sets Handle IPX=Server and the LAN on the other side of the connection has only NetWare clients, the DSLPipe on the client-only LAN should set Handle IPX=Client.

  If both LANs contain servers, both sides of the connection should set Handle IPX=None.
- Although Handle IPX=N/A if Bridge=No or IPX Frame=None, the DSLPipe automatically performs watchdog spoofing just as though you had set Handle IPX=Server; however, the DSLPipe does not filter as though you had set Handle IPX=Server.

Parameter Location: Connection Profile, Connections/IPX options

See Also: Dial Brdcast, NetWare t/o

Hop Count

Description: This parameter specifies the distance to the destination IPX network in hops. From the DSLPipe, the local IPX network is one hop away. The IPX network at the remote end of the route is two hops away—one hop across the WAN and one hop to the local IPX network.

Usage: Press Enter to open a text field. Then, type a valid hop count from 1 to 15. A hop count of 16 is considered unreachable and is not valid for static routes. Press Enter again to close the text field.

Dependencies: For the Hop Count parameter to apply, you must enable IPX routing in the Connection Profile by setting Route IPX=Yes.

Parameter Location: IPX Route Profile, IPX Routes

See Also: Route IPX

ICMP Redirects

Description: This parameter specifies whether the DSLPipe accepts or ignores Internet ICMP Redirect messages.

Usage: Press Enter to cycle through the choices.

- Accept specifies that the DSLPipe processes incoming ICMP Redirect messages.

  Accept is the default.
- Ignore specifies that the DSLPipe drops all incoming ICMP Redirect messages.

Dependencies: Set ICMP Redirects=Ignore whenever the DSLPipe maintains a routing table, because counterfeit ICMP Redirects pose a potential security threat. You should accept ICMP Redirects only when the DSLPipe has a single default route to another device.

Parameter Location: Ethernet Profile, Mod Config

Idle

Description: This parameter specifies the number of seconds the DSLPipe waits before clearing a call when a session is inactive.

Usage: Press Enter to open a text field; then, type a number between 0 and 65535. If you specify 0 (zero), DSLPipe does not enforce a limit; an idle connection stays open indefinitely.

The default setting is 120 seconds.

Press Enter again to close the text field.

Dependencies: Keep this additional information in mind:

- In an Answer Profile or Connection Profile, Idle does not apply to nailed-up links; that is, Idle=N/A when Call Type=Nailed.
- If MP+ encapsulation is in use and the bandwidth utilization *on both sides of the connection* drops below the value entered in the Idle Pct field, the DSLPipe clears the call, regardless of the value you enter for the Idle parameter.
- Idle in the Answer Profile applies to incoming calls for which no Connection Profile exists; if a Connection Profile exists, the setting of its Idle parameter takes precedence.
- If Profile Reqd=Yes in the Answer Profile, Idle does not apply (Idle=N/A) in the Answer Profile.
- Because the Idle Pct is parameter is dependent on traffic levels on both sides of the connection, we recommend that you use the Idle parameter in preference to it.

Parameter Location: Answer Profile, Answer/Session options
Connection Profile, Connections/Session options

See Also: Call Type, Dial, Dual Ports, Profile Reqd

Idle Logout

Description: This parameter specifies the number of minutes the Control Monitor or Telnet session can remain inactive before the DSLPipe logs out and hangs up.

The Control Monitor is a menu-based user interface for configuring, managing, and monitoring the DSLPipe. It consists of nine windows—eight status windows and a single edit window.

Telnet is a protocol used to link two computers in order to provide a terminal with a connection to the remote machine. The remote machine is known as the Telnet host. When you start a Telnet session, you connect to the Telnet host and log in. The connection enables you to work with the remote machine as though you were at a terminal connected to it.

Usage: Press Enter to open a text field. Then, type a number between 0 and 60. The default setting is 0; this setting disables automatic logout. Press Enter again to close the text field.

Parameter Location: System Profile, Sys Config

Idle Pct

Description: This parameter specifies a percentage of bandwidth utilization below which the DSLPipe clears a single-channel MP+ call. Bandwidth utilization must fall below this percentage on *both sides* of the connection before the DSLPipe clears the call.

Usage: Press Enter to open a text field. Then, type a number between 0 and 99. The default value is 0; this setting causes the DSLPipe to ignore bandwidth utilization when determining whether to clear a call. Press Enter again to close the text field.

Dependencies: Keep this additional information in mind:

- MP+ must be the selected encapsulation method (Encaps=MPP) in a Connection Profile.
- If the device at the remote end of the link enters an Idle Pct setting lower than the value you specify, the DSLPipe does not clear the call until bandwidth utilization falls below the lower percentage.
- If either end of a connection sets the Idle Pct parameter to 0 (zero), the DSLPipe ignores bandwidth utilization when determining when to clear a call.
- If the time set by the Idle parameter expires, the call disconnects whether or not bandwidth utilization falls below the Idle Pct setting.
- When bandwidth utilization falls below the Idle Pct setting, the call disconnects regardless of whether the time specified by the Idle parameter has expired.
- Because the Idle Pct parameter is dependent on traffic levels on both sides of the connection, we recommend that you use the Idle parameter in preference to it.

- Idle Pct in the Answer Profile applies to incoming calls for which no Connection Profile exists; if a Connection Profile exists, the setting of its Idle Pct parameter takes precedence.
- If Profile Reqd=Yes in the Answer Profile, Idle Pct does not apply (Idle=N/A) in the Answer Profile.

Parameter Location: Answer Profile, Answer/PPP options
Connection Profile, Connections/Encaps options

See Also: Call Filter, Encaps, Idle

Ignore Def Rt

Description: This parameter specifies whether the DSLPipe ignores RIP (Routing Information Protocol) updates to the default route (0.0.0.0/0) in its IP routing table.

Usage: Press Enter to toggle between Yes and No.

- Yes specifies that the DSLPipe ignores updates to the default route.
- No specifies the DSLPipe allows updates to the default route.
  No is the default.

Parameter Location: Ethernet Profile, Mod Config/Ether options

---

IP Adrs

Description: This parameter specifies the IP address of the DSLPipe on the local Ethernet network, and its subnet.

Usage: Press Enter to open a text field. Then, type the IP address of the DSLPipe on the local Ethernet network.

The address consists of four numbers between 0 and 255, separated by periods. Separate the optional netmask from the address with a slash. The IP address must be a valid IP address on the local Ethernet network.

The default value is 0.0.0.0/0.

Press Enter to close the text field.

Example: `10.2.1.1/24`

In this example, 10.2.1.1 is the DSLPipe's IP address. The number 24 represents the number of bits in the DSLPipe's netmask. Masking 24 bits in the DSLPipe's address provides a subnet of 10.2.1.0.

Dependencies: Keep this additional information in mind:

- The value of the IP Adrs parameter on the local DSLPipe must match the LAN Adrs parameter of the unit at the remote end of the link.
- The IP Adrs parameter does not apply (IP Adrs=N/A) if the DSLPipe does not support IP (Route IP=No).
- If you do not know the right IP address to enter, you must obtain it from the network administrator.

  Do not attempt to configure an IP address by guesswork!
- The IP Adrs parameter is the same as the My Addr parameter in the Configure Profile.

Parameter Location: Ethernet Profile, Mod Config/Ether options

See Also: Encaps, Route IP

IPX Alias

Description: This parameter specifies the network number assigned to a point-to-point link.

Generally, you need to enter a value in this parameter only if the DSLPipe operates with a non-Ascend router that uses a numbered interface. It does not apply if you are routing from one DSLPipe to another, or to a router that does not use a numbered interface.

Usage: Press Enter to open a text field. Then, enter an appropriate network number. The default value is 00000000. FFFFFFFF is invalid. Press Enter again to close the text field.

Dependencies: For the IPX Alias parameter to apply, you must enable IPX routing in the Connection Profile by setting Route IPX=Yes.

Parameter Location: Connection Profile, Connections

See Also: Route IPX

IPX Enet#

Description: This parameter specifies a unique IPX network number for the Ethernet interface.

The DSLPipe assigns an address to a workstation when it connects to the DSLPipe; it derives the address from the network number.

Usage: Press Enter to open a text field. Then, type an IPX network number using an 8-digit (4-byte) hexadecimal value. The default is 00000000. The number you specify must be unique within your wide-area IPX network, and must match the configuration of other routers on the local Ethernet network.

When you accept the default setting of 00000000, the DSLPipe learns its IPX network number from other routers on the Ethernet network. If you enter a value other than zero, the DSLPipe becomes the "seeding" router and sets its IPX network number for the other routers on the Ethernet network

Example: `DE040600`

Dependencies: The IPX Enet# parameter does not apply (IPX Enet#=N/A) if the DSLPipe is not set up for IPX routing (Route IPX=No).

Parameter Location: Ethernet Profile, Mod Config/Ether options

---

IPX Frame

Description: This parameter specifies the Ethernet frame type to use for IPX on the Ethernet interface. If you do not specify an Ethernet frame type, the DSLPipe cannot route IPX or perform watchdog spoofing for its IPX clients.

IPX packets can appear in more than one Ethernet frame type on an Ethernet segment. If your DSLPipe routes IPX, it can recognize only a single IPX frame type. The DSLPipe does not route other IPX frame types, and may attempt to bridge them. In addition, the DSLPipe can only route and perform watchdog spoofing for the IPX frame type specified by IPX Frame.

Usage: Press Enter to cycle through the choices.

- 802.3 specifies the 802.3 frame type.

  This setting indicates that IPX clients and servers on the local Ethernet cable follow the IEEE 802.3 protocol for the MAC header, also called Raw 802.3. The frame does not contain the LLC (Logical Link Control) header in addition to the MAC (Media Access Control) header.

  For NetWare 3.11 or earlier, select 802.3.

- 802.2 specifies the 802.2 frame type.

  This setting indicates that the IPX clients and servers on the local Ethernet cable follow the IEEE 802.2 protocol for the MAC header. The framer contains the LLC (Logical Link Control) header in addition to the MAC (Media Access Control) header.

  For NetWare 3.12 or later, select 802.2.

  802.2 is the default.

- SNAP specifies the SNAP frame type.

  This setting indicates that the IPX clients and servers on the local Ethernet network follow the SNAP (SubNetwork Access Protocol) for the MAC header. This specification includes the IEEE 802.3 protocol format plus additional information in the MAC header.

- Enet II specifies the Ethernet II frame type.

  This setting indicates that IPX clients and servers on the local Ethernet network follow the Ethernet II protocol for the MAC header.

- None disables IPX routing and other IPX-specific features.

  If you choose this setting, the DSLPipe can bridge IPX, but without watchdog spoofing or the automatic RIP (Routing Information Protocol) and SAP (Service Advertising Protocol) data filters described in Handle IPX.

Dependencies: To determine the IPX frame type in use, enter the Config command on a NetWare server, or look at the NET.CFG file on an IPX client. Choose a setting based on this information:

- Select 802.3 if Frame=Ethernet_802.3.
- Select 802.2 if Frame=Ethernet_802.2.
- Select SNAP if Frame=Ethernet_SNAP.
- Select Enet II if Frame=Ethernet_II.

Parameter Location: Ethernet Profile, Mod Config/Ether options

---

IPX Net#

Description: This parameter lets you create a static route to another Ethernet network through the Connection Profile.

The value of IPX Net# specifies the network number of the router at the remote end of the connection.

Usage: Press Enter to open a text field. Then, type an Ethernet network number using an 8-digit (4-byte) hexadecimal value. The default is 00000000.

Specify the network number of the router at the remote end of the connection only if the router requires that the DSLPipe know its network number before connecting. You almost never need to set this parameter in a Connection Profile.

If you accept the default of 00000000, the Connection Profile is still valid, but the DSLPipe does not advertise the route until it makes a connection to the Ethernet network.

Example: `DE040600`

Dependencies: The IPX Net# parameter does not apply (IPX Net#=N/A) if the DSLPipe is not set up for IPX routing (Route IPX=No).

Parameter Location: Connection Profile, Connections

See Also: Route IPX

IPX Pool#

Description: This parameter specifies a unique IPX network number for all NetWare clients that are running PPP encapsulation and dialing in directly. The DSLPipe assigns network addresses to dial-in NetWare clients when they connect to the DSLPipe; these addresses are derived from this network number.

When you enter a value for IPX Pool#, the DSLPipe advertises a route to this network.

Usage: Press Enter to open a text field. Then, type an Ethernet network number using an 8-digit (4-byte) hexadecimal value. The default is 00000000.

The number you specify must be unique within your wide area IPX network, and must match the configuration of other routers on the local Ethernet network.

Press Enter again to close the text field.

Dependencies: Keep this additional information in mind:

- The dial-in Netware client must accept the network number set by IPX Pool#, although it can provide its own node number or accept a node number provided by the DSLPipe.
- If IPX Frame=None or IPX Routing=No, IPX Pool#=N/A.

Example: `FF0000037`

Parameter Location: Ethernet Profile, Mod Config/Ether options

---

IPX RIP

Description: This parameter controls how IPX RIP will be handled on this WAN link.

When a DSLPipe is used to connect NetWare clients to a very large IPX network, the IPX routing table created by the DSLPipe may become very large and unmanageable, and can cause the DSLPipe to run out of memory. As an alternative to maintaining these large routing tables locally, the DSLPipe may have a static IPX route to the corporate network and disable IPX RIP. Either end of the WAN link may disable or fine-tune IPX RIP behavior.

Usage: Press Enter to cycle through the choices.

- Both indicates that the device will both send and receive RIP updates on this WAN link.

  Both is the default.
- Send means the device will send RIP updates but will not receive them.
- Recv means the device will receive RIP updates but will not send them.
- Off means the device will neither send nor receive IPX RIP updates on this WAN link.

Parameter Location: Connection Profile: Ethernet→Connection→any profile→ IPX options...

Dependencies: This parameter is N/A if Peer=Dialin. If this parameter is set to Off, a static IPX route is required to the remote network. A static route is defined in an IPX Routes Profile.

See Also: IPX SAP, Peer

IPX SAP

Description: This parameter controls how IPX SAP will be handled on this WAN link.

When a DSLPipe is used to connect NetWare clients to a very large IPX network, the IPX service table created by the DSLPipe may become very large and unmanageable, and can cause the DSLPipe to run out of memory. As an alternative to maintaining these large service tables locally, the DSLPipe may create static service table entries and turn off IPX SAP. Either end of the WAN link may disable or fine-tune IPX SAP behavior.

Usage: Press Enter to cycle through the choices.

- Both indicates that the device will both send and receive SAP updates on this WAN link.

  Both is the default.
- Send means the device will send SAP updates but will not receive them.
- Recv means the device will receive SAP updates but will not send them.
- Off means the device will neither send nor receive IPX SAP updates on this WAN link.

Parameter Location: Connection Profile: Ethernet→Connection→any profile→ IPX options...

Dependencies: This parameter is N/A if Peer=Dialin. If this parameter is set to Off, a static IPX service table entry is required to the remote network. A static service entry is configured in an IPX Routes Profile.

See Also: IPX RIP, Peer

IPX Routing

Description: This parameter specifies whether the DSLPipe can perform these functions:

- Establish IPX routing
- Forward IPX packets
- Generate RIP and SAP packets
- Interpret incoming RIP and SAP packets

Usage: Press Enter to toggle between Yes and No.

- Yes enables the DSLPipe to perform IPX routing functions.

  Yes is the default.
- No disables the DSLPipe from performing IPX routing functions.

  You may want to choose No if your network uses a protocol other than IPX, or if your IPX network maintains such large RIP and SAP tables that the DSLPipe is spending too much time maintaining them.

Dependencies: Keep this additional information in mind:

- The setting of the IPX Routing parameter does not affect watchdog spoofing in IPX bridging.
- If you set IPX Routing=No while a WAN connection routing IPX exists, the DSLPipe does not tear down the connection, but no further IPX traffic can take place on the connection.
- If IPX Routing=No, these parameters do not apply and are set to N/A:
  - Route IPX
  - Dial Query
  - IPX Enet#
  - IPX Alias

  You can still configure IPX routes using the Active, Connection #, Hop Count, Network, Node, Server Name, Server Type, Socket, and Tick Count parameters. However, the routes have no effect until IPX Routing=Yes.
- The show netware command on the terminal server still operates when IPX Routing=No.

Parameter Location: Ethernet Profile: Ethernet, Mod Config

See Also: Active, Connection #, Dial Query, Hop Count, IPX Alias, IPX Enet#, Network, Node, Route IPX, Server Name, Server Type, Socket, Tick Count

---

IPX SAP

Description: This parameter controls how IPX SAP will be handled on this WAN link.

When a DSLPipe is used to connect NetWare clients to a very large IPX network, the IPX service table created by the DSLPipe may become very large and unmanageable, and can cause the DSLPipe to run out of memory. As an alternative to maintaining these large service tables locally, the DSLPipe may create static service table entries and turn off IPX SAP. Either end of the WAN link may disable or fine-tune IPX SAP behavior.

Usage: Press Enter to cycle through the choices.

- Both indicates that the device will both send and receive SAP updates on this WAN link.

  Both is the default.
- Send means the device will send SAP updates but will not receive them.
- Recv means the device will receive SAP updates but will not send them.
- Off means the device will neither send nor receive IPX SAP updates on this WAN link.

Parameter Location: Connection Profile: Ethernet→Connection→any profile→ IPX options...

Dependencies: This parameter is N/A if Peer=Dialin. If this parameter is set to Off, a static IPX service table entry is required to the remote network. A static service entry is configured in an IPX Routes Profile.

See Also: IPX RIP, Peer

IPX SAP Filter

Description: This parameter specifies the number of an IPX SAP Filter Profile to be applied to a WAN session or to the Ethernet interface. Depending on how the IPX SAP Filter Profile has been defined, this parameter has one or both of the following effects:

- IPX SAP Input filters apply to all SAP packets that the Ascend unit receives.
  Input filters screen advertised services and exclude them from its service table as specified in the filters.
- IPX SAP Output filters apply to SAP response packets that the Ascend unit transmits.
  If the Ascend unit receives a SAP request packet, it applies Output filters before transmitting the SAP response, and excludes services from the response packet as specified in the filters.

Usage: Press Enter to open a text field. Then type a number between 1 and 8. The number corresponds to an IPX SAP Filter Profile in the IPX SAP Filters menu.

When you set IPX SAP Filter to 0 (zero), all SAP data is included in the service table. Zero is the default.

Press Enter again to close the text field.

Parameter Location: Ethernet Profile, Mod Config/Ether options
Answer Profile, Answer/Session options
Connection Profile, Connections/Session Options

See Also: IPX Enet #, IPX Frame, IPX Routing, Server Name, Server Type, Type, Valid

Description: For the DSLPipe to run in proxy mode, you must supply the remote IPX network number and configure a static IPX route to that network.

See Also: IPX SAP Proxy Net #

IPX SAP Proxy

Description: This parameter enables or disables IPX SAP proxy mode in the DSLPipe. When a DSLPipe is used to connect NetWare clients to a very large IPX network, the SAP table created by the DSLPipe can become very large and unmanageable. As an alternative, the DSLPipe operating in proxy mode discards all SAP broadcasts seen on the network and resolves SAP queries from NetWare clients as it receives them, by forwarding the queries over the WAN link.

SAP proxy mode is recommended when only NetWare clients (not servers) are on the Ethernet side of DSLPipe.

Note: If the DSLPipe running in SAP proxy mode has NetWare servers on its Ethernet, it stores the relevant SAP entries for those servers and advertises them across the WAN interface as a normal SAP broadcast.

Usage: Press Enter to toggle between Yes and No.

- Yes enables proxy mode.
- No disables proxy mode.
  No is the default.

Parameter Location: Ethernet Profile: Ethernet→Mod Config→Ether options...

Dependencies: For the DSLPipe to run in proxy mode, you must supply the remote IPX network number and configure a static IPX route to that network.

See Also: IPX SAP Proxy Net #

IPX SAP Proxy Net#

Description: This parameter specifies the IPX network number of the device on the other end of the WAN link. The IPX network number must also be specified in an IPX Route Profile.

Usage: Press Enter to open a text field. Then type an 8-digit hexadecimal IPX network number. Press Enter again to close the text field.

Parameter Location: Ethernet Profile: Ethernet→Mod Config→Ether options...

Dependencies: This parameter is N/A if IPX SAP Proxy =Off.

See Also: IPX SAP Proxy

LAN Adrs

Description: This parameter specifies the IP address of a station or router at the remote end of the link specified by the Connection Profile.

Usage: Press Enter to open a text field. Then, type the IP address of a remote station or router; you can also specify a netmask.

An IP address consists of four numbers between 0 and 255, separated by periods. If a netmask is in use on the network, you must specify it. Separate a netmask from the IP address with a slash.

The default setting is 0.0.0.0/0; an answering Connection Profile with this setting matches all incoming IP addresses.

If you do not enter a netmask, the DSLPipe assumes the default for your network class:

- Class A: 1.0.0.0 to 127.255.255.255 /8
- Class B: 128.0.0.0 to 191.255.255.255 /16
- Class C: 192.0.0.0 to 223.255.255.255 /24

The netmask should not mask any network bits. For example, 130.15.3.44/12 is not valid because it is a Class B address whose netmask cannot be smaller than 16.

If you enter a 32-bit mask, you are specifying a connection to a specific host, rather than to a group of hosts on a subnet.

After you make your specifications, press Enter to close the text field.

`Example:` `200.207.23.101/24`

Dependencies: Keep this additional information in mind:

- The LAN Adrs parameter in the first Connection Profile is the same as the Rem Addr parameter in the Configure Profile.

- The value of the LAN Adrs parameter on the local DSLPipe must match the IP Adrs parameter of the Ascend unit at the remote end of the link.
- No two calling Connection Profiles should have the same LAN Adrs.
- Setting LAN Adrs to 0.0.0.0/0 and clearing the Station parameter resets all parameters in the Connection Profile to their defaults.
- The LAN Adrs parameter does not apply (LAN Adrs=N/A) if the DSLPipe does not support IP (Route IP=No).
- If you do not know the right IP address to enter, you must obtain it from the network administrator.

  Do not attempt to configure an IP address by guesswork!

Parameter Location: Connection Profile, Connections

See Also: Encaps, IP Adrs, Route IP, Station

Length

Description: This parameter indicates the number of bytes in a packet that the DSLPipe compares to the setting of the Value parameter.

The Offset parameter specifies the starting position; the DSLPipe ignores the portion of the packet that exceeds the Length specification. In other words, the Offset parameter hides the left-most bytes of data, while the Length parameter hides the right-most bytes of data.

The DSLPipe applies the value of the Mask parameter before comparing the bytes to the setting of the Value parameter. The Mask value consists of the same number of bytes as the Length parameter. A mask hides the part of a number that appears behind the binary zeroes in the mask; for example, if Mask=ffff0000 in hexadecimal format, the DSLPipe uses only the first 16 binary digits in the comparison, since f=1111 in binary format.

Usage: Press Enter to open a text field. Then, type the number of bytes to use for comparison. You can enter a number between 0 and 8.

The default value is 0. When you accept the default, DSLPipe uses no bytes for comparison; all packets match the filter.

Press Enter again to close the text field.

Example: Suppose you have a filter that drops packets and has these specifications:

```
Forward=No
Offset=4
Length=3
Mask=ffffff
Value=123
More=No
```

When the 10-byte packet xycd123456 passes through the filter, the DSLPipe removes the leading four bytes, because Offset=4. The data 123456 remains. Next, the DSLPipe removes the trailing three bytes, because Length=3; only the value 123 remains. The Mask is ffffff, which contains all ones (1s) when converted to binary numbers; therefore, the Mask value does not hide any binary digits and passes 123 through. When the DSLPipe compares 123 to the setting of the Value parameter, a match occurs and the DSLPipe does not forward the packet.

Dependencies: In a Filter Profile, Length does not apply (Length=N/A) for an IP filter (Type=IP).

Parameter Location: Filter Profile, Filter/Generic

See Also: Offset, Mask, Value

Link Comp

Description: This parameter turns data compression on or off for a PPP link.

Usage: Press Enter to cycle through the choices.

- Stac turns on data compression.

  The DSLPipe applies the STACKER LZS compression/decompression algorithm. STAC is the default.
- MS-Stac turns on Microsoft LZS Coherency Compression for Windows95, a proprietary compression scheme for Windows 95 only (not for Windows NT).

  Both sides of the link must set Link Comp=Stac or Link Comp=MS-Stac to turn on data compression.

- None turns off data compression.

Dependencies: Keep this additional information in mind:

- Stacker LZS Compression (as defined in the Internet Draft of November 1995) and Microsoft LZS Coherency Compression for Windows 95 both use the same PPP option to indicate that their compression scheme is in use.

  Therefore, a router can have difficulty determining exactly which compression method a caller is requesting. Ascend units handle this ambiguity in the call by always using the compression scheme specified in the Connection Profile; if there is no Connection Profile, the Ascend unit uses the compression scheme specified in the Answer Profile.

  If the caller requests MS-Stac and the profile does not specify MS-Stac compression, the connection seems to come up correctly, but no data is routed. If the profile is configured with MS-Stac and the caller does not acknowledge that compression scheme, the DSLPipe attempts to use standard Stac compression. If it cannot use standard Stac compression, it uses no compression at all.
- Both sides of the link must set Link Comp=Stac to turn on data compression.
- The Link Comp parameter applies only if the link uses PPP encapsulation (Encaps=PPP or Encaps=MPP).

  When you choose Encaps=MPP, both the dialing side and the answering side of the link must support MP+. If only one side supports MP+, the connection uses MP or standard single-channel PPP. When you choose Encaps=PPP, the connection uses only PPP.
- Link Comp in the Answer Profile applies to incoming calls for which no Connection Profile exists; if a Connection Profile exists, the setting of its Link Comp parameter takes precedence.
- If Profile Reqd=Yes in the Answer Profile, Link Comp does not apply (Link Comp=N/A) in the Answer Profile.

Parameter Location: Answer Profile, Answer/PPP options
Connection Profile, Connections/Encaps options

See Also: VJ Comp

Link Mgmt

Description: This parameter specifies the link management protocol used between the DSLPipe and the frame relay switch.

From the viewpoint of the DSLPipe, a frame relay switch is an endpoint for all DLCIs (Data Link Connection Indicators) connecting to it. A DLCI identifies a Connection Profile as a logical link; because more than one Connection Profile can connect to a frame relay switch, a physical circuit can carry more than one logical link. The DLCI parameter enables the frame relay switch to identify each Connection Profile.

The frame relay switch connects the endpoints of the DLCIs to each other to make a virtual permanent circuit to which users can connect. The circuit acts like a wire between two endpoints with a fixed maximum bandwidth.

Usage: Press Enter to cycle through the choices.

- None specifies no link management.
  The DSLPipe assumes that the physical link is up and that all logical links (as defined by the DLCI parameter) are active on the physical link.
  None is the default.
- T1.617D specifies the link management protocol defined in ANSI T1.617 Annex D.
  Ask your service provider whether you should specify T1.617D.

Parameter Location: Frame Relay Profile, Frame Relay

See Also: DLCI

List Attempt

Description: This parameter enables or disables the DNS (Domain Name System) List Attempt feature.

DNS can return multiple addresses for a hostname in response to a DNS query. Unfortunately, DNS has no information about the availability of those hosts. Users typically attempt to access the first address in the list. If that host is unavailable, the connection fails and the user must initiate a new DNS query or

Telnet attempt. If the login attempt occurs automatically as part of Immediate Telnet, the DSLPipe tears down the physical connection when the initial connection attempt fails.

The DNS List Attempt feature helps the DSLPipe avoid tearing down physical links by enabling the user to try one entry in the DNS list of hosts when logging in through Telnet from the terminal server; if that connection fails, the user can try each succeeding entry.

Usage: Press Enter to toggle between Yes and No.

- Yes specifies that the DSLPipe enables a user to try the next host in the DNS list if the first Telnet login attempt fails.
- No turns off the List Attempt feature.

  No is the default.

Dependencies: The List Attempt parameter does not apply (List Attempt=N/A) if Telnet and Immediate Telnet are both disabled.

Parameter Location: Ethernet Profile: Ethernet→Mod Config→DNS

Location

Description: This parameter specifies the location of the DSLPipe.

Usage: Press Enter to open a text field. Then, type a description of the DSLPipe's location. You can enter up to 80 characters. An SNMP management application can read this field, but the value you enter does not affect the operation of the DSLPipe.

Press Enter again to close the text field.

Parameter Location: System Profile, Sys Config

See Also: Contact

Log Facility

Description: This parameter specifies how the Syslog host sorts system logs. The Syslog host is the station to which the DSLPipe sends system logs.

Usage: Press Enter to cycle through the choices. You can select one of these settings:

- Local0
  Local0 is the default.
- Local1
- Local2
- Local3
- Local4
- Local5
- Local6
- Local7

All system logs using the same setting are grouped together in the host's file system. That is, all system logs using the Local0 facility are grouped together, all system logs using the Local1 facility are grouped together, and so on.

Dependencies: The Log Facility parameter applies only when you have enabled the Syslog host by setting Syslog=Yes.

Parameter Location: Ethernet Profile, Mod Config/Log

See Also: Log Host, Syslog

Log Host

Description: This parameter specifies the IP address of the Syslog host—the station to which the DSLPipe sends system logs.

Usage: Press Enter to open a text field. Then, type the IP address of Syslog host.

An IP address consists of four numbers between 0 and 255, separated by periods. The default value is 0.0.0.0.

Press Enter to close the text field.

Example: `200.207.23.1`

Dependencies: Keep this additional information in mind:

- The Syslog host must be running UNIX.
- The Log Host parameter applies only if you enable the Syslog host by setting Syslog=Yes.

Parameter Location: Ethernet Profile, Mod Config/Log

See Also: Log Facility, Syslog

LQM

Description: This parameter specifies whether the DSLPipe requests Link Quality Monitoring (LQM) when answering a PPP call.

LQM is a feature that enables the DSLPipe to monitor the quality of a link. LQM counts the number of packets sent across the link and periodically asks the remote end how many packets it has received. Discrepancies are evidence of packet loss and indicate link quality problems.

LQM causes the generation of periodic link quality reports. Both ends of the link exchange these reports.

Usage: Press Enter to toggle between Yes and No.

- Yes specifies that the DSLPipe requests LQM.
- No specifies that the DSLPipe does not request LQM.
  No is the default.

Dependencies: Keep this additional information in mind:

- Both sides of the link negotiate the interval between periodic link quality reports; however, the interval must fall between the minimum interval (as set by LQM Min) and the maximum interval (as set by LQM Max).
- If LQM is turned off (LQM=No), the LQM Max and LQM Min parameters do not apply (LQM Max=N/A and LQM Min=N/A).
- LQM applies only if Encaps=PPP.

- LQM in the Answer Profile applies to incoming calls for which no Connection Profile exists; if a Connection Profile exists, the setting of its LQM parameter takes precedence.
- If Profile Reqd=Yes in the Answer Profile, LQM does not apply (LQM=N/A) in the Answer Profile.

Parameter Location: Answer Profile, Answer/PPP options
Connection Profile, Connections/Encaps options

See Also: Encaps, LQM Max, LQM Min

LQM Max

Description: This parameter specifies the maximum duration between link quality reports, measured in tenths of a second.

Usage: Press Enter to open a text field. Then, type a number between 0 and 600. The default is 600. Press Enter again to close the text field.

Dependencies: Keep this additional information in mind:

- If LQM=No, the LQM Max parameter does not apply (LQM Max=N/A).
- LQM Max in the Answer Profile applies to incoming calls for which no Connection Profile exists; if a Connection Profile exists, the setting of its LQM Max parameter takes precedence.
- If Profile Reqd=Yes in the Answer Profile, LQM Max does not apply (LQM Max=N/A) in the Answer Profile.

Parameter Location: Answer Profile, Answer/PPP options
Connection Profile, Connections/Encaps options

See Also: LQM, LQM Min

LQM Min

Description: This parameter specifies the minimum duration between link quality reports, measured in tenths of a second.

Usage: Press Enter to open a text field. Then, type a number between 0 and 600. The default is 600. Press Enter again to close the text field.

Dependencies: Keep this additional information in mind:

- If LQM=No, the LQM Min parameter does not apply (LQM Min=N/A).
- LQM Min in the Answer Profile applies to incoming calls for which no Connection Profile exists; if a Connection Profile exists, the setting of its LQM Min parameter takes precedence.
- If Profile Reqd=Yes in the Answer Profile, LQM Min does not apply (LQM Min=N/A) in the Answer Profile.

Parameter Location: Answer Profile, Answer/PPP options
Connection Profile, Connections/Encaps options

See Also: LQM, LQM Max

Mask

Description: In a filter of type Generic, this parameter specifies a 16-bit hexadecimal bitmask that the DSLPipe applies to the data contained in the specified bytes in a packet. A mask hides the part of a number that appears behind the binary zeroes in the mask; for example, if Mask=ffff0000, the DSLPipe uses only the first 16 binary digits in the comparison, since f=1111 in binary format.

The DSLPipe applies the Mask parameter starting at the position specified by the Offset parameter. The setting you specify for Mask must contain the same number of bytes as the Length parameter. The DSLPipe then compares the unmasked portion of the packet with the value specified by the Value parameter.

Usage: Press Enter to open a text field. Then, type a hexadecimal number. You can enter a number between 00 and ffffffffffffffff.

The default is 00. When you accept the default, the DSLPipe uses the data in the packet as is for comparison purposes.

Press Enter to close the text field.

Example: This example specifies that the DSLPipe masks all but the first 24 bits of the data:

```
Mask=ffffff0000000000
```

Dependencies: Mask does not apply (Mask=N/A) for an IP filter (Type=IP).

Parameter Location: Filter Profile, Filter/Generic

See Also: Length, Offset, Type, Value

Max Ch Count

Description: This specifies the maximum number of channels allowed on an MP+ call.

Usage: Press Enter to open a text field. Then, type a number between 1 and the maximum number of channels your system supports. The default setting is 1. Press Enter again to close the text field.

Dependencies: Keep this additional information in mind:

- The Max Ch Count parameter applies only to dynamic MP+ calls (Encaps=MPP).
- If Profile Reqd=Yes in the Answer Profile, Max Ch Count does not apply (Max Ch Count=N/A) in the Answer Profile.
- For optimum MP+ performance, both sides of a connection must set these parameters to the same values:
  - Base Ch Count (in the Connection Profile)
  - Min Ch Count (in the Answer Profile and the Call Profile)
  - Max Ch Count (in the Answer Profile and the Connection Profile)
- Max Ch Count in the Answer Profile applies to incoming calls for which no Connection Profile exists; if a Connection Profile exists, the setting of its Max Ch Count parameter takes precedence.

Parameter Location: Answer Profile, Answer/PPP options
Connection Profile, Connections/Encaps options

See Also: Add Pers, Base Ch Count, Call Mgm, Encaps

Metric

Description: This parameter appears in a Connection Profile and a Static Rtes Profile. Its functionality differs depending on the profile:

- In a Connection Profile, the Metric parameter determines the virtual hop count of the link.
- In a Static Rtes Profile, the Metric parameter determines the virtual hop count of the route.

If there are two routes available to a single destination network, you can ensure that the DSLPipe uses any available nailed-up channel before using a switched channel by setting the Metric parameter to a value higher than the metric of any nailed-up route. The higher the value entered, the less likely that the DSLPipe will bring the link or route online. The DSLPipe uses the lowest metric.

Usage: Press Enter to open a text field, Then, type a number between 1 and 15. This value is the virtual hop count. The default setting is 7. Press Enter again to close the text field.

Example: If a route to a station takes three hops over nailed-up lines, and Metric=4 in a Connection Profile that reaches the same station, the DSLPipe does not bring the Connection Profile's link online.

Dependencies: Keep this additional information in mind:

- The Metric parameter in a Connection Profile does not apply to bridged connections.
- If you enable RIP (Routing Information Protocol) across the WAN in a Connection Profile or an Answer Profile (RIP=Recv or RIP=Both), the hop count for the route can differ from the value of the Metric parameter in the Route Profile because the DSLPipe always uses the lower hop count.
- The hop count includes the metric of each switched link in the route.
- The Metric only applies to IP connections.

Parameter Location: Connection Profile: Ethernet→Connections→Any Connection Profile→IP Options
Route Profile: Ethernet→Static Rtes→Any Route Profile

See Also: Private, RIP

Min Ch Count

Description: This parameter specifies the minimum number of channels an MP+ call maintains.

Usage: Press Enter to open a text field. Then, type a number between 1 and 32. The default setting is 1. Press Enter again to close the text field.

Dependencies: The Min Ch Count parameter applies only to MP+ calls (Encaps=MPP). For optimum MP+ performance, both sides of a connection must set these parameters to the same values:

- Base Ch Count (in the Connection Profile)
- Min Ch Count (in the Answer Profile and the Call Profile)
- Max Ch Count (in the Answer Profile and the Connection Profile)

Parameter Location: Connection Profile, Connections/Encaps options
Answer Profile, Answer/PPP options

See Also: Max Ch Count

More

Description: In a filter of type Generic, this parameter specifies whether the DSLPipe passes the packet to the next filter specification in the profile.

Use this parameter when you need a generic filter wider than the 8-byte limit of the Length parameter. For example, suppose a packet is 16 bytes long (128 bits). You can compare only 8 bytes in a filter because the maximum value of the Length parameter is 8. To compare all 16 bytes, you specify two 8-byte filters linked by the More parameter.

Usage: Press Enter to toggle between Yes and No.

- Yes specifies that the DSLPipe applies the next filter in the profile before deciding whether to forward the packet.

If you set More=Yes, the filter can examine multiple noncontiguous bytes within a packet by "marrying" the current filter to the one that immediately follows it.

- No specifies that the DSLPipe does not apply the next filter in the profile before deciding whether to forward the packet.

  No is the default.

Example: Input filter 01 and input filter 02 examine different bytes of the same packet and apply a logical AND to the results in order to determine whether the packet matches the specification:

```
In filter 01...Valid=Yes
In filter 01...Type=Generic
In filter 01...Generic...Forward=No
In filter 01...Generic...Offset=04
In filter 01...Generic...Length=8
In filter 01...Generic...Value=abc
In filter 01...Generic...More=Yes

In filter 02...Valid=Yes
In filter 02...Type=Generic
In filter 02...Generic...Forward=No
In filter 02...Generic...Offset=2
In filter 02...Generic...Length=8
In filter 02...Generic...Value=123
In filter 02...Generic...More=No
```

In this example, the DSLPipe compares 16 bytes of each data packet. The match occurs only if *all the* noncontiguous bytes contain the specified values.

Dependencies: Keep this additional information in mind:

- The More parameter does not apply (More=N/A) if you are using an IP filter (Type=IP).

- The next filter must be a Generic filter (Type=Generic) and must be activated (Valid=Yes); otherwise, the DSLPipe ignores the filter.

Parameter Location: Filter Profile, Filter/Generic

See Also: Forward, Length, Offset, Type, Value, Valid

MRU

Description: This parameter specifies the maximum number of bytes the DSLPipe can receive in a single packet on a PPP link. MRU stands for Maximum Receive Unit.

Usage: The default setting is 1524; you should accept this default unless the device at the remote end of the link cannot support it.

If the administrator of the remote network specifies that you must change this value, press Enter to open a text field. For an Answer Profile or a Connection Profile, type a number between 1 and 1524. For a Frame Relay Profile, type a value between 128 and 1600.

Press Enter again to close the text field.

Dependencies: Keep this additional information in mind:

- The MRU parameter applies to any link using PPP encapsulation (Encaps=MPP or Encaps=PPP).

  When you choose Encaps=MPP, both the dialing side and the answering side of the link must support MP+. If only one side supports MP+, the connection uses MP or standard single-channel PPP. When you choose Encaps=PPP, the connection uses only PPP.
- MRU in the Answer Profile applies to incoming calls for which no Connection Profile exists; if a Connection Profile exists, the setting of its MRU parameter takes precedence.
- If Profile Reqd=Yes in the Answer Profile, MRU does not apply (MRU=N/A) in the Answer Profile.

Parameter Location: Answer Profile, Answer/PPP options
Connection Profile, Connections/Encaps options
Frame Relay Profile, Frame Relay

See Also: Encaps

My Addr

See “IP Adrs” on page 1-58.

My Name

See “Name” on page 1-87.

My Num A

Description: This parameter specifies the phone number assigned to the line. If two phone numbers are assigned to the line, specify one here and one in My Num B.

When the DSLPipe receives a multichannel MP+ call, it reports the primary phone number (My Num A) and the secondary phone number (My Num B) to the calling party. The calling DSLPipe can then add more channels. If you do not specify a phone number and the calling DSLPipe needs to add more channels, it redials the phone number it used to make the first connection.

Usage: Press Enter to open a text field and then type a telephone number. The character set is limited to the following characters:

1234567890()[]!z-*#”

You can include a hyphen in the phone number but no spaces.

Example: 5105551972

Parameter Location: Configure...

Dependencies: You must get this number from the telephone company providing your service.

See Also: My Num B

My Num B

Description: This parameter specifies the phone number assigned to the line. If two phone numbers are assigned to the line, specify one here and one in My Num A.

When the DSLPipe receives a multichannel MP+ call, it reports the primary phone number (My Num A) and the secondary phone number (My Num B) to the calling party. The calling DSLPipe can then add more channels. If you do not specify a phone number and the calling DSLPipe needs to add more channels, it redials the phone number it used to make the first connection.

Usage: Press Enter to open a text field and then type a telephone number. The character set is limited to the following characters:

1234567890()[]!z-*#”

You can include a hyphen in the phone number but no spaces.

Example: 5105551972

Parameter Location: Configure...

Dependencies: You must get this number from the telephone company providing your service.

See Also: My Num A

N391

Description: This parameter specifies how many polling cycles the DSLPipe waits before requesting a full status report.

Usage: Press Enter to open a text field. Then, type the number of polling cycles that you want the DSLPipe to wait. You can specify a number from 1 to 255. If you specify 1, the DSLPipe requests a full status report every polling cycle. The default is 6. Press Enter again to close the text field.

Dependencies: The N391 parameter applies only if Link Mgmt=T1.617D.

Parameter Location: Frame Relay Profile, Frame Relay

See Also: Link Mgmt

N392

Description: This parameter specifies the maximum number of error events that can occur in the sliding window defined by N393. The error events can include link reliability errors, protocol errors, and sequence number errors. If the DSLPipe exceeds the threshold defined by N392, the frame relay switch declares the DSLPipe inactive.

Usage: Press Enter to open a text field. Then, type a number between 1 and 10. The default is 3. Press Enter again to close the text field.

Dependencies: Keep this additional information in mind:

- The N392 parameter applies only if Link Mgmt=T1.617D.
- If you turn off the DSLPipe, disconnect its WAN connection, or set Active=No in the Frame Relay Profile, the setting of N392 multiplied by the setting of N391 indicates the time it takes the frame relay switch to declare an inactive state.

Parameter Location: Frame Relay Profile, Frame Relay

See Also: Link Mgmt, N391, N393

N393

Description: This parameter specifies the width of the sliding window used by the N392 parameter. For example, if N393=5, the sliding window begins five monitored events ago and extends to the present. A monitored event occurs when the DSLPipe makes a Status Enquiry.

Usage: Press Enter to open a text field. Then, type a number between 1 and 10. The default is 4. Press Enter again to close the text field.

Dependencies: The N393 parameter applies only if Link Mgmt=T1.617D.

Parameter Location: Frame Relay Profile, Frame Relay

See Also: Link Mgmt, N392

Nailed Grp

Description: This parameter associates a nailed-up Frame Relay group with the profile.

Usage: Press Enter to open a text field. Type a number from 1 to the maximum number of nailed-up channels that your DSLPipe allows. The default is 1. Press Enter again to close the text field.

Dependencies: Keep this additional information in mind:

- The Nailed Grp parameter does not apply (Nailed Grp=N/A) if the link consists entirely of switched channels (Call Type=Switched).
- Do not associate a group with more than one active Frame Relay Profile.

Parameter Location: Frame Relay Profile, Frame Relay

See Also: Activation, Call Type, Group

Name

Description: This parameter appears in each of these profiles:

- Filter Profile
- IPX SAP Filters Profile
- Security Profile
- SNMP Traps Profile
- Static Rtes Profile
- System Profile

The functionality of the Name parameter differs depending on the profile:

- In a Security Profile, Filter Profile, System Profile, or IPX SAP Filters Profile, the Name parameter specifies the name of the profile.

  The DSLPipe sends the System Profile name to the remote device whenever it establishes a PPP link. The System Profile name appears in the top line of the Edit display of the Control Monitor. Always enter a system name to identify the DSLPipe.

When the DSLPipe receives a PPP or MP+ call from an Ascend unit, it tries to match the caller's Name to the value of the Station parameter in some Connection Profile. If the DSLPipe finds a match and authentication is turned on, the DSLPipe then tries to match the caller's Send PW value to the Recv PW value in that same Connection Profile.

The Control Monitor is the menu-based user interface for configuring, managing, and monitoring the DSLPipe. It consists of nine windows—eight status windows and a single edit window.

Note: The Name parameter in the System Profile is the same as the My Name parameter in the Configure Profile.

- In a Static Rtes Profile, the Name parameter specifies the name of the route's destination.

  Note that you cannot change the name of the first route; its value is always Default.

- In an SNMP Traps Profile, the Name parameter specifies the SNMP manager to which the DSLPipe sends traps-PDUs (Protocol Data Units).

  SNMP (Simple Network Management Protocol) provides a way for computers to share networking information. In SNMP, two types of communicating devices exist: agents and managers. An agent provides networking information to a manager application running on another computer. The agents and managers share a database of information, called the Management Information Base (MIB).

  A trap is a mechanism in SNMP for reporting system change in real time. To report system change, the DSLPipe sends a traps-PDU across the Ethernet interface to the SNMP manager. A complete list specifying the events that cause the DSLPipe to send a traps-PDU appears in the Ascend Enterprise Traps MIB.

Usage: Press Enter to open a text field. Then, type a name. You can enter up to 16 characters for the Name parameter in all profiles except the Static Rtes Profile and the SNMP Traps Profile. In these profiles, you can enter up to 31 characters for the Name parameter.

Because the DSLPipe uses the Name parameter in the System Profile for authentication, you must type it exactly as the remote network expects it. In this case, Name is case sensitive.

Press Enter again to close the text field.

Parameter Location: Security Profile, Security
Filter Profile, Filters
System Profile, Sys Config
IPX SAP Filter Profile, IPX SAP Filters
Static Rtes Profile, Static Rtes
SNMP Traps Profile, SNMP Traps

Net Adrs

Description: In a Bridging Profile, this parameter specifies the IP address of a device at the remote end of the link.

The DSLPipe uses the Bridging Profile to build a bridge table of matching MAC and IP addresses. The Net Adrs parameter corresponds to the IP address of each remote device; the Enet Adrs parameter corresponds to the MAC address of each remote device.

These parameters enable the DSLPipe to perform proxy ARP (Address Resolution Protocol). Whenever the DSLPipe receives an ARP request from a specified IP address, it checks to see whether the IP address matches one in its bridge table. If it does, the DSLPipe returns its own MAC address.

Usage: Press Enter to open a text field. Then, type the IP address of the device on the remote network.

An IP address consists of four numbers between 0 and 255, separated by periods. If a netmask is in use on the network, you must specify it. Separate a netmask from the IP address with a slash.

The default value is 0.0.0.0/0.

Press Enter to close the text field.

Example: `200.207.23.101/24`

Parameter Location: Bridging Profile, Bridge Adrs

See Also: Enet Adrs

NetWare t/o

Description: This parameter specifies the length of time, in minutes, that the DSLPipe performs watchdog spoofing for NetWare connections. Here is an explanation of watchdog spoofing:

Ordinarily, when a NetWare server does not receive a reply to the watchdog session keepalive packets it sends to a client, it closes the connection. When you select Server mode for the Handle IPX parameter, however, the DSLPipe replies to NCP watchdog requests on behalf of clients on the other side of the bridge; in other words, the DSLPipe tricks the server watchdog process into believing that the link is still active.

The time period for watchdog spoofing specified by the NetWare t/o parameter begins when the WAN session goes offline. If the WAN session reconnects, the DSLPipe cancels the timeout.

NetWare t/o applies when the DSLPipe is on a LAN containing a NetWare server.

Usage: Press Enter to open a text field. Then, type the timeout value in minutes. You can enter any value from 0 to 65535. The default value is 0 (zero); when you accept the default, the DSLPipe responds to server watchdog requests indefinitely. Press Enter again to close the text field.

Dependencies: The NetWare t/o parameter does not apply (NetWare t/o=N/A) if Handle IPX=None.

Parameter Location: Connection Profile, Connections/IPX options

See Also: Handle IPX

Network

Description: This parameter specifies the unique internal network number assigned to the NetWare server.

Usage: Press Enter to open a text field. Then, type the unique 4-byte hexadecimal number provided by your network administrator. The values 00000000 and ffffffff are not valid. Press Enter again to close the text field.

Example: A00100001

Dependencies: For the Network parameter to apply, you must enable IPX routing in the Connection Profile by setting Route IPX=Yes.

Parameter Location: IPX Route Profile, IPX Routes

See Also: Route IPX

Node

Description: This parameter specifies the node number of the NetWare server.

Usage: Press Enter to open a text field. Then, type the node number of the server. Typically, a server running NetWare 3.11 or later has a node number of 0000000000001. Press Enter again to close the text field.

Dependencies: For the Node parameter to apply, you must enable IPX routing in the Connection Profile by setting Route IPX=Yes.

Parameter Location: IPX Route Profile, IPX Routes

See Also: Route IPX

Offset

Description: In a filter of type Generic, this parameter specifies the number of bytes masked from the start of the packet. The byte position specified by the Offset parameter is called the byte-offset.

Starting at the position specified by the Offset parameter, the DSLPipe applies the value of the Mask parameter. A mask hides the part of a number that appears behind the binary zeroes in the mask; for example, if Mask=ffff0000 in hexadecimal format, the DSLPipe uses only the first 16 binary digits in the comparison, since f=1111 in binary format. The DSLPipe then compares the unmasked portion of the packet specified by the Length parameter with the value specified by the Value parameter.

Usage: Press Enter to open a text field. Then, type the number of starting bytes in a packet that the DSLPipe ignores for comparison and masking purposes.

The default is 0. When you accept the default, the DSLPipe starts comparing and masking data at byte 1.

Press Enter again to close the text field.

Example: Suppose you have a filter that drops packets and has these specifications:

```
Forward=No
Offset=4
Length=3
Mask=ffffff
Value=123
More=No
```

When the 10-byte packet xycd123456 passes through the filter, the DSLPipe removes the leading four bytes, because Offset=4. The data 123456 remains. Next, the DSLPipe removes the trailing three bytes, because Length=3; only the value 123 remains. The Mask is ffffff, which contains all ones (1s) when converted to binary numbers; therefore, the Mask value does not hide any binary digits and passes 123 through. When the DSLPipe compares 123 to the setting of the Value parameter, a match occurs and the it does not forward the packet.

Dependencies: Keep this additional information in mind:

- The Offset parameter does not apply (Offset=N/A) for an IP filter (Type=IP).
- If a previous filter set More=Yes, Offset starts at the endpoint of the previous segment.

Parameter Location: Filter Profile, Filter

See Also: Length, Mask, More

Operations

Description: This parameter enables or disables read-only security.

Usage: Press Enter to toggle between Yes and No.

- Yes enables users to view DSLPipe profiles and change the value of any parameter.

Yes is the default.

- No permits users to view DSLPipe profiles, but not to change the value of any parameter.

  If you specify No, users cannot access most DO commands. Only DO Esc, DO Close Telnet, and DO password are available.

Parameter Location: Security Profile, Security

Passwd

Description: This parameter the password that activates a Security Profile. The first Security Profile, Default, has no password.

Usage: Press Enter to open a text field. Then, type up to 20 characters. Press Enter again to close the text field.

Dependencies: Keep this additional information in mind:

- Passwd is case sensitive.

  The user must enter the password exactly as you specify it here.

- If the value of the Passwd parameter in the Security Profile is *SECURE*, you cannot edit Security Profiles.

  If you want to edit Security Profiles, you must log into a Security Profile whose Edit Security parameter is set to Yes.

Parameter Location: Security Profile, Security

See Also: Edit Security

Peer

Description: This parameter lets you select between two classes of peers to connect via the DSLPipe—IPX routers and standalone workstations. It is best to allow two classes of peers to connect through an Ascend unit; other IPX routers, and standalone workstations. Typically, standalone workstations are mobile stations that connect via modem. By specifying a peer class for each Connection Profile, you can improve network security.

Usage: Press Enter to cycle through the choices.

- Router specifies that the caller is an IPX router.
  Router is the default.
- Dialin specifies that the caller is a dial-in NetWare client that incorporates PPP software and dial-out hardware, but does not have an Ethernet interface.
  This setting causes the DSLPipe to assign the caller an IPX address derived from the value of IPX Pool#.

Dependencies: If IPX Routing=No or Route IPX=No, the Peer parameter does not apply (Peer=N/A).

Parameter Location: Connection Profile, Connections/IPX options

See Also: IPX Pool#

Preempt

Description: This parameter specifies the number of idle seconds the DSLPipe waits before using one of the channels of an idle link for a new call.

Usage: Press Enter to open a text field. Then, type a number between 0 and 65535. The DSLPipe sets no time limit if you enter 0 (zero). The default setting is 60. Press Enter again to close the text field.

Dependencies: Keep this additional information in mind:

- If all channels of a link are nailed up (Call Type=Nailed), the Preempt parameter does not apply (Preempt=N/A) in either the Answer or Connection Profile.
- Preempt in the Answer Profile applies to incoming calls for which no Connection Profile exists; if a Connection Profile exists, the setting of its Preempt parameter takes precedence.
- If Profile Reqd=Yes in the Answer Profile, Preempt does not apply (Preempt=N/A) in the Answer Profile.

Parameter Location: Answer Profile, Answer/Session options
Connection Profile, Connections/Session options

See Also: Call Type

Preference

Description: This parameter specifies the preference value for a static IP route configured in an IP Route Profile or Connection Profile.

When choosing which routes to put in the routing table, the router first compares the Preference values, preferring the lower number. If the Preference values are equal, the router compares the Metric values, using the route with the lower Metric.

Usage: Press Enter to open a text field. Then, type a number between 0 and 255. Zero is the default for connected routes (such as the Ethernet). The value of 255 means "Don't use this route;" this value is meaningful only for Connection Profiles. Press Enter again to close the text field.

Dependencies: These are the default values for different types of routes:

- Routes learned from OSPF=10
- Routes learned from ICMP Redirects=30
- Routes learned from RIP=100

This set of preference values gives static routes and RIP routes an equal value, with ICMP Redirects taking precedence over both. Note that OSPF routes take precedence over all the other types.

Parameter Location: Connection Profile: Connections→Any Connection Profile→ IP Options
IP Route Profile: Static Rtes→Any Route Profile

Pri DNS

Description: This parameter specifies the IP address of the primary domain name server.

Domain Name System (DNS) is a TCP/IP service that enables you to specify a symbolic name instead of an IP address. A symbolic name consists of a username and a domain name in the format *username@domain name*. The *username* corresponds to the host number in the IP address. The *domain name* corresponds

to the network number in the IP address. A symbolic name might be steve@abc.com or joanne@xyz.edu.

DNS maintains a database of network numbers and corresponding domain names on a domain name server. When you use a symbolic name, DNS translates the domain name into an IP address, and sends it over the network. When the Internet service provider receives the message, it uses its own database to look up the username corresponding to the host number.

Usage: Press Enter to open a text field. Then, type the IP address of the primary domain name server.

The address consists of four numbers between 0 and 255, separated by periods. The default value is 0.0.0.0. Accept this default if you do not have a domain name server.

Press Enter again to close the text field.

Example: `200.207.23.1`

Parameter Location: Ethernet Profile, Mod Config/DNS

See Also: Domain Name, Sec DNS

Private

Description: This parameter appears in a Connection Profile and a Static Rtes Profile. Its functionality differs depending on the profile:

- In a Connection Profile, the Private parameter specifies whether the DSLPipe discloses the IP address indicated by LAN Adrs when queried by RIP (Routing Information Protocol) or another routing protocol.
- In a Static Rtes Profile, the Private parameter specifies whether the DSLPipe discloses the existence of the IP address indicated in the route when queried by RIP or another routing protocol.

Usage: Press Enter to toggle between Yes and No.

- Yes disables advertising.
  The DSLPipe does not advertise the IP address in RIP updates that it sends.
- No enables advertising.

The DSLPipe advertises the IP address in RIP updates that it sends.

No is the default.

Dependencies: Keep this additional information in mind:

- The Private parameter does not apply (Private=N/A) if the DSLPipe does not support IP (Route IP=No).

Parameter Location: Connection Profile, Connections/IP options
Static Rtes Profile, Static Rtes

See Also: LAN Adrs, Metric, RIP, Route IP

Profile Reqd

Description: This parameter specifies whether the DSLPipe rejects incoming calls for which it could find no Connection Profile and no entry on a remote authentication server.

Usage: Press Enter to toggle between Yes and No.

- Yes specifies that the DSLPipe rejects incoming calls for which it can find no Connection Profile and no entry on a remote authentication server.
- No specifies that the DSLPipe does not require a Connection Profile or a remote authentication entry.

  No is the default.

You can satisfy the Profile Reqd parameter in one of these ways:

- The source IP address of the caller matches the LAN Adrs parameter in a local Connection Profile.

  In this case, Encaps=MPP or Encaps=PPP.
- The source name of the caller matches the Station parameter in a local Connection Profile.

  In this case, Encaps=PPP or Encaps=MPP, and Recv Auth=PAP or Recv Auth=CHAP.
- The source MAC address of the caller matches the Station parameter in a local Connection Profile.

Dependencies: If you get incoming PPP bridging calls (Route IP=No) and Profile Reqd=Yes, you must also specify that the DSLPipe authenticate incoming calls using PAP or CHAP (Recv Auth=PAP or Recv Auth=CHAP). A Connection Profile cannot match a PPP bridging call except through the name of the caller that PAP or CHAP authentication provides.

Parameter Location: Answer Profile, Answer

See Also: Encaps, Recv Auth, Route IP

Protocol

Description: In a filter of type IP, this parameter specifies the protocol number to which the DSLPipe compares a packet's protocol number.

Usage: Press Enter to open a text field. Then, type the number of the protocol. You can enter a number between 0 and 255. The default setting is 0 (zero). When you accept the default, the DSLPipe disregards the Protocol parameter when applying the filter.

Protocols and their associated numbers appear in Table 1-2.

Table 1-2. Protocols

Number	Name
1	ICMP (Internet Control Message Protocol)
2	IGMP (Internet Group Management Protocol)
3	GGP (Gateway-to-Gateway Protocol)
4	IP (Internet Protocol)
5	ST (Stream)
6	TCP (Transmission Control Protocol)
7	UCL
8	EGP (Exterior Gateway Protocol)

Table 1-2. Protocols

Number	Name
9	Any private interior gateway protocol
10	BBN-RCC-MON (BBN RCC Monitoring)
11	NVP-II (Network Voice Protocol II)
12	PUP
13	ARGUS
14	EMCOM
15	XNET (Cross-Net Debugger)
16	CHAOS
17	UDP (User Datagram Protocol)
18	MUX (Multiplexing)
19	DCN-MEAS (DCN Measurement Subsystems)
20	HMP (Host Monitoring Protocol)
21	PRM (Packet Radio Measurement)
22	XNS IDP (Xerox Networking System Internetwork Datagram Protocol)
23	TRUNK-1
24	TRUNK-2
25	LEAF-1
26	LEAF-2
27	RDP (Reliable Data Protocol)

Table 1-2. Protocols

Number	Name
28	IRTP (Internet Reliable Transport Protocol)
29	ISO-TP4 (International Standards Organization Transport Protocol Class 4)
30	NETBLT (Bulk Data Transfer Protocol)
31	MFE-NSP (MFE Network Services Protocol)
32	MERIT-INP (MERIT Internodal Protocol)
33	SEP (Sequential Exchange Protocol)
34	3PC (Third Party Connect Protocol)
35	IDPR (Inter-Domain Policy Routing Protocol)
36	XTP
37	DDP (Datagram Delivery Protocol)
38	IDPR-CMTP (IDPR Control Message Transport Protocol)
39	TP++ (TP++ Transport Protocol)
40	IL (IL Transport Protocol)
41	SIP (Simple Internet Protocol)
42	SDRP (Source Demand Routing Protocol)
43	SIP-SR (SIP Source Route)
44	SIP-FRAG (SIP Fragment)
45	IDRP (Inter-Domain Routing Protocol)
46	RSVP (Reservation Protocol)

Table 1-2. Protocols

Number	Name
47	GRE (General Routing Encapsulation)
48	MHRP (Mobile Host Routing Protocol)
49	BNA
50	SIPP-ESP (SIPP Encap Security Payload)
51	SIPP-AH (SIPP Authentication Header)
52	I-NLSP (Integrated Net Layer Security Protocol)
53	SWIPE (IP with Encryption)
54	NHRP (Next Hop Resolution Protocol)
55-60	Unassigned
61	Any Host Internet Protocol
62	CFTP
63	Any local network
64	SAT-EXPAK (SATNET and Backroom EXPAK)
65	KRYPTOLAN
66	RVD (MIT Remote Virtual Disk Protocol)
67	IPPC (Internet Pluribus Packet Core)
68	Any distributed file system
69	SAT-MON (SATNET Monitoring)
70	VISA (VISA Protocol)

Table 1-2. Protocols

Number	Name
71	IPCU (Internet Packet Core Utility)
72	CPNX (Computer Protocol Network Executive)
73	CPHB (Computer Protocol Heart Beat)
74	WSN (Wang Span Network)
75	PVP (Packet Video Protocol)
76	BR-SAT-MON (Backroom SATNET Monitoring)
77	SUN-ND PROTOCOL-Temporary
78	WB-MON (WIDEBAND Monitoring)
79	WB-EXPAK (WIDEBAND EXPAK)
80	ISO-IP (International Standards Organization Internet Protocol)
81	VMTP
82	SECURE-VMTP
83	VINES
84	TTP
85	NSFNET-IGP (National Science Foundation Network Interior Gateway Protocol)
86	DGP (Dissimilar Gateway Protocol)
87	TCF
88	IGRP
89	OSPF (Open Shortest Path First)

Table 1-2. Protocols

Number	Name
90	Sprite-RPC
91	LARP (Locus Address Resolution Protocol)
92	MTP (Multicast Transport Protocol)
93	AX.25 (AX.25 Frames)
94	IPIP (IP-within-IP Encapsulation Protocol)
95	MICP (Mobile Internetworking Control Protocol)
96	SCC-IP (Semaphore Communications Security Protocol)
97	ETHERIP (Ethernet-within-IP Encapsulation)
98	ENCAP (Encapsulation Header)
99	Any private encryption scheme
100	GMTP
101-254	Unassigned
255	Reserved

Dependencies: The Protocol parameter applies only if the filter is of type IP (Type=IP) and is activated (Valid=Yes).

Parameter Location: Filter Profile, Filter/IP

See Also: Type, Valid

Proxy Mode

Description: This parameter specifies under what conditions the DSLPipe performs a proxy ARP (Address Resolution Protocol). The DSLPipe performs a

proxy ARP when it recognizes the IP address of a remote device in an ARP request, and then responds to the ARP request by sending its own MAC address.

Usage: Press Enter to cycle through the choices.

- Always specifies that the DSLPipe responds to an ARP request regardless of whether a connection to the remote site is up.
- Inactive specifies that the DSLPipe responds to an ARP request only for a remote IP address specified in a Connection Profile, and only if there is no connection to the remote site.
- Active specifies that the DSLPipe responds to an ARP request only if a connection to the remote site is up, regardless of whether a Connection Profile exists for the link.
- Off disables proxy mode.
  Off is the default.

Dependencies: Keep this additional information in mind:

- The Proxy Mode parameter does not apply (Proxy Mode=N/A) if the v does not support IP (Route IP=No).
- Enabling Proxy Mode may prevent the DSLPipe from placing calls simply for address lookups.

Parameter Location: Ethernet Profile, Mod Config/Ether options

See Also: Net Adrs, Route IP

R/W Comm

Description: This parameter specifies a read/write SNMP community name. If an SNMP manager sends this community name, it can access the Get, Get-Next, and Set SNMP agents.

SNMP (Simple Network Management Protocol) provides a way for computers to share networking information. In SNMP, two types of communicating devices exist: agents and managers. An agent provides networking information to a manager application running on another computer. The agents and managers share a database of information, called the Management Information Base (MIB).

SNMP security is implemented with the community name sent with each request. Ascend supports two community names: one with read-only access to the MIB (the Read Comm parameter), and the other with read/write access to the MIB (the R/W Comm parameter).

Usage: Press Enter to open a text field. Then, type the community name that the DSLPipe will use for authenticating the SNMP management station. You can enter letters and numbers, up to a limit of 16 characters. The default is Write.

Parameter Location: Ethernet Profile, Mod Config/SNMP options

See Also: Read Comm

Read Comm

Description: This parameter specifies a read-only SNMP community name. If an SNMP manager sends this community name, it can access the Get and Get-Next SNMP agents.

SNMP (Simple Network Management Protocol) provides a way for computers to share networking information. In SNMP, two types of communicating devices exist: agents and managers. An agent provides networking information to a manager application running on another computer. The agents and managers share a database of information, called the Management Information Base (MIB).

SNMP security is implemented with the community name sent with each request. Ascend supports two community names: one with read-only access to the MIB (the Read Comm parameter), and the other with read/write access to the MIB (the R/W Comm parameter).

Usage: Press Enter to open a text field. Then, type the community name that the DSLPipe uses for authenticating the SNMP management station. You can enter up to 16 alphanumeric characters. The default is Public.

Parameter Location: Ethernet Profile, Mod Config/SNMP options

See Also: R/W Comm

Recv Auth

Description: This parameter specifies the authentication protocol that the DSLPipe uses when receiving and verifying a password for an incoming PPP call.

Usage: Press Enter to cycle through the choices.

- None specifies that the DSLPipe does not use an authentication protocol to validate incoming calls.

  None is the default.

- PAP (Password Authentication Protocol) is a PPP authentication protocol.

  PAP provides a simple method for a host to establish its identity in a two-way handshake. Authentication takes place only upon initial link establishment, and does not use encryption.

  If you choose PAP, the DSLPipe uses this protocol for authentication. The remote device must support PAP.

- CHAP (Challenge Handshake Authentication Protocol) is a PPP authentication protocol.

  CHAP is more secure than PAP. CHAP provides a way to periodically verify the identity of a host using a three-way handshake and encryption. Authentication takes place upon initial link establishment; the DSLPipe can repeat the authentication process any time after the connection is made.

  If you choose CHAP, the DSLPipe uses this protocol for authentication. The remote device must support CHAP.

- Either specifies that the DSLPipe can use either PAP or CHAP.

  When you select Either, the DSLPipe first requests authentication using CHAP, the more secure protocol. If the dial-in call rejects the request (or doesn't acknowledge it), the DSLPipe then requests PAP authentication. If the dial-in call rejects the PAP request, the DSLPipe terminates the link and drops the call.

Dependencies: Keep this additional information in mind:

- The link must use PPP or MPP encapsulation (Encaps=PPP or Encaps=MPP).
- If you choose PAP or CHAP, you must also specify a password using Recv PW in a Connection Profile, or Auth Host on an authentication server.

- When you set Recv Auth=PAP, CHAP, or Either, the DSLPipe can determine the IP address of a caller, even if the caller does not specify an address; the DSLPipe derives the IP address from the Connection Profile.

Parameter Location: Answer Profile, Answer/PPP options

See Also: Recv PW, Send Auth, Send PW

Recv PW

Description: This parameter specifies the password that the remote end of the link must send; if the password specified by Recv PW does not match the remote end's value for Send PW, the DSLPipe disconnects the link.

Usage: Press Enter to open a text field. Then, type a password. You can enter up to 20 characters; the password is case sensitive. The default is null. Press Enter again to close the text field.

Dependencies: Keep this additional information in mind concerning the Recv PW parameter in the Connection Profile:

- If Recv Auth=None, the Recv PW parameter does not apply (Recv PW=N/A).
- You must specify a value for Recv PW when the link uses PPP encapsulation (Encaps=PPP or Encaps=MPP) and the DSLPipe uses either PAP or CHAP authentication (Recv Auth=PAP or Recv Auth=CHAP).

  When you choose Encaps=MPP, both the dialing side and the answering side of the link must support MP+. If only one side supports MP+, the connection uses MP or standard single-channel PPP. When you choose Encaps=PPP, the connection uses only PPP.

Parameter Location: Connection Profile: Ethernet→Connections→Any Connection Profile→Encaps Options

See Also: Encaps, Password Reqd, Recv Auth, Send Auth, Send PW

Rem Addr

See "LAN Adrs" on page 1-69.

Rem Name

See "Station" on page 1-131.

Remote Mgmt

Description: This parameter specifies whether the device at the remote end of an AIM call can operate the DSLPipe remotely using the DO Beg/End Rem Mgm command. In remote management, the DSLPipe uses bandwidth between sites over the management subchannel established by the MPP protocol.

Usage: Press Enter to toggle between Yes and No.

- Yes specifies that the remote device can remotely operate the DSLPipe. Yes is the default.
- No specifies that the remote device cannot remotely operate the DSLPipe. If the remote device tries to do so, the error message Remote Management Denied appears.

Dependencies: The Call Type parameter must be set to MPP or Nailed/MPP.

Parameter Location: System Profile, Sys Config

See Also: Call Type and DO Beg/End Rem Mgm in the DSLPipe *Reference Guide.*

Renewal Time

Description: This parameter specifies the lease time, in seconds, for the address defined in the Spoof Adr parameter. The default is 10 seconds. This value represents the amount of time the address will be assigned to the requesting client. After the specified number of seconds, the client must attempt to secure the IP address again. If an authenticated dial-up session is active, the DSLPipe refuses the request, forcing the client to obtain its real IP address from the DHCP server on the remote network.

Usage: Press Enter to open a text field, and then type a number between 3 and 65535 (default 10). Press Enter again to close the text field.

Example: 60

Parameter Location: Ethernet Profile, Mod Config/DHCP Spoofing...

Dependencies: The DHCP Spoofing and Spoof Adr parameters must be configured for this feature to work.

See Also: DHCP Spoofing, Spoof Adr

Restore Cfg

Description: This command restores profiles saved using the Save Cfg parameter, or transfers the profiles to another DSLPipe. Because the Save Cfg command does not save passwords, the Restore Cfg command does not restore them.

Usage: Follow these instructions to restore your configuration from backup:

1 Enable the Upload parameter in the Security Profile (Upload=Yes).

2 Verify that your terminal emulation program has a disk capture feature; this feature enables your emulator to capture to disk the ASCII characters it receives at its serial host port.

3 Verify that your terminal emulation program has an autotype feature; this feature enables your emulator to transmit over its serial host port the contents of a file it has built through disk capture.

4 Connect the backup device to the DSLPipe Control port.

5 Set the data rate of your terminal emulation program to 9600 baud or lower.

6 Set the Term Rate parameter in the System Profile to 9600.

7 Make certain that you have the Edit Security privilege; if you restore without having the Edit Security privilege, you can be locked out of some or all operations.

8 Select Restore Cfg from the Sys Diag menu.

9 When the `Waiting for upload data` prompt appears, turn on the autotype function on your emulator and supply the filename of the saved DSLPipe data.

10 Verify that the configuration data is going to your terminal emulation screen and is being restored to the target DSLPipe.

The restore process is complete when the message `Upload complete--type any key to return to menu` appears on your emulator's display.

Parameter Location: Sys Diag

See Also: Save Cfg

RIP

Description: This parameter specifies whether the DSLPipe send and/or receives RIP-v1 (version 1) or RIP-v2 (version 2) packets on the selected interface.

The RIP parameter appears in the Answer Profile, Connection Profiles, and the Ethernet Profile. Its functionality differs depending on the profile:

- In the Answer Profile or a Connection Profile, the RIP parameter controls RIP updates between the DSLPipe and a remote router.
- In the Ethernet Profile, the RIP parameter controls RIP updates between the DSLPipe and other IP routers on the local Ethernet network.

The most significant difference between RIP (Routing Information Protocol) versions 1 and 2 is that RIP-v2 allows neighboring hosts to communicate netmasks to each other. RIP-v1 forces routers to guess the netmask.

If the DSLPipe is communicating with other RIP-v2 routers and hosts, all routing tables contain the same addresses and routes. However, if the DSLPipe is communicating with a RIP-v1 router, that router ignores the netmask field in the RIP-v2 packet, making use only of the IP address without the netmask. For this reason, we do not recommend that you run RIP-v1 and RIP-v2 on the same network in such a way that both RIP-v1 and RIP-v2 hosts hear each other's advertisements.

Note: Ascend recommends that all routers and hosts run RIP-v2 instead of RIP-v1. The IETF has voted to move RIP version 1 into the "historic" category and its use is no longer recommended.

Usage: Press Enter to cycle through the choices.

- Off specifies that the DSLPipe does not transmit or receive RIP updates.

Off is the default.

- Recv-v1

  This setting specifies that the DSLPipe receives RIP-v1 updates, but does not transmit RIP updates on this interface (WAN or Ethernet).

- Send-v1

  This setting specifies that the DSLPipe transmits RIP-v1 updates, but does not receive RIP updates on this interface (WAN or Ethernet).

- Both-v1

  This setting means that the DSLPipe transmits and receives RIP-v1 updates on this interface (WAN or Ethernet).

- Send-v2

  This setting specifies that the DSLPipe transmits RIP-v2 updates, but does not receive RIP updates on this interface (WAN or Ethernet).

- Recv-v2

  This setting specifies that the DSLPipe receives RIP-v2 updates, but does not transmit RIP updates on this interface (WAN or Ethernet).

- Both-v2

  This setting means that the DSLPipe transmits and receives RIP-v2 updates on this interface (WAN or Ethernet).

Dependencies: Keep this additional information in mind:

- The RIP parameter does not apply if the DSLPipe does not support IP (Route IP=No).
- RIP in the Answer Profile applies to incoming calls for which no Connection Profile exists; if a Connection Profile exists, the setting of its RIP parameter takes precedence.
- If Profile Reqd=Yes in the Answer Profile, RIP does not apply (RIP=N/A) in the Answer Profile.

Parameter Location: Answer Profile: Ethernet→Answer→Session Options
Connection Profile: Ethernet→Connections→Any Connection Profile→IP Options
Ethernet Profile: Ethernet→ Mod Config→Ether Options

See Also: Route IP

RIP Policy

Description: This parameter determines whether the DSLPipe uses split horizon or poison reverse to handle RIP broadcasts over an interface that includes routes received from that interface. In either case, the DSLPipe keeps track of where it received RIP updates

Note: RIP Policy only applies to RIP version 1.

Usage: Press Enter to cycle through the choices.

- Split Hrzn specifies the split horizon policy.

  The DSLPipe does not propagate routes back to the subnet from which they were received.
- Poison Rvrs selects the poison reverse policy.

  The DSLPipe propagates routes back to the subnet from which they were received, but with a metric of 16.

  Poison Rvrs is the default.

Parameter Location: Ethernet Profile, Mod Config

RIP Summary

Description: This parameter specifies whether the DSLPipe summarizes subnet information when advertising routes.

Note: RIP Summary only applies to RIP version 1.

Summarizing means that when the DSLPipe has a route to a subnet, it advertises a route to all the subnets in a network of the same class. For example, if the DSLPipe has a routing table entry to 200.5.8.13/28, it advertises a route to 200.5.8.0, because 200.5.8.13/28 is part of a class C network. When the DSLPipe does not summarize information, it advertises each route in its routing table "as-is;" in our example, the DSLPipe advertises a route only to 200.5.8.13.

RIP (Routing Information Protocol) is defined without consideration for subnetting; entries in a RIP packet do not include a subnet mask. Therefore, the recipient of such updates must know or assume information about subnet masks. To work around this standard RIP behavior, the DSLPipe includes the RIP

Summary parameter. You can set this parameter to specify that the DSLPipe modify RIP to advertise implied subnet information.

Usage: Press Enter to toggle between Yes and No.

- Yes specifies that the DSLPipe summarizes subnet information when advertising routes outside its own network, but does not summarize subnet information when advertising routes inside its own network.

  For example, suppose the DSLPipe has an IP address of 200.8.143.5/28 and advertises across the WAN to a router that has the address 200.8.143.31/28. Even though the DSLPipe and the recipient are on different subnets, they are on the same network; therefore, no summarization takes place. The routes are sent "as-is."

  Yes is the default.

- No specifies that the DSLPipe never summarizes subnet information.

  When you select No, the recipient must know the subnet mask to apply to each route.

Dependencies: Keep this additional information in mind:

- The RIP Summary parameter applies only to RIP version 1 and has no affect on RIP version 2 advertisements.
- RIP Summary does not affect host routes.

  Suppose the DSLPipe has a routing table entry to 200.8.143.5/32. Regardless of whether routes are summarized, this route is advertised as 200.8.143.5.

Parameter Location: Ethernet Profile: Ethernet →Mod Config

Route

Description: This parameter specifies what type of routing (if any) applies to the first Connection Profile as well as to the Answer Profile.

Usage: Press Enter to cycle through the choices.

- None sets your DSLPipe as a bridge (default).
- IP sets your DSLPipe as an IP router.
- IPX sets your DSLPipe as an IPX router.
- IP + IPX sets your DSLPipe as a router for both IP and IPX.

Parameter Location: Configure Profile

Dependencies: Keep this additional information in mind:

- The Route setting in the Configure Profile determines the value of the Route IP and Route IPX parameters in the first Connection Profile and in the Answer Profile.
- If IP routing is enabled, you must set appropriate options in the IP Options submenu. Both sides of the connection must have IP routing enabled, so each side can be managed as a separate IP network or subnetwork.
- If IPX routing is enabled, you must set the IPX Frame type as well as appropriate options in the IPX Options submenu. Both sides of the connection must have IPX routing enabled, so each side can be managed as a separate IPX network.
- If routing is disabled, bridging must be enabled.

See Also: Route IP, Route IPX

Route IP

Description: This parameter enables or disables the routing of IP data packets over the link specified in the profile.

Usage: Press Enter to toggle between Yes and No.

- Yes enables IP routing
  Yes is the default.
- No disables IP routing.

Dependencies: The effect of the Route IP parameter depends upon how you set the Bridge parameter:

- If Bridge=Yes and Route IP=Yes, the DSLPipe routes IP packets, and bridges all other packets.
- If Bridge=Yes and Route IP=No, the DSLPipe bridges all packets.
- If Bridge=No and Route IP=Yes, the DSLPipe routes only IP packets.
- If Bridge=No and Route IP=No, an error occurs and you cannot save the profile.
  You must enable bridging or routing, or both.

These additional dependencies apply:

- The Route parameter in the Configure Profile affects the Route IP value in the first Connection Profile. For example, if you set Route=IPX in the Configure Profile (that is, route *only* IPX), Route IP=No in the first Connection Profile.
- IP routing must be enabled on both the dialing and answering sides of the link.

  The Connection Profile on the dialing side and the Answer Profile on the answering side must both set the Route IP parameter to Yes. Otherwise, the DSLPipe does not route IP packets.
- Route IP in the Answer Profile applies to incoming calls for which no Connection Profile exists; if a Connection Profile exists, the setting of its Route IP parameter takes precedence.
- If Profile Reqd=Yes in the Answer Profile, Route IP does not apply (Route IP=N/A) in the Answer Profile.

Parameter Location: Answer Profile, Answer/PPP options
Connection Profile, Connections

See Also: Bridge, Encaps, Profile Reqd, Route, Route IPX

Route IPX

Description: This parameter specifies whether or not the DSLPipe requests IPX routing for the connection.

Usage: Press Enter to toggle between Yes and No.

- Yes specifies that the DSLPipe requests IPX routing.
- No specifies that the DSLPipe does not route IPX.

  No is the default.

Dependencies: If the link supports PPP or MP+ (Encaps=PPP or Encaps=MPP), both sides of the connection must set Route IPX=Yes for IPX routing to take place.

In addition, the effect of the Route IPX parameter depends upon how you set the Bridge parameter:

- If Bridge=Yes and Route IPX=Yes, the DSLPipe routes IPX packets, and bridges all other packets.
- If Bridge=Yes and Route IPX=No, the DSLPipe bridges all packets.
- If Bridge=No and Route IPX=Yes, the DSLPipe routes only IPX packets.
- If Bridge=No and Route IPX=No, an error occurs and you cannot save the profile.

  You must enable bridging or routing, or both.

This additional dependency applies:

- The Route parameter in the Configure Profile affects the Route IPX value in the first Connection Profile. For example, if you set Route=IP in the Configure Profile (that is, route *only* IP), Route IPX=No in the first Connection Profile.

Parameter Location: Answer Profile, Answer/PPP options
Connection Profile, Connections

See Also: Bridge, Route, Route IP

Save Cfg

Description: This command enables you to save all DSLPipe profiles (except Security Profiles) to disk.

The process does not save passwords; that is, the Save Cfg command does not save the Send PW and Recv PW parameters in a Connection Profile, or the Passwd parameter in a Security Profile or an Ethernet Profile.

Usage: Follow these instructions to save your configuration:

1 Enable the Download parameter in the Security Profile (Download=Yes).

2 Verify that your terminal emulation program has a disk capture feature; this feature enables your emulator to capture to disk the ASCII characters it receives at its serial host port.

3 Verify that your terminal emulation program has an autotype feature; this feature enables your emulator to transmit over its serial host port the contents of a file it has built through disk capture.

4 Connect the backup device to the DSLPipe Control port.

5 Set the data rate of your terminal emulation program to 9600 baud or lower.

6 Set the Term Rate parameter in the System Profile to 9600.

7 Select Save Cfg from the Sys Diag menu.

8 Turn on the autotype function on your emulator, and start the save process by typing any key on the emulator.

9 Verify that configuration data is being echoed to the terminal emulation screen and that the captured data is being written to a file on your disk.

The save process is complete when the message `Download complete--type any key to return to menu` appears on your emulator's display. The backup file is an ASCII file.

10 Turn off the autotype feature.

Parameter Location: Sys Diag

See Also: Restore Cfg

Sec DNS

Description: This parameter specifies the IP address of the secondary domain name server.

Domain Name System (DNS) is a TCP/IP service that enables you to specify a symbolic name instead of an IP address. A symbolic name consists of a username and a domain name in the format *username@domain name*. The *username* corresponds to the host number in the IP address. The *domain name* corresponds to the network number in the IP address. A symbolic name might be steve@abc.com or joanne@xyz.edu.

DNS maintains a database of network numbers and corresponding domain names on a domain name server. When you use a symbolic name, DNS translates the domain name into an IP address, and sends it over the network. When the Internet service provider receives the message, it uses its own database to look up the username corresponding to the host number.

Usage: Press Enter to open a text field. Then, type the IP address of the secondary domain name server.

The address consists of four numbers between 0 and 255, separated by periods. The default value is 0.0.0.0. Accept this default if you do not have a secondary domain name server.

Press Enter again to close the text field.

Example: `200.207.23.1`

Dependencies: The Sec DNS parameter applies only to Telnet connections running under the DSLPipe terminal server interface.

A terminal server is a computing device to which a terminal can connect over a LAN or WAN link. The DSLPipe supports all the common capabilities of standard terminal servers, including Telnet, Domain Name Services (DNS), login and password control, call detail reporting, and authentication services.

Telnet is a protocol used to link two computers in order to provide a terminal with a connection to the remote machine. The remote machine is known as the Telnet host. When you start a Telnet session, you connect to the Telnet host and log in. The connection enables you to work with the remote machine as though you were at a terminal connected to it.

Parameter Location: Ethernet Profile, Mod Config/DNS

See Also: Domain Name, Pri DNS

Sec History

Description: This parameter specifies the number of seconds the DSLPipe uses as a sample for calculating average line utilization (ALU) of transmitted data; the DSLPipe arrives at this average using the algorithm specified by the Dyn Alg parameter.

When ALU exceeds the Target Util threshold for a period of time greater than the value of the Add Pers parameter, the DSLPipe attempts to add a channel.When ALU falls below the Target Util threshold for a period of time greater than the value of the Sub Pers parameter, the DSLPipe attempts to remove a channel.

The number of seconds you choose for the Sec History parameter depends on your device's traffic patterns. For example, if you want to average spikes with

normal traffic flow, you may want the DSLPipe to establish a longer historical time period. If, on the other hand, traffic patterns consist of many spikes that are short in duration, you may want to specify a shorter period of time; doing so assigns less weight to the short spikes.

Usage: Press Enter to open a text field. Then, type a number between 1 and 300. The default value for MP+ calls is 15 seconds; the default value for dynamic AIM calls is 30 seconds. Press Enter again to close the text field.

Dependencies: Keep this additional information in mind:

- The Sec History parameter applies only to dynamic MP+ calls (Encaps=MPP).
- If you specify a small value for the Sec History parameter, and increase the values of the Add Pers parameter and the Sub Pers parameter relative to the value of Sec History, the system becomes less responsive to quick spikes.
- The easiest way to determine the proper values for Sec History, Add Pers, and Sub Pers is to observe usage patterns; if the system is not responsive enough, the value of Sec History is too high.

Parameter Location: Answer Profile, Answer/PPP options
Connection Profile, Connections/Encaps options

See Also: Add Pers, Dyn Alg, Encaps, Sub Pers, Target Util

Secondary

Description: This parameter specifies a secondary Connection Profile to be dialed in the event that a session using the primary Connection Profile cannot be established.

Usage: Press Enter to open a text field. Then, type the name of the secondary Connection Profile. The name you specify must match the value of the Name parameter in a local Connection Profile.

Dependencies: Keep this additional information in mind:

- Secondary Profiles cannot be chained. That is, secondary Connection Profiles cannot also have Secondary Connection profiles.

- Do not confuse the Secondary parameter with the Backup parameter. A BackUp Connection Profile is used to re-establish an existing connection that has terminated; a Secondary Connection Profile is used to establish a new connection if the primary Connection Profile cannot.
- Parameters that you define in the primary Connection Profile do not automatically apply to the secondary Connection Profile.

  For example, if you set the primary Connection Profile to filter Telnet packets, you must set the secondary profile to filter Telnet packets as well.
- Outgoing Frame Relay packets are the only packets that follow the primary Connection Profile definitions. All other packets follow the backup Connection Profile definitions.

Parameter Location: Ethernet Profile, Connections\Session options...

See Also: Backup

Security

Description: This parameter specifies whether the DSLPipe enables trapping of particular system events.

SNMP (Simple Network Management Protocol) provides a way for computers to share networking information. In SNMP, two types of communicating devices exist: agents and managers. An agent (such as the DSLPipe) provides networking information to a manager application running on another computer. The agents and managers share a database of information, called the Management Information Base (MIB).

A trap is a mechanism in SNMP for reporting system change in real time. To report system change, the DSLPipe sends a traps-PDU across the Ethernet interface to the SNMP manager. A complete list specifying the events that cause the DSLPipe to send a traps-PDU appears in the Ascend Enterprise Traps MIB.

Usage: The Security parameter in this profile enables you to specify whether the DSLPipe traps these events:

- authenticationFailure

  This event occurs when authentication has failed. See RFC-1215 for a full explanation of this event.

- consoleStateChange
  This event occurs when a VT100 or Telnet port changes its state.

Press Enter to toggle between Yes and No.

- Yes specifies that the DSLPipe traps the events.
- No specifies that the DSLPipe does not trap the events.
  No is the default.

Parameter Location: SNMP Traps Profile, SNMP Traps

See Also: Comm, Dest

Send Auth

Description: This parameter specifies the authentication protocol that the DSLPipe requests when initiating a connection using PPP or MP+ encapsulation. The answering side of the connection determines which authentication protocol, if any, the connection uses.

Usage: Press Enter to cycle through the choices.

- None specifies that the DSLPipe does not request an authentication protocol for outgoing calls.
  None is the default.
- PAP (Password Authentication Protocol) is a PPP authentication protocol.
  PAP provides a simple method for the DSLPipe to establish its identity in a two-way handshake. Authentication takes place only upon initial link establishment, and does not use encryption.
  If you choose PAP, the DSLPipe requests this protocol for authentication. The remote device must support PAP.
  Note that if you choose this setting, the DSLPipe requests PAP authentication but will use CHAP authentication if the called unit requires CHAP. Choose this setting for non-token card authentication if you would allow sending your password unencrypted.
- CHAP (Challenge Handshake Authentication Protocol) is a PPP authentication protocol. If you choose CHAP, the DSLPipe requests this protocol for authentication. The remote device must support CHAP.

CHAP is more secure than PAP. CHAP provides a way for the remote device to periodically verify the identity of the DSLPipe using a three-way handshake and encryption. Authentication takes place upon initial link establishment; a device can repeat the authentication process any time after the connection is made.

Note that if you choose this setting, the DSLPipe will not bring up the connection using PAP. Choose this setting for non-token card authentication if you do not wish to send your password unencrypted; that is, if you do not wish to be authenticated through PAP.

- PAP-TOKEN is an extension of PAP authentication. This requires the following:
  - the Network Access Server (NAS) must be running the Ascend RADIUS daemon
  - there is a RADIUS profile that matches the caller's name
  - the RADIUS profile accesses an ACE or SAFEWORD authentication server

  In PAP-TOKEN, the user making outgoing calls from the DSLPipe authenticates his or her identity by entering a password derived from a hardware device, such as a hand-held security card. The DSLPipe prompts the user for this password, possibly along with a challenge key. The NAS obtains the challenge key from a security server that it accesses through RADIUS.

  RADIUS (Remote Authentication Dial In User Service) is a protocol by which users can have access to secure networks through a centrally managed server. You can store virtually all Connection Profile information on the RADIUS server in a flat ASCII database.
- PAP-TOKEN-CHAP is nearly identical to PAP-TOKEN. This requires the following:
  - the NAS be running the Ascend RADIUS daemon
  - there is a RADIUS profile that matches the caller's name
  - the RADIUS profile accesses an ACE or SAFEWORD authentication server
  - the user profile must specify an auxiliary password (Ascend-Receive-Secret) that matches the Aux Send PW parameter in the Connection Profile.

Note that if Aux Send PW and Ascend-Receive-Secret do not match, it does not prevent the initial connection from succeeding, but the DSLPipe cannot extend an MP+ call beyond a single channel.

In all authentication protocols, including PAP-TOKEN and PAP-TOKEN-CHAP, the DSLPipe individually authenticates all channels of an MP+ call. If the answering unit requires security card authentication, PAP-TOKEN and PAP-TOKEN-CHAP begin identically when authenticating the first channel of an MP+ call. However, when the DSLPipe adds additional channels to the MP+ call, PAP-TOKEN requires security-card authentication for each new channel, while PAP-TOKEN-CHAP uses CHAP authentication for all new channels. CHAP authentication works automatically, without the use of a hand-held security card.

- CACHE-TOKEN begins authentication using a hand-held security card, and fills a token cache set up for you on the RADIUS server at the remote site. This requires the following:
  - the NAS must be running the Ascend RADIUS daemon
  - there is a RADIUS user profile that matches the caller's name
  - the RADIUS user profile accesses an ACE or SAFEWORD authentication server
  - the RADIUS user profile must specify an auxiliary password (Ascend-Receive-Secret) which matches the Send PW parameter in the Connection Profile and defines Ascend-Token-Expiry in its first line.

    Note that if Send PW and Ascend-Receive-Secret do not match, it does not prevent the initial connection from succeeding, but subsequent connections (specifically, disconnecting/reconnecting or adding channels) fail until the cached token expires.

  CHAP authenticates your subsequent calls without using your hand-held security card. After a period of time configured in your entry in the RADIUS users file, the token cache expires and the next call you place must again be authenticated using your hand-held security card.

Dependencies: Keep this additional information in mind:

- The link must use PPP or MP+ encapsulation (Encaps=PPP or Encaps=MPP).
- If you request PAP or CHAP, you must also specify a password using Send PW in a Connection Profile.

- On a nailed-up link (Call Type=Nailed), you must set Recv Auth and Send Auth to the same value at both ends of the connection; that is, Recv Auth at the local and remote ends, and Send Auth at the local and remote ends, must all contain the same value.
- PAP-TOKEN and PAP-TOKEN-CHAP require configuration of a SAFEWORD or ACE entry in the NAS's RADIUS users file with the caller's name.
- For information on prompting the user for his or her password at the DSLPipe terminal server, see the description of the `set password` command in the *DSLPipe User's Guide*.
- For information on prompting for a password at a host, see the APP Server, APP Host, and APP Port parameters.
- Dial Brdcast must be enabled when a PC on the same Ethernet as the DSLPipe runs APPSRVR1 or APPSRVR2 to open a connection protected by security-card authentication.

Parameter Location: Connection Profile, Connection/Encaps options

See Also: APP Host, APP Port, APP Server, Call Type, Dial Brdcast, Encaps, Recv Auth, Recv PW, Send PW

Send PW

Description: This parameter specifies the password that the DSLPipe sends to the remote end of a connection on outgoing calls. If the password specified by Send PW does not match the remote end's value for Recv PW, the remote end disconnects the link.

Usage: Press Enter to open a text field. Then, type the password that the remote end requires the DSLPipe to send.

You can enter up to 20 characters; the password is case sensitive. Leave the field blank if the remote end does not require a password.

Press Enter again to close the text field.

Dependencies: Keep this additional information in mind:

- You must specify a value for Send PW when the link uses PPP encapsulation (Encaps=PPP or Encaps=MPP) and the DSLPipe uses PAP, CHAP, or

CACHE-TOKEN authentication (Send Auth=PAP, Send Auth=CHAP, or Send Auth=CACHE-TOKEN).

When you choose Encaps=MPP, both the dialing side and the answering side of the link must support MP+. If only one side supports MP+, the connection uses MP or standard single-channel PPP. When you choose Encaps=PPP, the connection uses only PPP.

Parameter Location: Connection Profile, Connection/Encaps options

See Also: Encaps, Recv Auth, Recv PW, Send Auth

Server Name

Description: This parameter appears in an IPX Routes Profile and an IPX SAP Filter Profile. Its functionality differs depending on the profile.

- In an IPX Routes Profile, the Server Name parameter specifies the name of an IPX server.
- In an IPX SAP Filters Profile, the Server Name parameter specifies the name of a NetWare server to be excluded from or included in the Ascend unit's service table.

Usage: You usage differs depending on the profile.

IPX Routes Profile

Press Enter to open a text field. Then, type the name of an IPX server. You can enter up to 48 characters, and you must limit your specification to uppercase letters, numbers, and the underscore symbol. Press Enter again to close the text field.

IPX SAP Filter Profile

Press Enter to open a text field. Then, type the server's name. You can specify letters, digits, and the underscore, up to a maximum of 20 characters. The wildcard characters * and ? may be used for partial name matches. Press Enter again to close the text field.

Dependencies: For the Server Name parameter to apply in an IPX Route Profile, you must enable IPX routing in the Connection Profile by setting Route IPX=Yes.

Parameter Location: IPX Routes Profile, IPX Routes
IPX SAP Filter Profile, IPX SAP Filters

See Also: Route IPX, Server Type

Server Type

Description: This parameter appears in an IPX Route Profile and an IPX SAP Filter Profile. Its functionality differs depending on the profile:

- In an IPX Route Profile, the Server Type parameter specifies the SAP (Service Advertising Protocol) service type for the server.
- In an IPX SAP Filters Profile, the Server Type parameter specifies the SAP Service Type that will be excluded from or included in the service table.

Usage: Your usage differs depending on the profile.

IPX Route Profile

Press Enter to open a text field. Then, type a valid SAP service type for the server. The SAP service type for a NetWare server is type 4. Press Enter again to close the text field.

For information on SAP service types, refer to your Novell NetWare documentation.

IPX SAP Filter Profile

Press Enter to open a text field. Then type a hexadecimal number. You can enter a number from 1 to FFFE. The default value is 0. Press Enter again to close the text field.

Parameter Location: IPX Route Profile, IPX Routes
IPX SAP Filter Profile, IPX SAP Filters

See Also: Server Name, Type, Valid

Shared Prof

Description: This parameter enables multiple incoming calls to share a local Connection Profile.

Usage: Press Enter to toggle between Yes and No.

- Yes specifies that multiple incoming calls can share a local Connection Profile.

  The DSLPipe must first authenticate the caller by using the Name and Recv PW parameters in the profile. If an incoming call has an IP address that conflicts with an existing caller IP address the DSLPipe rejects the call.
- No specifies that multiple incoming calls cannot share a local Connection Profile.

  No is the default.

Parameter Location: Ethernet Profile, Mod Config

See Also: Encaps, Name, Recv PW

Socket

Description: This parameter specifies the socket number of the NetWare server.

Usage: Press Enter to open a text field. Then, type the socket number for the server. You should advertise only those NetWare servers that have well-known socket numbers. Press Enter again to close the text field.

Example: `DE040600`

Dependencies: For the Socket parameter to apply, you must enable IPX routing in the Connection Profile by setting Route IPX=Yes.

Parameter Location: IPX Routes Profile, IPX Routes

See Also: Route IPX

Spoof Adr

Description: This parameter specifies an IP address and netmask that will be assigned to the DHCP client when spoofing takes place. It must be a valid IP address on the local network.

Usage: Press Enter to open a text field, and then type a valid IP address and netmask. Press Enter again to close the text field.

Example: 188.0.5.8/24

Parameter Location: Ethernet Profile, Mod Config/DHCP Spoofing...

Dependencies: The DHCP Spoofing and Renewal Time parameters must be configured for this feature to work.

See Also: DHCP Spoofing, Renewal Time

Src Adrs

Description: In a filter of type IP, this parameter specifies the source address to which the DSLPipe compares a packet's source address.

Usage: Press Enter to open a text field. Then, type the source address the DSLPipe should use for comparison when filtering a packet. The address consists of four numbers between 0 and 255, separated by periods.

The null address 0.0.0.0 is the default; this setting matches all packets.

Press Enter to close the text field.

Example: `200.62.201.56`

Dependencies: Src Adrs does not apply (Src Adrs=N/A) if you are using a generic filter (Type=Generic) or if you have not activated the IP filter (Valid=No).

Parameter Location: Filter Profile, Filters/IP

See Also: Src Mask

Src Mask

Description: In a filter of type IP, this parameter specifies the bits that the DSLPipe should mask when comparing a packet's source address to the value of the Src Adrs parameter. The masked part of an address is hidden; the DSLPipe does not use it for comparisons with Src Adrs. A mask hides the part of a number that appears behind each binary 0 (zero) in the mask; the DSLPipe uses only the part of a number that appears behind each binary 1 for comparison.

The DSLPipe applies the mask to the address using a logical AND after the mask and address are both translated into binary format.

Usage: Press Enter to open a text field. Then, type the IP mask in dotted decimal format. The value 0 (zero) hides all bits, because the decimal value 0 is the binary value 00000000; the value 255 does not mask any bits, because the decimal value 255 is the binary value 11111111.

The null address 0.0.0.0 is the default; this setting indicates that the DSLPipe masks all bits. To specify a single source address, set Src Mask=255.255.255.255 and set Src Adrs to the IP address that the DSLPipe uses for comparison.

Press Enter to close the text field.

Example: Suppose a packet has the source address 10.2.1.1. If Src Adrs=10.2.1.3 and Dst Mask=255.255.255.0, the DSLPipe masks the last digit and uses only 10.2.1, which matches the packet.

Dependencies: Src Mask does not apply (Src Mask=N/A) if you are using a generic filter (Type=Generic) or if you have not activated the IP filter (Valid=No).

Parameter Location: Filter Profile, Filters/IP

See Also: Src Adrs

Src Port #

Description: In a filter of type IP, this parameter specifies the source port number to which the DSLPipe compares the packet's source port number.

The Src Port Cmp criterion determines how the DSLPipe carries out the comparison.

Usage: Press Enter to open a text field. Then, type the number of the source port the DSLPipe should use for comparison when filtering packets. You can enter a number between 0 and 65535.

The default setting is 0 (zero); this setting means that the DSLPipe forwards all packets.

Press Enter to close the text field.

Example: 25

Port 25 is reserved for SMTP, so that socket is dedicated to receiving mail messages. Port 20 is reserved for FTP data messages, Port 21 for FTP control sessions, and Port 23 for Telnet sessions.

Parameter Location: Filter Profile, Filters/IP

See Also: Dst Port #, Dst Port Cmp, Src Port Cmp

Src Port Cmp

Description: In a filter of type IP, this parameter specifies the type of comparison the DSLPipe makes when filtering for source port numbers using the Src Port # parameter.

Usage: Press Enter to cycle through the choices.

- None specifies that the DSLPipe does not compare the packet's source port number to the value specified by Src Port #.

  None is the default.
- Less specifies that port numbers with a value less than the value specified by Src Port # match the filter.

- Eql specifies that port numbers equal to the value specified by Src Port # match the filter.
- Gtr specifies that port numbers with a value greater than the value specified by Src Port # match the filter.
- Neq specifies that port numbers not equal to the value specified by Src Port # match the filter.

Dependencies: Keep this additional information in mind:

- This parameter works only for TCP and UDP packets.

  You must set Src Port Cmp=None if the Protocol parameter is not set to 6 (TCP) or 17 (UDP).
- Src Port Cmp does not apply (Src Port Cmp=N/A) if you are using a generic filter (Type=Generic) or if you have not activated the IP filter (Valid=No).

Parameter Location: Filter Profile, Filters/IP

See Also: Src Port #

Station

Description: This parameter specifies the name of the remote device to which the DSLPipe makes a connection.

Usage: Press Enter to open a text field. Then, type the name or MAC address of the remote device.

You can enter up to 31 characters.

The value you specify is case sensitive, and must exactly match the name of the remote device. If you are not sure about the exact name, contact the administrator of the remote network.

Press Enter again to close the text field.

Dependencies: Keep this additional information in mind:

- The Station parameter for the first Connection Profile is the same as Rem Name parameter in the Configure Profile.

- The Station parameter setting appears in the list of Connection Profiles in the Connection menu; however, if you leave the parameter blank, the LAN Adrs setting appears instead.
- The remote device that the Station parameter specifies is the device actually placing or answering the call; it is not necessarily the same as the source or destination of packets using the link.
- The DSLPipe does not currently use the Domain Name System (DNS) to determine the IP address of the device specified by the Station parameter.
- When the DSLPipe receives a PPP or MP+ call from an Ascend unit, it tries to match the caller's Name to the value of the Station parameter in some Connection Profile.

  If the DSLPipe finds a match and authentication is turned on, the DSLPipe then tries to match the caller's Send PW value to the Recv PW value in that same Connection Profile.

Parameter Location: Connection Profile, Connections

Sub-Adr

Description: This parameter determines how the DSLPipe treats incoming calls based on whether they convey an ISDN subaddress.

Usage: Press Enter to cycle through the options.

- Termsel specifies that the DSLPipe must use an ISDN subaddress to determine whether a call is answered.

  The called-party number must have a subaddres. Otherwise, the DSLPipe ignores the call. If the DSLPipe accepts the call, the subaddress becomes part of the incoming phone number.
- None specifies that the DSLPipe does not use subaddressing.

Dependencies: Keep this additional information in mind:

- Sub-Adr applies only to ISDN lines.
- Sub-Adr=TermSel is intended for a scenario in which equipment is connected to a multidrop ISDN BRI line.

Parameter Location: System Profile, Sys Config

See Also: Pri Num, Sec Number, Dial #

Sub Pers

Description: This parameter specifies the number of seconds average line utilization (ALU) of transmitted data must fall below the threshold indicated by the Target Util parameter before the DSLPipe begins removing bandwidth from a session. The DSLPipe determines the ALU for a session using the algorithm specified by the Dyn Alg parameter.

When utilization falls below the threshold for a period of time greater than the value of the Sub Pers parameter, the DSLPipe attempts to remove a channel. Using the Add Pers and Sub Pers parameters prevents the system from continually adding and subtracting bandwidth, and can slow down the process of allocating or removing bandwidth.

Usage: Press Enter to open a text field. Type a number between 1 and 300. Press Enter again to close the text field.

When the DSLPipe is using MP+ (Encaps=MPP), the default value is 10.

Dependencies: Keep this additional information in mind:

- One channel must be up at all times.
- Removing bandwidth cannot (a) cause the ALU to exceed the threshold specified by the Target Util parameter or (b) cause the number of channels to fall below the amount specified by the Min Ch Count parameter.
- Sub Pers in the Answer Profile applies to incoming calls for which no Connection Profile exists; if a Connection Profile exists, the setting of its Sub Pers parameter takes precedence.
- If Profile Reqd=Yes in the Answer Profile, Sub Pers does not apply (Sub Pers=N/A) in the Answer Profile.
- Add Pers and Sub Pers have little or no effect on a system with a high Sec History value.

  However, if the value of Sec History is low, the Add Pers and Sub Pers parameters provide an alternative way to ensure that spikes persist for a certain period of time before the system responds.

Parameter Location: Connection Profile, Connections/Encaps option
Answer Profile, Answer/PPP options

See Also: Add Pers, Dyn Alg, Min Ch Count, Sec History, Target Util

Switch Type

Description: This parameter specifies the network switch that provides the BRI line to the DSLPipe and connects the line to the WAN.

A switch is the device that connects the calling party to the answering party. The connection is a switched circuit consisting of one or more channels.

Usage: Press Enter to cycle through the choices. Your choices differ depending on the profile.

You can select one of the switch types listed in Table 1-3.

Table 1-3. Configure Profile switch types

Switch type	Explanation
AT&T/P-T-P	AT&T Point-to-Point is the default.
AT&T/Multi-P	ATT&T Mulitpoint.
NTI	Northern Telecommunications, Inc. Use this setting if your switch is DMS-100 Custom.
NI-1	National ISDN 1.
NI-2	National ISDN-2
U.K.	United Kingdom: ISDN-2 Hong Kong: HKT Switchline BRI Singapore: ST BRI Euro ISDN countries: Austria, Belgium, Denmark, Germany, Finland, Italy, Netherlands, Portugal, Spain, Sweden This is identical to NET 3.

Table 1-3. Configure Profile switch types

Switch type	Explanation
SWISS	Switzerland: Swiss Net 2
NET 3	This is identical to U.K.
GERMAN	Germany 1TR6 version: DBP Telecom
MP GERMAN	Germany: 1TR6 multipoint
FRANC	France: FT Numeris
DUTCH	Netherlands 1TR6 version: PTT Netherlands BRI
BELGIUM	Belgium: Pre-Euro ISDN Belgacom Aline
JAPAN	Japan: NTT INS-64
AUSTRALIA	Australia and New Zealand

Dependencies: Keep this additional information in mind:

- The Switch Type parameter does not apply to a link using inband signaling (Call Type=56K or 56KR) or consisting entirely of nailed-up channels (Call Type=Nailed).

  For inband signaling, a line uses 8 kbps of each 64-kbps channel for WAN synchronization and signaling. The remaining 56 kbps handle the transmission of user data.

  Switched-56 lines use inband signaling.
- All international switch types except German operate in multipoint mode.

Parameter Location: Configure Profile

Switch Usage

Description: This parameter enables or disables the serial WAN feature in the DSLPipe. If serial WAN is disabled or if the sliding switch on the back panel of the unit is in the Off position, the Control port of the DSLPipe is used only for

configuration purposes. If the switch is in the On position (away from the terminal port if the switch is horizontal or down if the switch is vertical) and serial WAN is enabled, all Connection Profiles are sampled once every 10 seconds. If a Connection Profile is configured for leased line operation and the Nailed Group parameter in that profile is set to 3, then the Control port is programmed for synchronous HDLC mode and an attempt is made to bring up the connection on that port.

Usage: Press Enter to cycle through the choices.

- Unused (default) means that the sliding switch on the back panel of the unit has no effect.
- Serial WAN means that the terminal port of the DSLPipe will be used as the serial WAN port when the sliding switch on the back panel is in the On position

Parameter Location: System, Sys Config

Dependencies: Keep this additional information in mind:

- The sliding switch on the back panel of the unit must be set to the On position for this parameter to take effect.

See Also: Activation, Group

Syslog

Description: This parameter specifies whether the DSLPipe sends warning, notice, and CDR (Call Detail Reporting) records from the system logs to the Syslog host.

CDR is a feature that provides a database of information about each call, including date, time, duration, called number, calling number, call direction, service type, and associated inverse multiplexing session and port. Because the network carrier bills for bandwidth on an as-used basis, and bills each connection in an inverse multiplexed call independently, you can use CDR to understand and manage bandwidth usage and the cost of each inverse multiplexed session.

The Syslog host is the station to which the DSLPipe sends system logs.

Usage: Press Enter to toggle between Yes and No.

- Yes enables the DSLPipe to send warning, notice, and CDR records to the Syslog host.
- No disables the Syslog host, or specifies that a Syslog host is not available.

  No is the default.

Dependencies: If Syslog=Yes, you must enter the IP address of the Syslog host in the Log Host field.

Parameter Location: Ethernet Profile, Mod Config

See Also: Log Facility, Log Host

Sys Reset

Description: This command restarts the DSLPipe and clears all calls without disconnecting the device from its power source. The DSLPipe logs off all users, and returns user security to its default state. In addition, the DSLPipe performs power-on self tests (POSTs) when it restarts. These POSTs are diagnostic tests.

Usage: To perform a system reset, follow these steps:

1 Select Sys Reset and press Enter.

The DSLPipe prompts you to confirm that you want to perform the reset.

2 Confirm the reset.

The DSLPipe displays the message `System reset in progress`. In addition to clearing calls, the DSLPipe performs a series of POSTs. The POST display appears.

If you do not see the POST display, press Ctrl-L.

While the yellow CON LED on the front panel remains solidly lit, the DSLPipe checks system memory, configuration, and line connections. If the DSLPipe fails any of these tests, the CON LED remains lit or blinks.

When the tests are complete, this message appears:

```
Power-On Self Test PASSED
```

3 Press any key to display the Main Edit menu.

Parameter Location: Sys Diag

T391

Description: This parameter specifies the number of seconds between Status Enquiry messages.

Usage: Press Enter to open a text field. Then, type a number between 5 and 30. The default is 10. Press Enter again to close the text field.

Dependencies: The T391 parameter applies only if Link Mgmt=T1.617D and T392 is set to a nonzero value.

Parameter Location: Frame Relay Profile, Frame Relay

See Also: Link Mgmt

T392

Description: This parameter specifies the number of seconds that the DSLPipe waits for a Status Enquiry message before recording an error.

Usage: Press Enter to open a text field. Then, type 0 (zero), or a number between 5 and 30. The default is 15.

If you specify 0 (zero), the DSLPipe does not process WAN-side Status Enquiry messages. If you specify a nonzero value, the DSLPipe uses T1.617D (a link management protocol defined in ANSI T1.617 Annex D) to monitor another Ascend unit over a nailed-up connection.

Press Enter again to close the text field.

Dependencies: The T392 parameter applies only if Link Mgmt=T1.617D.

Parameter Location: Frame Relay Profile, Frame Relay

See Also: Link Mgmt

Target Util

Description: The Target Util parameter specifies the percent bandwidth utilization at which the DSLPipe adds or subtracts bandwidth dynamically.

This parameter specifies the target percentage of bandwidth utilization for an MP+ call (Encaps=MPP).

The DSLPipe uses the historical time period specified by the Sec History parameter as the basis for calculating average line utilization (ALU) of transmitted data. It then compares ALU to the amount specified in the Target Util parameter.

When ALU exceeds the threshold defined by Target Util for a period of time greater than the value of the Add Pers parameter, the DSLPipe attempts to add a channel. When ALU falls below the threshold defined by Target Util for a period of time greater than the value of the Sub Pers parameter, the DSLPipe attempts to remove a channel.

Usage: Press Enter to open a text field. Then, type a number between 0 and 100. Press Enter again to close the text field.

The default is 70. When the value is 70%, the device adds bandwidth when it exceeds a 70 percent utilization rate, and subtracts bandwidth when it falls below that number.

Dependencies: When selecting a target utilization value, keep these guidelines in mind:

- Monitor how the application behaves when using different bandwidths.
  For example, an application might be able to use 88% of a 64-kbps link, but only 70% of a 256-kbps link.
- Monitor the application at different loads.

Parameter Location: Answer Profile, Answer/PPP options
Connection Profile, Connections/Encaps options

See Also: Add Pers, Call Type, Dyn Alg, Sec History, Sub Pers

TCP Estab

Description: In a filter of type IP, this parameter specifies whether the filter should match only established TCP connections.

An established TCP connection is one in which the TCP session has already sent its first packet. A not established TCP connection is one in which the TCP sessions has not sent its first packet. Specifically, the first packet is the "connection request" packet which has SYN bit set to 1, while both the ACK and RST bits are set to 0.

Usage: Press Enter to toggle between Yes and No.

- Yes specifies that you want the filter to match only those TCP connections that are established.

  Yes causes the filter to accept TCP connection request packets, then begin filtering on the rest of the incoming packets.
- No specifies that you want the filter to match both initial and established TCP connections.

  No is the default.

Dependencies: The TCP Estab parameter does not apply (TCP Estab=N/A) if the Protocol field is set to any value other than 6 (TCP).

Parameter Location: Filter Profile, Filter/IP

Telnet PW

Description: This parameter specifies the password that you must enter before you can access the DSLPipe user interface through Telnet.

Telnet is a protocol used to link two computers in order to provide a terminal with a connection to the remote machine. The remote machine is known as the Telnet host. When you start a Telnet session, you connect to the Telnet host and log in. The connection enables you to work with the remote machine as though you were at a terminal connected to it.

Usage: Press Enter to open a text field. Then, type a password containing up to 20 alphanumeric characters. The default is [ ].

If you leave Telnet PW blank, the DSLPipe does not prompt you for a password. If you specify a password for Telnet PW, you have three tries of 60 seconds each to enter the correct password.

Parameter Location: Ethernet Profile, Mod Config/Ether options

Term Rate

Description: This parameter specifies the data rate for the Control Monitor port in bits per second.

The Control Monitor is a menu-based user interface for configuring, managing, and monitoring the DSLPipe. It consists of nine windows—eight status windows and a single edit window.

Usage: Press Enter to cycle through the choices.

- 57600
- 38400
- 19200
- 9600
  9600 is the default.
- 4800
- 2400
- 1200
- 300

Dependencies: Whenever you modify the Term Rate parameter, you must set the data rate of your terminal accordingly.

- When you operate the DSLPipe from a local terminal, the most common data rate is 9600 bps.
- If you are managing an Ascend unit remotely, you may want to increase the baud rate on the local terminal to a higher speed for improved performance.

Parameter Location: System Profile, Sys Config

Term Serv

Description: This command starts a local terminal server session.

A terminal server is a computing device to which a terminal can connect over a LAN or WAN link. A terminal server session is an end-to-end connection between a terminal and a terminal server. Usually, the terminal server session begins when the call goes online and ends when the call disconnects.

The DSLPipe supports local terminal server sessions only. A local terminal server session takes place when a terminal (or a computer emulating a terminal) is connected to the DSLPipe Control port, or when you open a Telnet connection to the DSLPipe from a local IP host.

Select the Term Serv command from the Sys Diag menu and press Enter to begin the terminal server session. A local terminal server session has access to only a subset of the commands available to a remote terminal server session.

The DSLPipe supports all the common capabilities of standard terminal servers, including Telnet, Domain Name Services (DNS), login and password control, call detail reporting, and authentication services.

Usage: Highlight Term Serv and press Enter to begin the local terminal server session.

Do not use the Term Serv parameter to return to the terminal server command-line interface from a local Telnet session; use Ctrl-D-C instead.

For complete information on the tasks you can carry out during a terminal server session, see the *DSLPipe User's Guide*.

Parameter Location: Sys Diag

See Also: Telnet PW

Tick Count

Description: This parameter identifies the distance to the destination network in IBM PC clock ticks (18 Hz). This value is for round-trip timer calculation and for determining the nearest server of a given type.

Usage: In most cases, the default value (12) is appropriate. If you need to change this value, press Enter to open a text field. Then, type an appropriate value. Press Enter again to close the text field.

Dependencies: For the Tick Count parameter to apply, you must enable IPX routing in the Connection Profile by setting Route IPX=Yes.

Parameter Location: IPX Routes Profile, IPX Routes

See Also: Route IPX

Type

Description: This parameter appears in a Filter Profile or an IPX SAP Filter Profile. Its functionality differs depending on the profile:

- In a Filter Profile, the Type parameter specifies how the DSLPipe applies a filter to a packet.
- In an IPX SAP Profile, the Type parameter specifies whether the filter excludes the service from the service table.

Usage: Your usage differs depending on the profile.

Filter Profile

Press Enter to cycle through the choices.

- Generic specifies that the filter examines byte and offset values within a packet, regardless of which protocol is in use.
- Ip specifies that the filter examines the protocol ID number, address, and port specifications in an IP packet.

IPX SAP Filter Profile

Press Enter to cycle through the choices.

- Exclude specifies that the filter excludes the service from the service table. Exclude is the default.
- Include specifies that the filter includes the service in the service table.

Dependencies: Keep this additional information in mind:

- In a Filter Profile for a filter of type Generic, the DSLPipe uses these parameters to specify how the filter operates:
  - Length
  - Mask
  - More
  - Offset
  - Value
- In a Filter Profile for a filter of type IP, the DSLPipe uses these parameters to specify how the filter operates:
  - Dst Adrs
  - Dst Mask
  - Dst Port #
  - Dst Port Cmp
  - Protocol
  - Src Adrs
  - Src Mask
  - Src Port #
  - Src Port Cmp
  - TCP Estab

Parameter Location: Filter Profile, Filters
IPX SAP Filter Profile, IPX SAP Filters

See Also: Server Name, Server Type, Station, UDP Port, Valid

UDP Cksum

Description: This parameter specifies that the Ascend unit generates a UDP checksum whenever it sends out a UDP packet.

Currently the DSLPipe uses UDP when generating queries and responses for the following protocols:

- ATMP
- SYSLOG
- DNS
- ECHOSERV
- RADIUS
- TACACS
- RIP
- SNTP
- TFTP

Usage: Press Enter to toggle between Yes and No.

- Yes specifies that the Ascend unit generates a UDP checksum when transmitting a UDP packet.

  Specify this setting if data integrity is of the highest concern for your environment, and having redundant checks is important; this setting is also appropriate if your UDP-based servers are located on the remote side of a WAN link that is prone to errors.

- No specifies that the Ascend unit does not generate a UDP checksum when transmitting a UDP packet.

  No is the default. Accept this setting if you plan to use the data integrity guarantee of the Ethernet or PPP checksum only.

Parameter Location: Ethernet Profile: Ethernet→Mod Config

Valid

Description: This parameter activates or deactivates a filter. Its functionality differs depending on the profile:

- In a Filter Profile, the Valid parameter activates or deactivates a call filter or a data filter.
- In an IPX SAP Filter Profile, the Valid parameter activates or deactivates the Input filter or the Output filter.

Usage: Press Enter to toggle between Yes and No.

- Yes activates the filter.
- No deactivates the filter.
  No is the default.

Dependencies: Keep this additional information in mind:

- When Valid=No, N/A appears in all fields of the filter specification; therefore, you cannot define a filter specification unless Valid=Yes.
- If you are using more than one filter, set Valid=Yes and Forward=Yes in at least one filter; otherwise, the DSLPipe drops all packets.
- To forward all packets, set all filters to Valid=No.

Parameter Location: Filter Profile, Filters
IPX SAP Filter Profile, IPX SAP Filters

See Also: Server Name, Server Type, Type

Value

Description: In a filter of type Generic, this parameter specifies a 16-bit hexadecimal value to compare against the data contained within the specified bytes in a packet. You specify the bytes using the Length, Offset, and Mask parameters.

Usage: Press Enter to open a text field. Then, type a hexadecimal number. You can enter a number from 00 to ffffffffffffffff.

The default is 00. When you accept the default, the bytes must contain nothing to match the filter.

Press Enter again to close the text field.

Example: `e0e0030000000000`

Dependencies: Keep this additional information in mind:

- The DSLPipe compares only the unmasked portion of a packet to the Value parameter.
- The length of the Value parameter must contain the number of bytes specified by the Length parameter.

Parameter Location: Filter Profile, Filter/Generic

See Also: Length, Mask, Offset

VJ Comp

Description: This parameter turns TCP/IP header compression on or off. VJ Comp stands for Van Jacobson Compression.

Usage: Press Enter to toggle between Yes and No.

- Yes turns on TCP/IP header compression for both ends of the link.
  Yes is the default. The Ascend unit must include the optional compression module.
- No turns off TCP/IP header compression.

Dependencies: Keep this additional information in mind:

- VJ Comp applies only to packets in TCP applications, such as Telnet.
  Telnet is a protocol used to link two computers in order to provide a terminal with a connection to the remote machine. The remote machine is known as the Telnet host. When you start a Telnet session, you connect to the Telnet host and log in. The connection enables you to work with the remote machine as though you were at a terminal connected to it.
- Turning on header compression is most effective in reducing overhead when the data portion of the packet is small.

Parameter Location: Answer Profile, Answer/PPP options
Connection Profile, Connections/Encaps options

WAN Alias

Description: This parameter specifies the IP address of the link's remote interface to the WAN.

The WAN Alias parameter applies only if the remote end of a link uses an implementation of PPP that requires that both ends of a WAN connection be on the same subnet.

If a router requires an IP number for each interface over which it sends or receives packets, that router is said to use numbered interfaces. The WAN Alias parameter assigns a single IP number to all WAN lines connected to the DSLPipe. Furthermore, the DSLPipe assumes that all devices using numbered interfaces have agreed on the network number of the WAN; that is, if 10.0.2.1 is the DSLPipe interface to the WAN, then the WAN has a network number 10.0.2.0 and all other devices using numbered interfaces agree to have a 10.0.2.*x* address.

Usage: Press Enter to open a text field. Then, type the IP address of the remote device.

An IP address consists of four numbers between 0 and 255, separated by periods. If a netmask is in use on the network, you must specify it. Separate the netmask from the IP address with a slash.

The default is 0.0.0.0/0.

Press Enter again to close the text field.

Example: `200.207.23.7/24`

Dependencies: The WAN Alias parameter does not apply if the DSLPipe does not support IP (Route IP=No).

Parameter Location: Connection Profile, Connections

See Also: Route IP, Route

Index

Numerics

A

B

C

D

E

F

G

H

I

L

M

N

O

P

R

S

T

U

V

W

Y